

Pivotal Cloud Foundry®

Version v2.2

Published: 25 June 2019

Table of Contents

| | |
|--|-----|
| Table of Contents | 2 |
| PCF v2.2 Feature Highlights | 10 |
| Pivotal Cloud Foundry Release Notes | 15 |
| PCF v2.2 Breaking Changes | 16 |
| PCF Ops Manager v2.2 Release Notes | 19 |
| Pivotal Application Service v2.2 Release Notes | 38 |
| PAS for Windows v2.2 Release Notes | 68 |
| PCF Isolation Segment v2.2 Release Notes | 73 |
| Stemcell Release Notes | 82 |
| Stemcell (Linux) Release Notes | 84 |
| Stemcell v1709.x (Windows Server version 1709) Release Notes | 124 |
| Tiles Using Xenial Stemcells in PCF | 129 |
| Platform Architecture and Planning | 130 |
| AWS Reference Architecture | 136 |
| Azure Reference Architecture | 140 |
| GCP Reference Architecture | 147 |
| OpenStack Reference Architecture | 154 |
| vSphere Reference Architecture | 157 |
| Using Edge Services Gateway on VMware NSX | 168 |
| Upgrading vSphere without PCF Downtime | 181 |
| Migrating PCF to a New Datastore in vSphere | 183 |
| Control Plane Reference Architectures | 185 |
| Implementing a Multi-Foundation PKS Deployment | 193 |
| Global DNS Load Balancers for Multi-Foundation Environments | 195 |
| Architecture and Installation Overview | 197 |
| Preparing Your Firewall | 200 |
| IaaS Permissions Guidelines | 202 |
| Installing PCF in Airgapped Environments | 203 |
| Installing Pivotal Cloud Foundry on AWS | 211 |
| AWS Permissions Guidelines | 215 |
| Installing PCF on AWS Manually | 216 |
| Configuring BOSH Director on AWS | 238 |
| Deploying PAS on AWS | 256 |
| Installing PCF on AWS using Terraform | 296 |
| Deploying Ops Manager on AWS Using Terraform | 297 |
| Configuring BOSH Director on AWS Using Terraform | 301 |
| Deploying PAS on AWS Using Terraform | 318 |
| Deleting PCF from AWS | 358 |
| Creating a Proxy ELB for Diego SSH | 362 |
| Upgrading BOSH Director on AWS | 365 |
| Installing Pivotal Cloud Foundry on Azure | 369 |
| Installing PCF on Azure Manually | 372 |
| Preparing to Deploy Ops Manager on Azure Manually | 373 |
| Deploying Ops Manager on Azure Manually | 377 |
| Configuring BOSH Director on Azure Manually | 386 |
| Deploying PAS on Azure | 404 |
| Installing PCF on Azure Using Terraform | 443 |
| Deploying Ops Manager on Azure Using Terraform | 444 |

| | |
|---|-----|
| Configuring BOSH Director on Azure Using Terraform | 447 |
| Deploying PAS on Azure Using Terraform | 465 |
| Troubleshooting PCF on Azure | 503 |
| Deleting a PCF on Azure Installation | 506 |
| Upgrading BOSH Director on Azure | 507 |
| Installing Pivotal Cloud Foundry on GCP | 512 |
| Recommended GCP Quotas | 515 |
| Installing PCF on GCP Manually | 516 |
| Preparing to Deploy Ops Manager on GCP Manually | 517 |
| Deploying Ops Manager on GCP Manually | 537 |
| Configuring BOSH Director on GCP Manually | 540 |
| Deploying PAS on GCP | 555 |
| Installing PCF on GCP Using Terraform | 598 |
| Deploying Ops Manager on GCP Using Terraform | 599 |
| Configuring BOSH Director on GCP Using Terraform | 603 |
| Deploying PAS on GCP Using Terraform | 618 |
| Configuring a Shared VPC on GCP | 659 |
| Deleting PCF from GCP | 663 |
| Troubleshooting PCF on GCP | 665 |
| Upgrading BOSH Director on GCP | 667 |
| Installing Pivotal Cloud Foundry on OpenStack | 671 |
| Deploying Ops Manager on OpenStack | 674 |
| Configuring BOSH Director on OpenStack | 684 |
| Deploying PAS on OpenStack | 704 |
| PCF on vSphere Requirements | 744 |
| vSphere Service Account Requirements | 748 |
| Deploying Ops Manager on vSphere | 752 |
| Configuring BOSH Director on vSphere | 755 |
| Deploying PAS on vSphere | 773 |
| Deploying PAS with NSX-T Networking | 813 |
| vSphere Virtual Disk Types | 825 |
| Using the Cisco Nexus 1000v Switch with Ops Manager | 827 |
| Using BOSH Resurrector and vSphere HA | 830 |
| Configuring Pivotal Cloud Foundry SSL Termination for vSphere Deployments | 833 |
| Availability Zones in vSphere | 835 |
| Updating NSX Security Group and Load Balancer Information | 837 |
| Installing PCF Isolation Segment | 840 |
| Getting Started with Small Footprint PAS | 855 |
| Upgrading Pivotal Cloud Foundry | 861 |
| What Happens During PAS Upgrades | 866 |
| Upgrade Preparation Checklist for PCF v2.2 | 869 |
| Configuring PAS for Upgrades | 877 |
| Upgrade Load Example: Pivotal Web Services | 881 |
| Upgrading PAS and Other Pivotal Cloud Foundry Products | 884 |
| cf push Availability During Pivotal Application Service Upgrades | 887 |
| PCF Dev Overview | 888 |
| Backing Up and Restoring Pivotal Cloud Foundry | 890 |
| Disaster Recovery in Pivotal Cloud Foundry | 891 |
| Backing Up Pivotal Cloud Foundry with BBR | 896 |
| Enabling External Blobstore Backups | 911 |

| | |
|--|------|
| PAS Component Availability During Backup | 914 |
| Restoring PCF from Backup with BBR | 917 |
| Setting Up Your Jumpbox for BBR | 931 |
| Troubleshooting BBR | 933 |
| Using Ops Manager | 936 |
| Using the Ops Manager API | 938 |
| Using the Ops Manager Interface | 941 |
| Adding and Deleting Products | 952 |
| Importing and Managing Stemcells | 956 |
| Applying Changes to BOSH Director | 958 |
| Creating UAA Clients for BOSH Director | 959 |
| Using Your Own Load Balancer | 961 |
| Creating and Managing Ops Manager User Accounts | 963 |
| Configuring Role-Based Access Control (RBAC) in Ops Manager | 965 |
| Logging In to Apps Manager | 969 |
| Adding Existing SAML or LDAP Users to a PCF Deployment | 970 |
| Modifying Your Ops Manager Installation and Product Template Files | 972 |
| Managing Errands in Ops Manager | 975 |
| Monitoring PCF VMs from Ops Manager | 978 |
| PAS Concepts | 980 |
| Cloud Foundry Overview | 981 |
| How Apps Are Staged | 984 |
| Application Container Lifecycle | 987 |
| High Availability in Cloud Foundry | 989 |
| How Cloud Foundry Maintains High Availability | 993 |
| Orgs, Spaces, Roles, and Permissions | 994 |
| Cloud Foundry Security | 997 |
| Container Security | 1002 |
| Container-to-Container Networking | 1006 |
| Application Security Groups | 1010 |
| GrootFS Disk Usage | 1017 |
| Cloud Foundry Components | 1019 |
| Cloud Controller | 1022 |
| Cloud Controller Blobstore | 1024 |
| Messaging (NATS) | 1026 |
| Gorouter | 1028 |
| User Account and Authentication (UAA) Server | 1031 |
| Garden | 1041 |
| HTTP Routing | 1043 |
| Diego Components and Architecture | 1049 |
| Application SSH Components and Processes | 1054 |
| How Diego Balances App Processes | 1055 |
| PCF Operator Guide | 1058 |
| Identifying the API Endpoint for Your PAS Instance | 1059 |
| Creating New PAS User Accounts | 1060 |
| Configuring SSL/TLS Termination at HAProxy | 1061 |
| Configuring Frontend Idle Timeout for Gorouter and HAProxy | 1064 |
| Configuring Route Service Lookup | 1065 |
| Configuring Proxy Settings for All Applications | 1069 |
| Restricting App Access to Internal PCF Components | 1071 |

| | |
|--|------|
| Configuring Application Security Groups for Email Notifications | 1075 |
| Configuring SSH Access for PCF | 1078 |
| Securing Services Instance Credentials with Runtime CredHub | 1080 |
| Identifying PAS Jobs Using vCenter | 1083 |
| Configuring Logging in PAS | 1085 |
| Configuring UAA Password Policy | 1092 |
| Managing Internal MySQL for PAS | 1094 |
| Scaling Internal MySQL for PAS | 1095 |
| Migrating to Internal Percona MySQL | 1099 |
| Running mysql-diag | 1102 |
| Recovering From MySQL Cluster Downtime | 1105 |
| Configuring Authentication and Enterprise SSO for PAS | 1111 |
| Configuring ADFS as an Identity Provider | 1118 |
| Configuring CA as an Identity Provider | 1120 |
| Configuring PingFederate as an Identity Provider | 1123 |
| Switching Application Domains | 1124 |
| Scaling PAS | 1127 |
| Using Docker Registries | 1131 |
| Configuring Cell Disk Cleanup Scheduling | 1134 |
| Custom Branding Apps Manager | 1137 |
| Reporting App, Task, and Service Instance Usage | 1142 |
| Reporting Instance Usage with Apps Manager | 1147 |
| Providing a Certificate for Your TLS Termination Point | 1149 |
| Enabling NFS Volume Services | 1151 |
| Rotating Runtime CredHub Encryption Keys | 1154 |
| Administrating PAS | 1156 |
| Managing the Runtime | 1157 |
| Stopping and Starting Virtual Machines | 1158 |
| Creating and Modifying Quota Plans | 1161 |
| Using Feature Flags | 1165 |
| Examining GrootFS Disk Usage | 1167 |
| Managing Custom Buildpacks | 1172 |
| Using Docker in Cloud Foundry | 1174 |
| User Accounts and Communications | 1176 |
| Creating and Managing Users with the cf CLI | 1177 |
| Creating and Managing Users with the UAA CLI (UAAC) | 1179 |
| Getting Started with the Notifications Service | 1185 |
| Routing | 1188 |
| Enabling IPv6 for Hosted Applications | 1189 |
| Supporting WebSockets | 1190 |
| Configuring Load Balancer Healthchecks for Cloud Foundry Routers | 1192 |
| Securing Traffic into Cloud Foundry | 1194 |
| Enabling TCP Routing | 1203 |
| Isolation Segments | 1206 |
| Managing Isolation Segments | 1207 |
| Routing for Isolation Segments | 1211 |
| Monitoring PAS | 1217 |
| Key Performance Indicators | 1218 |
| Key Capacity Scaling Indicators | 1241 |
| Selecting and Configuring a Monitoring System | 1247 |

| | |
|--|------|
| Pivotal Application Service for Windows | 1249 |
| Deploying .NET Apps | 1251 |
| Product Architecture | 1252 |
| Downloading or Creating Windows Stemcells | 1254 |
| Creating a Windows Stemcell for vSphere Manually | 1256 |
| Creating a Windows Stemcell for vSphere Using stembuild (Beta) | 1265 |
| Installing and Configuring PASW | 1272 |
| Windows Cells in Isolation Segments | 1276 |
| Migrating Apps to PAS for Windows | 1278 |
| Upgrading PAS for Windows and Windows Cells | 1280 |
| Using SMB Volumes in .NET Apps | 1281 |
| Troubleshooting Windows Cells | 1285 |
| Using Apps Manager | 1290 |
| Getting Started with Apps Manager | 1291 |
| Managing Orgs and Spaces Using Apps Manager | 1293 |
| Managing User Roles with Apps Manager | 1296 |
| Managing Apps and Service Instances Using Apps Manager | 1299 |
| Scaling an Application Using App Autoscaler | 1315 |
| Using the App Autoscaler CLI | 1321 |
| Viewing ASGs in Apps Manager | 1326 |
| Configuring Spring Boot Actuator Endpoints for Apps Manager | 1328 |
| Using Spring Boot Actuators with Apps Manager | 1331 |
| Using the Cloud Foundry Command Line Interface (cf CLI) | 1339 |
| Installing the cf CLI | 1340 |
| Getting Started with the cf CLI | 1343 |
| Using the cf CLI with a Proxy Server | 1348 |
| Using the cf CLI with a Self-Signed Certificate | 1351 |
| Using cf CLI Plugins | 1353 |
| Developing cf CLI Plugins | 1356 |
| Cloud Foundry CLI Reference Guide | 1357 |
| Developer Guide | 1365 |
| cf push | 1366 |
| Deploy an Application | 1367 |
| Deploying with Application Manifests | 1371 |
| Deploy an App with Docker | 1383 |
| Deploying a Large Application | 1387 |
| Starting, Restarting, and Restaging Applications | 1389 |
| Pushing an App with Multiple Processes (Beta) | 1391 |
| Running cf push Sub-Step Commands (Beta) | 1393 |
| Using Blue-Green Deployment to Reduce Downtime and Risk | 1395 |
| Troubleshooting Application Deployment and Health | 1398 |
| SSH for Apps and Services | 1403 |
| Application SSH Overview | 1404 |
| Accessing Apps with SSH | 1406 |
| Accessing Services with SSH | 1411 |
| Routes and Domains | 1413 |
| Routes and Domains | 1414 |
| Managing Services | 1424 |
| Managing Service Instances with the cf CLI | 1425 |
| Sharing Service Instances (Beta) | 1430 |

| | |
|---|------|
| Delivering Service Credentials to an Application | 1433 |
| Managing Service Keys | 1436 |
| Configuring Play Framework Service Connections | 1438 |
| Using an External File System (Volume Services) | 1439 |
| User-Provided Service Instances | 1444 |
| Detailed documentation to help you install, understand, and succeed with Pivotal's enterprise-grade software. | 1446 |
| owner: | 1446 |
| Streaming Application Logs to Log Management Services | 1447 |
| Service-Specific Instructions for Streaming Application Logs | 1450 |
| Streaming Application Logs to Splunk | 1457 |
| Streaming Application Logs with Fluentd | 1459 |
| Streaming Application Logs to Azure OMS Log Analytics (Beta) | 1460 |
| Detailed documentation to help you install, understand, and succeed with Pivotal's enterprise-grade software. | 1464 |
| owner: | 1464 |
| Running Tasks | 1465 |
| Scaling an Application Using cf scale | 1468 |
| Using Application Health Checks | 1469 |
| Configuring Container-to-Container Networking | 1472 |
| Cloud Foundry Environment Variables | 1475 |
| Cloud Controller API Client Libraries | 1483 |
| Considerations for Designing and Running an Application in the Cloud | 1484 |
| PCF Security and Compliance Guide | 1487 |
| Security Processes | 1488 |
| Pivotal Cloud Foundry Security Overview and Policy | 1489 |
| PCF Testing, Release, and Security Lifecycle | 1491 |
| Security Concepts | 1494 |
| PCF Infrastructure Security | 1495 |
| Stemcell Security | 1496 |
| Linux Stemcell Hardening | 1497 |
| Certificates and TLS in PCF | 1501 |
| TLS Connections in PCF | 1502 |
| Custom Certificate Authorities | 1509 |
| Managing Certificates with the Ops Manager API | 1510 |
| Rotating Certificates | 1512 |
| Trusted System Certificates | 1521 |
| Disk Encryption | 1522 |
| Security Event Logging | 1525 |
| Network Security | 1531 |
| BOSH DNS Network Communications | 1532 |
| Cloud Controller Network Communications | 1535 |
| Consul Network Communications | 1537 |
| Container-to-Container Networking Communications | 1539 |
| CredHub Network Communications | 1540 |
| Diego Network Communications | 1541 |
| Loggregator Network Communications | 1543 |
| MySQL Network Communications | 1544 |
| NATS Network Communications | 1546 |
| Routing Network Communications | 1547 |

| | |
|---|------|
| UAA Network Communications | 1549 |
| Credential and Identity Management | 1550 |
| Pivotal Cloud Foundry User Types | 1552 |
| Retrieving Credentials from Your Deployment | 1555 |
| CredHub | 1561 |
| CredHub Credential Types | 1564 |
| Security for Apps and Services | 1565 |
| Compliance and Other Security-Related Topics | 1566 |
| Assessment of Pivotal Cloud Foundry against NIST SP 800-53(r4) Controls | 1567 |
| General Data Protection Regulation | 1568 |
| Security-Related PCF Tiles and Add-ons | 1573 |
| Security Guidelines for Your IaaS Provider | 1574 |
| How to Use This Topic | 1574 |
| Buildpacks | 1575 |
| About Buildpacks | 1577 |
| Buildpacks | 1578 |
| Stack Association | 1583 |
| Pushing an Application with Multiple Buildpacks | 1585 |
| Using a Proxy | 1586 |
| Supported Binary Dependencies | 1587 |
| Production Server Configuration | 1588 |
| Binary Buildpack | 1590 |
| Go Buildpack | 1592 |
| HWC Buildpack | 1596 |
| Creating an Extension Buildpack for .NET Apps | 1599 |
| Tips for .NET Developers | 1602 |
| Java Buildpack | 1606 |
| Tips for Java Developers | 1608 |
| Getting Started Deploying Java Apps | 1615 |
| Getting Started Deploying Grails Apps | 1616 |
| Getting Started Deploying Ratpack Apps | 1623 |
| Getting Started Deploying Spring Apps | 1629 |
| Configuring Service Connections | 1635 |
| Configuring Service Connections for Grails | 1636 |
| Configuring Service Connections for Play Framework | 1639 |
| Configuring Service Connections for Spring | 1640 |
| Cloud Foundry Java Client Library | 1648 |
| .NET Core Buildpack | 1651 |
| NGINX Buildpack | 1657 |
| Node.js Buildpack | 1659 |
| Tips for Node.js Applications | 1662 |
| Environment Variables Defined by the Node Buildpack | 1665 |
| Configuring Service Connections for Node.js | 1666 |
| PHP Buildpack | 1668 |
| Tips for PHP Developers | 1671 |
| Getting Started Deploying PHP Apps | 1672 |
| PHP Buildpack Configuration | 1675 |
| Composer | 1679 |
| Sessions | 1681 |
| New Relic | 1682 |

| | |
|---|------|
| Python Buildpack | 1683 |
| R Buildpack | 1687 |
| Ruby Buildpack | 1690 |
| Tips for Ruby Developers | 1693 |
| Getting Started Deploying Ruby Apps | 1699 |
| Getting Started Deploying Ruby Apps | 1700 |
| Getting Started Deploying Ruby on Rails Apps | 1705 |
| Configure Rake Tasks for Deployed Apps | 1708 |
| Environment Variables Defined by the Ruby Buildpack | 1709 |
| Configure Service Connections for Ruby | 1710 |
| Support for Windows Gemfiles | 1713 |
| Staticfile Buildpack | 1714 |
| Customizing and Developing Buildpacks | 1719 |
| Creating Custom Buildpacks | 1720 |
| Packaging Dependencies for Offline Buildpacks | 1723 |
| Merging from Upstream Buildpacks | 1726 |
| Upgrading Dependency Versions | 1727 |
| Using CI for Buildpacks | 1732 |
| Releasing a New Buildpack Version | 1733 |
| Updating Buildpack-Related Gems | 1735 |
| Services | 1736 |
| Overview | 1737 |
| Managing Service Brokers | 1739 |
| Managing Access to Service Plans | 1743 |
| Dashboard Single Sign-On | 1746 |
| Example Service Brokers | 1750 |
| Binding Credentials | 1751 |
| Enabling Service Instance Sharing | 1753 |
| Application Log Streaming | 1755 |
| Route Services | 1756 |
| Supporting Multiple Cloud Foundry Instances | 1761 |
| Logging and Metrics | 1762 |
| Overview of Logging and Metrics | 1763 |
| Loggregator Architecture | 1765 |
| Loggregator Guide for Cloud Foundry Operators | 1767 |
| Deploying a Nozzle to the Loggregator Firehose | 1769 |
| Installing the Loggregator Firehose Plugin for cf CLI | 1775 |
| Application Logging in Cloud Foundry | 1777 |
| Customizing Platform Log Forwarding | 1781 |
| Troubleshooting and Diagnostics | 1783 |
| Diagnosing Problems in PCF | 1784 |
| Troubleshooting Problems in PCF | 1789 |
| Advanced Troubleshooting with the BOSH CLI | 1794 |
| Troubleshooting Slow Requests in Cloud Foundry | 1801 |
| Troubleshooting TCP Routes | 1804 |
| Troubleshooting Router Error Responses | 1807 |
| Troubleshooting Ops Manager for VMware vSphere | 1809 |

PCF v2.2 Feature Highlights

This topic highlights important new features included in Pivotal Cloud Foundry (PCF) v2.2.

PCF Operations Manager (Ops Manager) Highlights

Ops Manager v2.2 includes the following major features:

Ops Manager API Documentation is Public

In time for the Ops Manager v2.2 release, Ops Manager API documentation is accessible publicly through docs.pivotal.io. Previously, you could only access the Ops Manager API documentation through your own Ops Manager.

For v2.2 Ops Manager API documentation, see [PCF Ops Manager API Reference](#).

Multiple Data Centers on vSphere

Ops Manager now supports multiple vSphere vCenters on a single vSphere BOSH Director tile. This allows you to spread instances across regions without having to deploy and manage multiple PCF foundations.

For more information about how to add, edit, and delete vCenters, see [Managing Multiple vSphere vCenters](#).

Selectively Deploy Tiles in Ops Manager or via an API Endpoint

You can now choose to deploy a selection of tiles rather than all tiles in Ops Manager. This feature allows you to reduce the amount of change in any given deployment, which drastically reduces deployment time.

This feature is in beta for Ops Manager, and is generally available as an API endpoint. For more information, see [Triggering an install process](#) in the Ops Manager API documentation.



Note: Ops Manager is soliciting feedback for this feature. Submit feedback through your product architect or directly by emailing opsmanager-feedback+selective_deploys@pivotal.io.

Ops Manager Stores Past Manifests

Through the Ops Manager API, you can see Ops Manager's manifest history. Manifest history is helpful for running `diff` commands on manifests to see changes over time.

Azure Stack is Generally Available

Pivotal officially supports Azure Stack.

Azure Stack is a hybrid cloud platform that lets you deliver Azure services from your own on-premise datacenter. For more information about Azure Stack, see [What is Azure Stack?](#) from the Microsoft Azure documentation.

Ops Manager Supports Azure China

Ops Manager now supports a special region in Azure called Azure China. Azure China is a physically separated instance of cloud services that is located in China and independently operated. For more information about Azure China, see [What is Azure China 21Vianet?](#) in the Azure China documentation.


Ops Manager Credentials Stored in CredHub

For even greater security, Ops Manager sends user-specified credentials to BOSH CredHub on each deployment. For more information about where Ops Manager-specific credentials are stored, see [BOSH CredHub](#).

For information about how this feature affects tile authors, see [PCF v2.2 Partners Release Notice](#) in the *PCF Tile Developer Guide*.

Secret Text Areas

Ops Manager v2.2 supports secret text areas in tile configuration panes. This feature is useful for tiles that require PCF operators to enter multi-line credentials during configuration.

When a user enters text into a secret text area and clicks **Save**, the Ops Manager UI replaces the text with an . Additionally, users of the Ops Manager API can not retrieve text entered in secret text areas. Ops Manager stores this text in CredHub.


Tile authors can mark a text area as `secret` by setting `type: secret` and `display_type: text_area` in the property blueprint for their tile.

For more information, see the [Custom Forms and Properties](#) section of the *Tile Generator* topic.

Specify a Custom Trusted SSL Certificate

Operators can specify a custom trusted SSL certificate and key for the Ops Manager server so that traffic isn't exposed to man-in-the-middle attacks when using Ops Manager.

By default, Ops Manager uses an auto-generated self-signed certificate. To change this configuration to your own SSL certificate, go to **Settings** from the Ops Manager Installation Dashboard and select the **SSL Certificate** pane. For more information about Ops Manager settings, see [Settings Page](#) in the *Understanding the Ops Manager Interface* topic.

 **Note:** Custom SSL certificate and key is persisted between upgrades. Custom SSL only needs a one-time configuration.

Configure an Ops Manager Syslog Server

You can configure a syslog server for Ops Manager logs. Logs include rails production logs, audit logs, UAA logs, nginx logs, and upstart logs for Ops Manager processes. Previous to this change, Ops Manager logs were not centralized in one accessible location. You also have the option to TLS-encrypt your logs.

For more information about configuring syslog for Ops Manager, see [Settings Page](#) in the *Understanding the Ops Manager Interface* topic.

TLS for Internal Blobstore Supported

Ops Manager now supports TLS communications for your internal blobstore. Ops Manager automatically generates and rotates TLS certifications for you.

To enable internal blobstore TLS communications, all of your tiles must have stemcells v3468 or later. You must also disable **Allow Legacy Agents** in the **Director Config** pane of the BOSH Director tile.

Custom TLS Certificate for External MySQL Database Supported

Ops Manager now allows you to configure a custom TLS certificate for an external MySQL database.


For more information, see the **Director Config Page** section of the [Ops Manager Director installation topic for your IaaS](#).

Custom Identification Tags Supported


If you have more than one PCF foundation, identification tags allow you to easily identify which foundation your VMs belong to when viewing your IaaS. You are able to set custom **Identification Tags** in the **Director Config** pane of your BOSH Director tile.

BOSH DNS Enabled By Default

BOSH DNS is enabled for both app containers and PCF components in v2.2. In previous versions, Consul managed service discovery between PCF components, but Consul is being replaced by BOSH DNS. BOSH DNS lets app containers and PCF components look up services with the BOSH DNS service discovery mechanism. To support BOSH DNS, the Ops Manager Director colocates a BOSH DNS server on every deployed VM. This does not negatively impact performance.

 **Note:** In PCF v2.2, Consul and BOSH DNS are both available in PCF, but BOSH DNS is the only service used for DNS requests.

BOSH DNS is enabled by default. You can disable BOSH DNS if instructed to do so by Pivotal support. From the Ops Manager installation dashboard, click the Ops Manager tile. In the **Director Config** tab, select the **Disable BOSH DNS server for troubleshooting purposes**.

 **warning:** Do not disable BOSH DNS without instructions from Pivotal support. Disabling BOSH DNS will also disable PKS, NSX-T, and several PAS features. If you disabled BOSH DNS in PCF v2.1, reenable it before upgrading to PCF v2.2.

Change Log Includes Products Deployed but Unchanged

The [Change Log](#) pane lists products as **Unchanged** when they remain deployed, but their configuration has not changed from a prior deployment, so Ops Manager did not re-deploy them.


Pivotal Application Service (PAS) Highlights

More Secure Cipher Suites for CF SSH

For greater security, the SSH proxy now accepts a narrower range of ciphers, MACs, and key exchanges when you call `cf ssh` from the CF CLI.

TLS-Encrypted Option for Internal System Databases

For internal system databases, PAS now supports a more secure [Percona Server](#) database with TLS-encrypted communication between server nodes, as well as the previous [MariaDB](#) option. See [Migrating to Internal Percona MySQL](#) for details.

 **warning:** Migrating PAS internal databases to using TLS causes temporary downtime of PAS system functions. It does not interrupt apps hosted by PAS.

Support for AWS Instance Profiles

PAS now supports [AWS instance profiles](#) when you are configuring an S3 filestore. Either an instance profile or an access and secret key are required.

For more information, see the **External or S3 Filestore** section of the [PAS installation topic for your IaaS](#).

Unversioned S3 Buckets for Backups

PAS can now back up unversioned S3 buckets used for external file storage, saving backup artifacts to separate, dedicated backup buckets. For more information, see the **External or S3 Filestore** section the [PAS installation topic for your IaaS](#).

Gorouter Logging Changes for GDPR Compliance

You can now disable logging of client IP addresses in the Gorouter to comply with the General Data Protection Regulation (GDPR).

For more information about this feature, see [Gorouter Logging Changes for GDPR Compliance](#) in *Pivotal Application Service v2.2 Release Notes*.


New Format for Diego Timestamps

You can now use a human- and machine-readable format, RFC 3339, for Diego timestamps in logs. RFC 3339 format also prevents the need for log aggregation systems to parse a complex timestamp.

New installations of the PAS, PAS for Windows, PAS for Windows 2012R2, and PCF Isolation Segment tiles now default to RFC 3339 format.

The Unix epoch format is set by default for upgrades to v2.2. You can enable the new timestamp format for Diego logs in the PAS tile.

For more information, see the **Configure Application Containers** section of the [PAS installation topic for your IaaS](#).

 **Breaking Change:** Before enabling RFC 3339 format for Diego logs, ensure that your log aggregation system anticipates the timestamp format change. If you experience issues, you can disable RFC 3339 format in the PAS tile.

Service Discovery for Container-to-Container Networking Enabled By Default

In PAS v2.1, service discovery for container-to-container networking was an experimental feature that you could opt in to use. In PAS v2.2, this feature is enabled by default, and you can opt out of using it.

For more information about disabling service discovery for container-to-container networking, see the **Configure Application Developer Controls** section of the [PAS installation topic for your IaaS](#).

DNS Search Domains


PAS v2.2 allows you to configure the DNS search domains used in containers by entering a comma-separated list.

For more information, see the **Container Networking** section of the [PAS installation topic for your IaaS](#).

Loggregator Introduces Log Cache

Loggregator adds an in-memory caching layer for logs and metrics and provides a RESTful interface for retrieving them. Unlike the `cf logs APP-NAME --recent` command, Log Cache gives you queryable, filterable data when you use it to retrieve recent logs for your apps.

For more information, see [Enable Log Cache](#).

 **Breaking Change:** If you disable Log Cache, App Autoscaler will fail. For more information about Log Cache, see [Loggregator Introduces Log Cache](#).

Forwarding of DEBUG Syslog Messages Disabled by Default

PAS v2.2 adds the **Don't Forward Debug Logs** checkbox, which disables forwarding of DEBUG syslog messages to external services.

The **Don't Forward Debug Logs** checkbox is enabled in PAS v2.2 by default. For more information about this feature, see [Forwarding of DEBUG Syslog Messages Disabled by Default](#)

Improved App Autoscaler CLI

App Autoscaler now allows you to create custom autoscaling rules and scheduled limit changes for your apps through the App Autoscaler CLI.

For more information about the App Autoscaler CLI, see [Using the App Autoscaler CLI](#).

Apps Manager Highlights

App Autoscaler UI Integrated into Apps Manager

The App Autoscaler UI is now integrated into Apps Manager. This enables users to configure autoscaling for their apps through Apps Manager.

For more information about scaling apps using App Autoscaler, see [Scaling an Application Using App Autoscaler](#).

PCF Isolation Segment Highlights

Gorouter Logging Changes for GDPR Compliance

See [Pivotal Application Service \(PAS\) Highlights](#) above and [Gorouter Logging Changes for GDPR Compliance](#) in *PCF Isolation Segment v2.2 Release Notes*.

New Format for Diego Timestamps

PCF Isolation Segment shares the [New Format for Diego Timestamps](#) feature in PAS.

DNS Search Domains

PCF Isolation Segment shares the new [DNS Search Domains](#) feature in PAS.

Pivotal Cloud Foundry Release Notes

Pivotal Cloud Foundry is certified by the Cloud Foundry Foundation for 2019.

Read more about the [certified provider program](#) and the [requirements of providers](#).

This topic provides links to the release notes for Pivotal Cloud Foundry (PCF). Release notes include new features, breaking changes, bug fixes, and known issues.

To find release notes for PCF services, navigate to the documentation for the desired service from [Pivotal Documentation](#).

PCF Release Notes

- [PCF v2.2 Breaking Changes](#)
- [PCF Ops Manager v2.2 Release Notes](#)

PCF Runtime Release Notes

- [Pivotal Application Service v2.2 Release Notes](#)
- [PAS for Windows v2.2 Release Notes](#)
- [PCF Isolation Segment v2.2 Release Notes](#)
- [Pivotal Container Service \(PKS\) v1.1 Release Notes](#)
- [Pivotal Container Service \(PKS\) v1.2 Release Notes](#)

Stemcell Release Notes

[Stemcell Release Notes](#)

PCF v2.2 Breaking Changes

This topic describes the breaking changes you need to be aware of when upgrading to Pivotal Cloud Foundry (PCF) v2.2. For more information about important preparation steps you must follow before beginning an upgrade, see [Upgrading Pivotal Cloud Foundry](#).

Pivotal Cloud Foundry

[PKS v1.3 Does Not Support Ops Manager v2.2](#)

PKS v1.3 only supports Ops Manager v2.3 and v2.4. Do not use PKS v1.3 with any other version of Ops Manager.

Tile Patch Releases Use Xenial Stemcells

Ubuntu 14.04 LTS (Trusty) stemcells are reaching end-of-support in April 2019. Starting in September 2018, Pivotal and its partners will begin releasing product tile versions for PCF that require Ubuntu 16.04 LTS (Xenial) stemcells instead of Trusty stemcells. Using Xenial stemcells is necessary to avoid exposure to security vulnerabilities. A PCF deployment may include some products running on Trusty stemcells and others running on Xenial.

Before deploying any tiles that require a Xenial stemcell, you must manually download and import a new Xenial stemcell into the **Ops Manager Stemcell Library**. As a consequence of using Xenial stemcells, any automation you have set up to update the existing tile using Trusty stemcells may break.

Before you upgrade PCF, always verify that any tiles that you have installed, either from Pivotal or a partner, are compatible with the version of PCF you are deploying and its supported stemcells. For more information on checking PCF and stemcell compatibility, see [Tile Compatibility](#) in the Upgrade Checklist.

To find out which stemcell version is used by a product tile version, check the release notes or the Pivotal Network download page for the tile.

Pivotal Application Service (PAS)

Downtime when Upgrading from v2.1 to v2.2.7 or Later

Upgrading directly from PAS v2.1.x to v2.2.7 or later may cause significant app downtime. If you are upgrading from v2.1.x, Pivotal recommends that you upgrade to v2.2.6 or an earlier patch release of v2.2.x. Once you are on v2.2.6 or an earlier patch release of v2.2.x, you can then upgrade to v2.2.7.

A fix for this issue is planned for v2.2.12.

For more information, see the following article in the Pivotal Knowledge Base: [How to avoid app downtime while upgrading from PAS v2.1.x to v2.2.7](#).

CredHub Database Cannot be External on GCP

Log Aggregation Systems May Parse Diego Timestamps Incorrectly

The timestamps in the Diego component logs are now in a format compatible with [RFC 3339](#).

This timestamp format is enabled by default for new PAS v2.2 deployments. Upgrades from earlier PAS versions retain the previous component log format with Unix epoch timestamps.

You can enable the new timestamp format in your PAS tile configuration. Before enabling the new timestamp format for Diego logs, ensure that your log aggregation system anticipates the timestamp format change.

If you experience issues, you can disable RFC 3339 format in the PAS tile. For more information about this PCF v2.2 feature, see [PCF v2.2 Feature Highlights](#) and [New Format for Timestamps in Diego Component Logs](#) in *Pivotal Application Service v2.2 Release Notes*.

SSH Proxy May Restrict Client Access

The SSH proxy now accepts a narrower range of ciphers, MACs, and key exchanges. This feature may have complications if you use a SSH client other than `cf ssh` to connect. For more information, see [Application SSH Access without cf CLI](#).

Temporary Downtime when Migrating Internal System Databases

If you use internal system databases, migrating the databases to the new option of **Internal Databases - MySQL - Percona XtraDB Cluster** causes temporary downtime of PAS system functions. Migrating the database does not interrupt apps running on PAS, but does temporarily prevent you from pushing new ones. For more information, see [Migrating to Internal Percona MySQL](#).

PAS v2.2 deprecates the MariaDB Galera internal database option, and Pivotal plans to remove MariaDB Galera as a database option in PAS v2.3. To continue using internal system databases in future versions of PAS, you need to migrate them to Percona while you are running PAS v2.2, or else when you upgrade to PAS v2.3.

This change has no effect if you have **External Databases** selected in the PAS tile **Databases** pane.

App Autoscaler Fails When Loggregator's Log Cache Is Disabled

App Autoscaler relies on API endpoints in Loggregator's Log Cache component. If you disable Log Cache, App Autoscaler will fail. For more information about Log Cache, see [Loggregator Introduces Log Cache](#).

Read-only Volume Mounts

We back-ported a fix from NFS 1.3.1 to NFS 1.2.1 for an incompatibility between our NFS Volume release and Diego's container runtime, garden. But, because the fix was in the NFS Service Broker, and service bindings created by old versions of this broker won't get migrated during upgrade, existing NFS service bindings that specify read-only mounts will still exhibit the incompatibility.

As a result, customers upgrading from versions containing `nfs-volume-release < 1.2.1` that have NFS services bound read-only to their applications will see that their applications crash after upgrade.

To fix this condition, customers should unbind the service, rebind it, and then restage the application.

Alternately, customers wishing to avoid application down time can temporarily re-bind their applications as read/write before upgrading, and then switch to read-only afterwards.

Diego Cell Garden Healthcheck Fails and Becomes Unhealthy

You may observe the following error in the Diego Cell Garden logs:

```
cfnetworking: cni up failed: add network list failed: initialize net out: creating chain: iptables call: running [/var/vcap/packages/iptables/sbin/iptables -t filter -N netout--executor-healthcheck --wait]: exit status 1: ip
```

This is a symptom of a failed Diego healthcheck, which can cause the Diego cell to become unhealthy. If you encounter this error, see the following Pivotal Knowledge Base article to understand and resolve the issue: [Diego Cell Garden healthcheck fails and becomes unhealthy](#).

PCF Operations Manager (Ops Manager)

Redeploy All Products After Upgrading to Ops Manager v2.2

When upgrading to PCF v2.2, redeploy all product tiles by clicking **Apply Changes** in the Ops Manager installation dashboard. A universal redeploy ensures that the updated BOSH DNS release applies consistently to all products.

Do not use the **Review Pending Changes** button to deploy product tiles individually during the upgrade to PCF v2.2. Instead, redeploy everything and selectively deploy individual product tiles only after you have successfully upgraded to PCF v2.2.

For more information about selective deployment, see [\(Beta\) Selectively Deploy Ops Manager Tiles](#).

Ops Manager Logs Have Changed Locations

Ops Manager centralized its logs in `/var/log/opsmanager` so that you can now configure a syslog server in the Ops Manager **Settings**.

Because of this change for Ops Manager v2.2, you cannot run scripts to fetch Ops Manager logs at their previous locations. For example, you cannot fetch logs from `/var/tempest` or `/var/vcap/sys`.

For more information about the syslog feature, see [Configure an Ops Manager Syslog Server](#) in the *PCF Ops Manager v2.2 Release Notes*.

Ops Manager API Does Not Return Secret Properties

For security, Ops Manager API responses from the `/api/v0/staged/director/properties` endpoint no longer include the following properties:

- GCS blobstore service key `service_account_key` (on Google Cloud Services)
- Health Monitor emailer SMTP password `smtp_password`
- Health Monitor PagerDuty service key `service_key`

This change may break any code that relies on retrieving these properties from a `GET /api/v0/staged/director/properties` call.

For more information, see the [Ops Manager API v2.2 documentation](#).

PCF Isolation Segment

Log Aggregation Systems May Parse Diego Timestamps Incorrectly

See [New Format for Timestamps in Diego Component Logs](#) in *PCF Isolation Segment v2.2 Release Notes* and breaking changes for [Pivotal Application Service \(PAS\)](#) for more information.

PCF Ops Manager v2.2 Release Notes

Pivotal Cloud Foundry is certified by the Cloud Foundry Foundation for 2019.

Read more about the [certified provider program](#) and the [requirements of providers](#).



Note: Ops Manager API documentation is now public. For more information, see [PCF v2.2 Feature Highlights](#).

How to Upgrade

The [Upgrading Pivotal Cloud Foundry](#) topic contains instructions for upgrading to Pivotal Cloud Foundry (PCF) Ops Manager v2.2.

Releases

2.2.24

Ops Manager v2.2.24 uses the following component versions:

| Component | Version |
|----------------|----------------|
| Ops Manager | 2.2-build.468* |
| Stemcell | 3586.118 |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.16.0 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |
| CredHub | 1.9.12 |
| Syslog | 11.4.0 |
| UAA | 57.10* |
| BPM | 0.12.3 |
| Networking | 8 |
| OS Conf | 20.0.0 |
| AWS CPI | 70 |
| Azure CPI | 35.5.2* |
| Google CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| Credhub CLI | 1.7.7 |
| BBR CLI | 1.5.1 |

** Components marked with an asterisk have been updated.*

2.2.23

- **[Bug Fix]** UAA session timeouts obey the access or refresh token lifetime.

Ops Manager v2.2.23 uses the following component versions:

| Component | Version |
|-------------|----------------|
| Ops Manager | 2.2-build.464* |
| Stemcell | 3586.118* |

| Component | Version |
|---|----------|
| BBR SDK | 1.6.0 |
| BOSH Director | 266.16.0 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |
| CredHub | 1.9.12 |
| Syslog | 11.4.0 |
| UAA | 57.9 |
| BPM | 0.12.3 |
| Networking | 8 |
| OS Conf | 20.0.0 |
| AWS CPI | 70 |
| Azure CPI | 35.4.0 |
| Google CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| Credhub CLI | 1.7.7 |
| BBR CLI | 1.5.1* |
| * Components marked with an asterisk have been updated. | |

2.2.22

- **[Bug Fix]: Apply Changes** no longer fails if copying credentials to CredHub takes longer than ten minutes.
- **[Bug Fix]:** Exporting installation settings no longer causes the BOSH Director to incorrectly show that it has staged changes.
- **[Bug Fix]:** Harbor now installs successfully on deployments that already have PKS installed. For more information about Harbor, see [VMware Harbor Registry](#).
- **[Bug Fix]:** Operators can no longer change persistent disk size to custom values.

Ops Manager v2.2.22 uses the following component versions:

| Component | Version |
|----------------|----------------|
| Ops Manager | 2.2-build.457* |
| Stemcell | 3586.100* |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.16.0 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |
| CredHub | 1.9.12* |
| Syslog | 11.4.0 |
| UAA | 57.9 |
| BPM | 0.12.3 |
| Networking | 8 |
| OS Conf | 20.0.0 |
| AWS CPI | 70 |
| Azure CPI | 35.4.0 |
| Google CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| Credhub CLI | 1.7.7 |
| BBR CLI | 1.5.1* |

| BBR CLI Component | 1.5.0 Version |
|---|------------------|
| * Components marked with an asterisk have been updated. | |

2.2.21

- **[Bug Fix]:** You can now configure Azure deployments to use Availability Zones after upgrading from an earlier version.
- **[UI Improvement]:** The notification banner that appears when a certificate in your deployment is about to expire is updated for clarity.

Ops Manager v2.2.21 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.436* |
| Stemcell | 3586.93* |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.16.0 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |
| CredHub | 1.9.11* |
| Syslog | 11.4.0 |
| UAA | 57.9 |
| BPM | 0.12.3 |
| Networking | 8 |
| OS Conf | 20.0.0 |
| AWS CPI | 70 |
| Azure CPI | 35.4.0 |
| Google CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| Credhub CLI | 1.7.7 |
| BBR CLI | 1.5.0* |
| * Components marked with an asterisk have been updated. | |

2.2.20

- There are no additional features or fixes in this release.

Ops Manager v2.2.20 uses the following component versions:

| Component | Version |
|----------------|---------------|
| Ops Manager | 2.2-build.427 |
| Stemcell | 3586.86 |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.16.0 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |
| CredHub | 1.9.9 |
| Syslog | 11.4.0 |
| UAA | 57.9 |
| BPM | 0.12.3 |
| Networking | 8 |
| OS Conf | 20.0.0 |

| Component | Version |
|--|------------------|
| AWS CPI | 70 |
| Azure CPI | 35.4.0 |
| Google CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| Credhub CLI | 1.7.7 |
| BBR CLI | 1.4.0 |
| <i>Components marked with an asterisk have been updated.</i> | |

2.2.19

- **[Security Fix]:** Updates bootstrap from 3.4.0 to 3.4.1.

Ops Manager v2.2.19 uses the following component versions:

| Component | Version |
|--|----------------|
| Ops Manager | 2.2-build.424* |
| Stemcell | 3586.79 |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.16.0 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |
| CredHub | 1.9.9 |
| Syslog | 11.4.0 |
| UAA | 57.7 |
| BPM | 0.12.3 |
| Networking | 8 |
| OS Conf | 20.0.0 |
| AWS CPI | 70 |
| Azure CPI | 35.4.0 |
| Google CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| Credhub CLI | 1.7.7 |
| BBR CLI | 1.4.0* |
| <i>* Components marked with an asterisk are updated.</i> | |

2.2.18

- There are no additional features or fixes in this release.

Ops Manager v2.2.18 uses the following component versions:

| Component | Version |
|----------------|----------------|
| Ops Manager | 2.2-build.418* |
| Stemcell | 3586.79* |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.16* |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |

| Component | Version |
|--|---------|
| Syslog | 11.4 |
| UAA | 57.7 |
| AWS CPI | 70 |
| Azure CPI | 35.4 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| <i>* Components marked with an asterisk are updated.</i> | |

2.2.17

- **[New Feature]:** You can now upgrade from the most recent version of v2.2, which may use multiple NATS certificate authorities (CAs) to a version of v2.3 that only supports one NATS CA and was released prior to the version of v2.2 from which you are upgrading.
- **[New Feature]:** You can now change a selected option of a selector through the API using the human-readable name of the option. Send a `PUT` to `/api/v0/staged/products/:guid/properties` with a `selected_option` key. The `PUT` API endpoint can also parse both `value`, for the human-readable value, and `option_value`, for the machine-readable value.
- **[Bug Fix]:** When an Azure-based Ops Manager Director is configured with invalid Azure account credentials (such as a subscription ID, tenant, or other credentials) and you try to create a network, you now an error message, rather than a 500 error.
- **[Bug Fix]:** Ops Manager now uses GCP images that are located in the United States. This should prevent image object generation problems sometimes seen in images based in Europe and Asia.
- **[Bug Fix]:** The Azure CPI is reverted to 35.4 to resolve a customer issue.

Ops Manager v2.2.17 uses the following component versions:

| Component | Version |
|--|----------------|
| Ops Manager | 2.2-build.414* |
| Stemcell | 3586.70 |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.15 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22 |
| CredHub | 1.9.3 |
| Syslog | 11.4 |
| UAA | 57.7 |
| AWS CPI | 70 |
| Azure CPI | 35.4* |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| <i>* Components marked with an asterisk are updated.</i> | |

2.2.16

- **[Security Fix]:** A potential XSS vulnerability in the `resource_config` API endpoint is mitigated.
- **[New Feature]:** NATS certificate information, including expiration dates, is now available through the API. Use the `api/v0/deployed/certificates` endpoint to view this information.
- **[New Feature]:** You can now use the BOSH Backup and Restore (BBR) CLI from the Ops Manager VM. This means you no longer have to download or upgrade BBR when you upgrade the Ops Manager VM.
- **[Bug Fix]:** Ops Manager now reloads NGINX when the configuration is updated. Previously, Ops Manager would restart NGINX, which could cause temporary downtime. NGINX now serves traffic consistently when it is updating.

Ops Manager v2.2.16 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.406* |
| Stemcell | 3586.70* |
| BBR SDK | 1.6.0 |
| BOSH Director | 266.15* |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.22* |
| CredHub | 1.9.3 |
| Syslog | 11.4* |
| UAA | 57.7* |
| AWS CPI | 70 |
| Azure CPI | 35.5 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| * Components marked with an asterisk are updated. | |

2.2.15

- **[Security Fix]:** Information about the web server (NGINX) no longer appears in server response headers.
- **[New Feature]:** Credentials now return in some API calls. If you have sufficient permissions, sending a GET to `director/properties` or `director/iaas_configurations/guid` or `products/guid/properties` with the `redact=false` parameter will return all keys and values, including credentials.
- **[Feature Improvement]:** Selectors without a default option display in the list of `/api/v0/staged/products/product-guid/properties` as `null`.
- **[Feature Improvement]:** Some error messages that appear in the API are more reader-friendly.
- **[Bug Fix]:** You can no longer export using the API without deploying.
- **[Bug Fix]:** `/api/v0/deployed/director/manifest` now works when upgrading from 2.1 to 2.2.
- **[Bug Fix]:** Installation Change records now have a deployment status other than `null`.

Ops Manager v2.2.15 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.398* |
| Stemcell | 3586.66* |
| BBR SDK | 1.6 |
| BOSH Director | 266.14 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.6 |
| AWS CPI | 70 |
| Azure CPI | 35.5 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| * Components marked with an asterisk are updated. | |

2.2.14

- **[Bug Fix]:** Viewing product properties API endpoint for selector properties no longer fails when no option is selected, it returns null for that field.
- **[Security Fix]:** GETs to any Ops Manager or UAA API endpoint no longer return any information about the web server, including version numbers.

Ops Manager v2.2.14 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.386* |
| Stemcell | 3586.60 |
| BBR SDK | 1.6 |
| BOSH Director | 266.14 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.6 |
| AWS CPI | 70 |
| Azure CPI | 35.5* |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.4 |
| * Components marked with an asterisk are updated. | |

2.2.13

- **[New Feature]:** A banner appears on the Dashboard when certificates are about to expire.
- **[New Feature]:** The Ops Manager API has a selected option identifier for a selector property. For example, `properties.SELECTOR_NAME.SELECTOR_OPTION.OPTION-NAME`. This helps identify what properties are associated with the selected option on a selector.
- **[New Feature]:** Ops Manager operators with permissions to see credentials can send a `GET` to `director/properties`, `director/iaas_configurations/guid`, `director/iaas_configurations`, or `products/guid/properties` with the `redact=false` parameter to see an API response that includes credentials.
- **[Bug Fix]:** The API docs corrected `PUT /api/v0/settings/ssl_certificate` details.

Ops Manager v2.2.13 uses the following component versions:

| Component | Version |
|----------------|----------------|
| Ops Manager | 2.2-build.382* |
| Stemcell | 3586.60* |
| BBR SDK | 1.6 |
| BOSH Director | 266.14 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.6 |
| AWS CPI | 70 |
| Azure CPI | 35.4 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| | |

| Component | Version |
|---|---------|
| * Components marked with an asterisk are updated. | |

2.2.12

- **[Security Fix]:** Bumps activejob to 5.0.4 to resolve [CVE-2018-16476](#).
- **[New Feature]:** Ops Manager operators with sufficient permissions to see credentials can now send a GET to `director/properties`, `director/iaas_configurations/guid`, `director/iaas_configurations`, or `products/guid/properties` with the `redact=false` parameter to see an API response that includes credentials.
- **[Feature Improvement]:** When a user who has not logged into Ops Manager is prompted to log in to view a page, logging in returns them to the page they tried to access, rather than the Installation Dashboard.
- **[Bug Fix]:** Internal IDP metadata no longer changes when authentication protocols switch between internal authentication and SAML. Specifically, the `ds:DigestValue` and `ds:SignatureValue` values no longer change.
- **[Bug Fix]:** The API docs now show `instance_groups` in some locations where they previously referenced jobs.

Ops Manager v2.2.12 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.379* |
| Stemcell | 3586.57 |
| BBR SDK | 1.6 |
| BOSH Director | 266.14 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.6 |
| AWS CPI | 70 |
| Azure CPI | 35.4 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50.0.3* |
| * Components marked with an asterisk are updated. | |

2.2.11

- **[Bug Fix]:** The SAML certificate now regenerates when authentication method changes from SAML to internal, rather than when SAML is enabled. This facilitates a greater number of authentication method workflows, including those which change Ops Manager metadata.
- **[Bug Fix]:** Ops Manager now captures changes to the database, including reversions to old passwords, more completely.
- **[Feature Improvement]:** There are now API docs for the GET and PUT `ssh_banner_contents` endpoints.

Ops Manager v2.2.11 uses the following component versions:

| Component | Version |
|----------------|----------------|
| Ops Manager | 2.2-build.376* |
| Stemcell | 3586.57 |
| BBR SDK | 1.6 |
| BOSH Director | 266.14 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |

| Component | Version |
|--|---------|
| AWS CPI | 70 |
| Azure CPI | 35.4 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| <i>* Components marked with an asterisk are updated.</i> | |

2.2.10

- **[Security Fix]:** Upgrades Loofah to 2.2.3 to address a CVE.
- **[Security Fix]:** Upgrades Rack to 2.0.6 to address a CVE.
- **[New Feature]:** A Pivotal-specific GUID now appears in the global CPI options for Azure deployments. View this key/value pair in the CPI configuration of the BOSH Director manifest.

Ops Manager v2.2.10 uses the following component versions:

| Component | Version |
|--|----------------|
| Ops Manager | 2.2-build.372* |
| Stemcell | 3586.57* |
| BBR SDK | 1.6 |
| BOSH Director | 266.14* |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.6 |
| AWS CPI | 70 |
| Azure CPI | 35.4 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| <i>* Components marked with an asterisk are updated.</i> | |

2.2.9

- **[Security Fix]:** Bumps Nokogiri to 1.8.5 to address [CVE-2018-14404](#).
- **[Security Fix]:** Bumps UAA to 57.6 to address [CVE-2018-15761](#).
- **[Bug Fix]:** Now Application Load Balancers (ALBs) also apply to the Director VM for AWS deployments.

Ops Manager v2.2.9 uses the following component versions:

| Component | Version |
|----------------|----------------|
| Ops Manager | 2.2-build.359* |
| Stemcell | 3586.52* |
| BBR SDK | 1.6 |
| BOSH Director | 266.13 |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| | |

| Syslog Component | Version |
|---|---------|
| UAA | 57.6* |
| AWS CPI | 70 |
| Azure CPI | 35.4 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.8

- **[Security Fix]:** Bumps stemcell to 3586.48 to address [USN-3777-2](#).
- **[New Feature]:** Operators can tune the swap size as a percent of total memory size per instance group.
- **[Bug Fix]:** Bumps Azure CPI up to 35.4 to fix `LockTimeoutError` issues.
- **[Bug Fix]:** Operators can change the Director Hostname without losing connection between BOSH Director and VMs.
- **[Bug Fix]:** Stemcells no longer accidentally downgrade when upgrading to a new Ops Manager. This rare bug occurred when a product had a newer stemcell patch than Ops Manager included during the upgrade.
- **[Bug Fix]:** Operators can work around an expired SAML service provider cert by disabling and enabling SAML.
- **[Feature Improvement]:** The expiring certificates endpoint (`/api/v0/deployed/certificates`) now includes information about the SAML service provider cert.
- **[Feature Improvement]:** When you import products that use the future Unified Syslog feature, you are warned that some syslog features will not be active in this version of Ops Manager.
- **[Bug Fix]:** Dynamic JS pages now show the message from server-side errors instead of alert boxes with JavaScript errors (such as `[Object object]` or `t.filter()`).
- **[New Feature]:** You can now configure custom DNS handlers using the Ops Manager API.
- **[New Feature]:** You can now configure recursor timeouts using the Ops Manager API.

Ops Manager v2.2.8 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.339* |
| Stemcell | 3586.48* |
| BBR SDK | 1.6 |
| BOSH Director | 266.13* |
| BOSH DNS | 1.10.0 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4 |
| AWS CPI | 70 |
| Azure CPI | 35.4 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.7

- **[Bug Fix]:** You are now only prompted to unlock Ops Manager once when enabling [Rescue Mode](#).
- **[Bug Fix]:** Ops Manager sets the storage account type and Director ephemeral disk correctly for Azure deployments.

Ops Manager v2.2.7 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.334* |
| Stemcell | 3586.43* |
| BBR SDK | 1.6 |
| BOSH Director | 266.12 |
| BOSH DNS | 1.10.0* |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4 |
| AWS CPI | 70 |
| Azure CPI | 35.4* |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.6

- **[Feature]:** Operators can rotate BOSH DNS healthiness certificates to a new certificate authority (CA) that is valid for four years.
- **[UI Enhancement]:** An error message appears when Ops Manager fails to import an installation.
- **[UI Enhancement]:** An error message appears when a file downloaded from Pivotal Network is invalid or corrupt.

Ops Manager v2.2.6 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.319* |
| Stemcell | 3586.40 |
| BBR SDK | 1.6 |
| BOSH Director | 266.12* |
| BOSH DNS | 1.8 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4 |
| AWS CPI | 70 |
| Azure CPI | 35.2 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.5

- **[Feature]:** New CAs for BOSH DNS healthiness and DNS API apply automatically on upgrade. These CAs are valid for four years.
- **[Feature]:** All DNS healthiness certificates are signed by a Credhub CA.
- **[Feature]:** Operators can rotate DNS healthiness certificates using `POST/api/v0/certificate_authorities/active/regenerate`.
- **[Feature Improvement]:** Ops Manager API warns you when you attempt to regenerate certificates without first applying changes to propagate CA

changes.

- **[Bug Fix]:** Verifiers work in vCenter v6.7. Fixes the [Ops Manager “Required Datacenter privileges” Error on vSphere](#) known issue.

Ops Manager v2.2.5 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.316* |
| Stemcell | 3586.40 |
| BBR SDK | 1.6 |
| BOSH Director | 266.10 |
| BOSH DNS | 1.8 |
| Metrics Server | 0.0.21 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4 |
| AWS CPI | 70 |
| Azure CPI | 35.2 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.4

- **[Security Fix]:** Bumps stemcell to 3586.40.
- **[Bug Fix]:** Pivotal Network integrates successfully with Pivotal Application Service (PAS) tile and Small Footprint PAS.
- **[Feature Improvement]:** You can use the Ops Manager API to delete individual OpenStack or vCenter Configs. For more information, see [Deleting IaaS Configuration](#) [↗](#) in the Ops Manager API documentation.
- **[Bug Fix]:** You cannot import an installation with no deployed products.

Ops Manager v2.2.4 uses the following component versions:

| Component | Version |
|---|---------------|
| Ops Manager | 2.2-build.312 |
| Stemcell | 3586.40* |
| BBR SDK | 1.6 |
| BOSH Director | 266.10 |
| BOSH DNS | 1.8 |
| Metrics Server | 0.0.21* |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4 |
| AWS CPI | 70 |
| Azure CPI | 35.2 |
| GCP CPI | 27.0.1 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.3

- **[Security Fix]:** Bumps stemcell to 3586.36

Ops Manager v2.2.3 uses the following component versions:

| Component | Version |
|---|---------------|
| Ops Manager | 2.2-build.304 |
| Stemcell | 3586.36* |
| BBR SDK | 1.6 |
| BOSH Director | 266.10* |
| BOSH DNS | 1.8* |
| Metrics Server | 0.0.17 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4 |
| AWS CPI | 70 |
| Azure CPI | 35.2 |
| GCP CPI | 27.0.1* |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.2

- **[Bug Fix]:** Fixes Xenial stemcell upload issue. This resolves [Error When Importing Xenial Stemcell](#).

Ops Manager v2.2.2 uses the following component versions:

| Component | Version |
|---|----------------|
| Ops Manager | 2.2-build.300* |
| Stemcell | 3586.27* |
| BBR SDK | 1.6 |
| BOSH Director | 266.8.0* |
| BOSH DNS | 1.6 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4 |
| AWS CPI | 70 |
| Azure CPI | 35.2 |
| GCP CPI | 27 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.1

- **[Bug Fix]:** Fixes critical manifest generation grammar issue.
- **[Bug Fix]:** You can now delete an unused AZ in an installation after clicking **Apply Changes**.
- **[Bug Fix]:** Certain VM image components no longer write to the persistent disk after reboot.
- **[Bug Fix]:** Ops Manager now verifies certificates successfully when connecting to S3 blobstores with TLS. This resolves a [known issue](#) in Ops Manager

v2.2.0. For more information, see [Operations Manager Validation returns TLS error when configuring Bosh Director S3 blobstore](#).

- **[Security Fix]:** Bumps Nokogiri to 1.8.4 to remediate [CVE-2017-15412](#).
- **[Feature Improvement]:** Installation Dashboard and deployment status pages may load more quickly.

Ops Manager v2.2.1 uses the following component versions:

| Component | Version |
|---|---------------|
| Ops Manager | 2.2-build.296 |
| Stemcell | 3586.25* |
| BBR SDK | 1.6 |
| BOSH Director | 266.6* |
| BOSH DNS | 1.6 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.4* |
| AWS CPI | 70 |
| Azure CPI | 35.2 |
| GCP CPI | 27 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |
| * Components marked with an asterisk are updated. | |

2.2.0

Ops Manager v2.2.0 uses the following component versions:

| Component | Version |
|---------------|---------|
| Stemcell | 3586.24 |
| BBR SDK | 1.6 |
| BOSH Director | 266.5 |
| BOSH DNS | 1.6 |
| CredHub | 1.9.3 |
| Syslog | 11.3 |
| UAA | 57.3 |
| AWS CPI | 70 |
| Azure CPI | 35.2 |
| GCP CPI | 27 |
| OpenStack CPI | 38 |
| vSphere CPI | 50 |

New Features in Ops Manager v2.2

Ops Manager v2.2 includes the following major features:

Multiple Data Centers on vSphere

Ops Manager now allows you to configure multiple vSphere vCenters to a single BOSH Director.

You can add additional data centers in the **vSphere Config** pane of your vSphere BOSH Director tile. For more information about how to add, edit, and delete vCenters, see [Managing Multiple vSphere vCenters](#).

Note: If you use the Ops Manager API and multiple vSphere configs exist, the GET HTTP request for Director properties omits the `iaas_configuration` key.

Selectively Deploy Tiles in Ops Manager or by an API Endpoint

You can now choose to deploy a selection of tiles rather than all tiles in Ops Manager. If you choose to selectively deploy your environment, you can drastically reduce the time to **Apply Changes**. This feature is ideal to limit updates to one or more tiles, which reduces the amount of change in any given deployment.

To access this feature, click **Review Pending Changes** underneath the **Apply Changes** button in the Ops Manager Installation Dashboard. For more information, see [Reviewing Pending Changes with Ops Manager](#).

In the Ops Manager UI, this feature is in beta. It is generally available as an API endpoint. To selectively deploy tiles using the API, send a POST to `/api/v0/installations`. For more information, see [Triggering an install process](#) in the Ops Manager API documentation.

Warning: Do not selectively deploy tiles when upgrading to PCF v2.2. Instead, redeploy all product tiles using **Apply Changes** on the Ops Manager Installation Dashboard. For more information, see [Redeploy All Products After Upgrading to Ops Manager v2.2](#).

Note: Ops Manager is soliciting feedback for this feature. Submit feedback through your product architect or directly by emailing opsmanager-feedback+selective_deploys@pivotal.io.

Ops Manager Stores Past Manifests

Through the Ops Manager API, you can see Ops Manager's manifest history. Manifest history is helpful for running `diff` commands on manifests to see changes over time.

For this feature, use the following Ops Manager API endpoints:

- `/api/v0/installations/:installation_id/products/:product_guid/manifest`: For more information, see [Getting BOSH manifests from historical installations](#) from the Ops Manager API documentation.
- `/api/v0/installations`: For more information, see [Getting a list of recent install events](#) from the Ops Manager API documentation.

Azure Stack is Generally Available

Pivotal officially supports Azure Stack.

Azure Stack is a hybrid cloud platform that lets you deliver Azure services from your own on-premise datacenter. For more information about Azure Stack, see [What is Azure Stack?](#) from the Microsoft Azure documentation.

You can configure Azure Stack through the **BOSH Director for Azure** tile. For more information about Azure Stack-specific configurations, see the steps in the [Azure Config Page](#) section of the *Configuring BOSH Director on Azure* topic.

Ops Manager Supports Azure China

Ops Manager now supports a special region in Azure called Azure China. Azure China is a physically separated instance of cloud services that is located in China and independently operated. For more information about Azure China, see [What is Azure China 21Vianet?](#) in the Azure China documentation.

To tell the BOSH Director that you are using an Azure China environment, go to the **BOSH Director for Azure** tile and select `Azure China Cloud` from the **Azure Environment** field. For more information, see [Azure Config Page](#) in the *Configuring Ops Manager on Azure* manual installation topic.

Ops Manager Credentials Stored in CredHub

On each **Apply Changes**, Ops Manager sends your user-specified credentials to BOSH CredHub. This feature offers greater security for your credentials. For more information about where Ops Manager stores your credentials, see [BOSH CredHub](#).

For information about how this feature affects tile authors, see [PCF v2.2 Partners Release Notice](#) in the *PCF Tile Developer Guide*.

Multi-Line Credentials

Ops Manager v2.2 now supports text areas for any type of multi-line credential. If you want a `secret` property to use a text area instead of the default single-line text field, you must set `display_type` to `text_area` in the `property_inputs` section of your property blueprint, as in the example below.

```
property_inputs:
- reference: secret_meaning
  label: 'Secret Meaning'
  description: 'If you play it backwards...!'
  display_type: 'text_area'
```


For more information, see the [Custom Forms and Properties](#) section of the *Tile Generator* topic.

Specify a Custom Trusted SSL Certificate

Operators can specify a custom trusted SSL certificate and key for the Ops Manager server so that traffic isn't exposed to man-in-the-middle attacks when using Ops Manager.

By default, Ops Manager uses an auto-generated self-signed certificate. To change this configuration to your own SSL certificate, navigate to **Settings** from the Ops Manager Installation Dashboard and select the **SSL Certificate** pane to enter your **Certificate** and **Private Key**.

For more information about navigating the Ops Manager Settings page, see [Settings Page](#) in the *Understanding the Ops Manager Interface* topic.

 **Note:** Custom SSL certificate and key is persisted between upgrades. Custom SSL only needs a one-time configuration.

Delete Your Pivotal Network API Token

You can now delete your Pivotal Network API token, along with the Pivotal Network release dashboard and all of the tile metadata from Pivotal Network products.


For more information, see [Settings Page](#) in the *Understanding the Ops Manager Interface* topic.

Configure an Ops Manager Syslog Server

You can configure a syslog server for Ops Manager logs. Logs include rails production logs, audit logs, UAA logs, nginx logs, and upstart logs for Ops Manager processes as well as additional log types. Previous to this change, Ops Manager logs were not centralized in one accessible location. You also have the option to TLS-encrypt your logs.

To configure syslog for Ops Manager, go to **Syslog** from Ops Manager **Settings**, select **Yes** to enable syslog and fill the required fields. Only administrators can view the Syslog pane.

For more information about configuring syslog for Ops Manager, see [Settings Page](#) in the *Understanding the Ops Manager Interface* topic.

 **Note:** When you enter your syslog credentials, Ops Manager does not validate them. You should test your syslog server to ensure that the credentials were entered correctly and the server is receiving Ops Manager logs.

 **Breaking Change:** If you were running scripts to get Ops Manager logs, those scripts break on upgrade to Ops Manager v2.2 and later.

Xenial Stemcell Upgrade Support

As of April 2019, Trusty stemcells will no longer receive support, nor will Pivotal have CVE patches for them. Ops Manager v2.2 allows tile authors to upgrade from Trusty stemcells to Xenial stemcells.

TLS for Internal Blobstore Supported


Ops Manager now supports TLS communications if you choose to use an internal blobstore.

To enable internal blobstore TLS communication, all of your tiles must have stemcell v3586 or later. You can configure internal TLS by clicking **Enable TLS** in the **Director Config** pane of the BOSH Director tile.

Custom TLS Certificate for External MySQL Database Supported

Ops Manager now allows you to configure a custom TLS certificate for an external MySQL database.

To configure a custom TLS certificate, navigate to **Director Config > Database Location** and select **External MySQL Database** to fill in the relevant fields.

 **Note:** You must select **Enable TLS for Director Database** to configure the TLS-related fields.

For more information, see the **Director Config Page** section of the [Ops Manager Director installation topic for your IaaS](#).

UI Improvements to Installation Dashboard

The following lists UI changes to the Ops Manager Installation Dashboard:

- **Stemcell Library** is persistently in the page header. You can now access Stemcell Library from anywhere in Ops Manager.
- **Changelog** is persistently in the page header. You can now access the changelog from anywhere in Ops Manager.
- **Review Pending Changes BETA** button is below **Apply Changes**. For more information about this feature, see [Selectively Deploy Ops Manager Tiles](#).
- **Azure Logo** is updated.
- **BOSH Director tile name** is changed to “BOSH Director for YOUR_IaaS”.
- **Changelog** page shows tiles which were not changed but were still deployed.

For more information about the Ops Manager UI, see [Installation Dashboard Page](#) in the *Understanding the Ops Manager Interface* topic.

Change Log Includes Products Deployed but Unchanged

The [Change Log](#) pane lists products as **Unchanged** when they remain deployed, but their configuration has not changed from a prior deployment, so Ops Manager did not re-deploy them.

More Detail Available By Ops Manager API Endpoint

A new API endpoint is available for Ops Manager. Send a `GET` to `/v0/staged/pending_changes` to see details about your Ops Manager installation, including tile names, errand names, build version, and deployment status. The API response will show information on all tiles, whether they are deployed or have pending changes.

For more information about setting up the Ops Manager API, see [Using the Ops Manager API](#).

Custom Identification Tags Supported


You can specify a single set of tags that apply to all VMs and disks for your foundation. Identification tags allow you to easily identify which foundation your VMs belong to when viewing your IaaS. You are able to set custom **Identification Tags** in the **Director Config** pane of your BOSH Director tile.

For more information about configuring identification tags, see the **Director Config Page** section of the [Ops Manager Director installation topic for your IaaS](#).


BOSH DNS Enabled By Default

BOSH DNS is enabled by default for both app containers and PCF components in PCF v2.2.

In previous versions, Consul managed service discovery between PCF components, but Consul is being replaced by BOSH DNS.

 **Note:** In PCF v2.2, Consul and BOSH DNS are both available in PCF, but BOSH DNS is the only service used for DNS requests.


You can disable BOSH DNS if instructed to do so by Pivotal support. If you disabled BOSH DNS in PCF v2.1, reenable it before upgrading to PCF v2.2. For more information, see [BOSH DNS Enabled By Default](#).

 **warning:** Do not disable BOSH DNS without instructions from Pivotal support. Disabling BOSH DNS will also disable PKS, NSX-T, and several PAS features.

“When Changed” Errand Setting Removed

Ops Manager no longer includes a **When Changed** option for tile errands. In the **Errands** pane for a given tile, you can set errands **On** to run them or **Off** to not run them. The default setting is **On**.

Known Issues

 **warning:** Ops Manager v2.2 is not supported by PKS starting in PKS v1.3. Use a later version of Ops Manager if you wish you use PKS v1.3.

DNS Server Hangs or DNS Lookups Fail

With BOSH DNS, every BOSH-deployed VM has a DNS server. In large PCF installations, this DNS server may hang or DNS lookups may fail when the VM experiences too many DNS lookups in a short amount of time.

This error is caused by a race condition and deadlock in the VM's DNS server.

To fix this problem, run `monit` on the VM with failing DNS to restart its `bosh-dns` process.

Error When Importing Xenial Stemcell

Ops Manager v2.2.0 and later support Xenial stemcells. However, the Ops Manager UI returns an error when you attempt to import a Xenial stemcell.

As a workaround, you can upload the stemcell and assign it to a product using the [Ops Manager API](#).

This issue is fixed in Ops Manager v2.2.2.

Ops Manager Validation Returns TLS Error When Configuring BOSH Director S3 Blobstore

If a remote S3 blobstore uses a privately signed SSL certificate, operators see an error when configuring the BOSH Director to use an S3 blobstore.

The error reads:

```
SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed (OpenSSL::SSL::SSLError) Unable to verify certificate. This may be an issue with the remote host or with Excon. Excon has certificates bundled, but these can be customized:
```

This error appears because Ops Manager attempts to validate the S3 blobstore by testing the SSL certificate. Ops Manager does not use trusted certificates to make this connection, so the connection fails.

A workaround is available for this issue. Operators can install the public CA certificate directly into the OS config of Ops Manager by following these steps:

1. SSH into the Ops Manager VM.
2. Copy the public CA certificate into `/etc/ssl/certs`.
3. Run `sudo update-ca-certificates -f -v`. This installs the new CA certificate.

Upon successful execution, “1 added” displays in the output. For example:

```
Updating certificates in /etc/ssl/certs... 1 added, 0 removed;
done.
```

This indicates the new certificate is installed.

For more information, see the Knowledge Base article [Operations Manager Validation Returns TLS Error When Configuring BOSH Director S3 Blobstore](#).

Ops Manager Deployment Fails Because Monit Reports Job as Failed

This issue causes Ops Manager deployments to fail with an error indicating one or more jobs are not running after an update.

The error reads:

```
Error: 'cloud_controller/6632bf71-7493-4383-a3f9-9401bafb4710 (1)' is not running after update. Review logs for failed jobs:
cloud_controller_ng
```

Additionally, when you SSH into a VM and run `monit summary`, monit reports jobs as “Execution Failed”.

To remediate this issue, use monit to restart the affected processes.

For more information, see the Knowledge Base article [Deployment Fails Because Monit Reports Job as Failed](#).

Ops Manager “Required Datacenter privileges” Error on vSphere

Ops Manager on vSphere v6.7 fails with an error message: “Could not log in: Required Datacenter privileges could not be verified: SystemError: A general system error occurred: Authorize Exception”

You can ignore this error message. Click “Ignore errors and start the install” to authenticate.

This issue is fixed in Ops Manager v2.2.5 and v2.3.0 or later.

Pivotal Application Service v2.2 Release Notes

Pivotal Cloud Foundry is certified by the Cloud Foundry Foundation for 2019.

Read more about the [certified provider program](#) and the [requirements of providers](#).

Releases

2.2.16

- **[Security Fix]** Fix insecure gradle dependency in CredHub
- **[Bug Fix]** Allow persistent disk size on backup and restore to be configured
- Bump ubuntu-trusty-stemcell to version `3586.100`
- Bump cflinuxfs2 to version `1.283.0`
- Bump credhub to version `1.9.12`

| Component | Version |
|-----------------------------------|----------|
| ubuntu-trusty-stemcell | 3586.100 |
| backup-and-restore-sdk | 1.12.0 |
| binary-offline-buildpack-lts | 1.0.30 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.16 |
| cf-autoscaling | 201.11 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.16.0 |
| cf-networking | 2.3.3 |
| cf-smoke-tests | 40.0.40 |
| cf-syslog-drain | 6.8 |
| cflinuxfs2 | 1.283.0 |
| consul | 195 |
| credhub | 1.9.12 |
| diego | 2.8.7 |
| dotnet-core-offline-buildpack-lts | 2.2.5 |
| garden-runc | 1.16.8 |
| go-offline-buildpack-lts | 1.8.33 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |
| loggregator | 102.8 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.6 |
| nodejs-offline-buildpack-lts | 1.6.43 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.70 |

| Component | Version |
|----------------------------------|----------|
| push-apps-manager-release | 665.0.32 |
| push-usage-service-release | 666.0.12 |
| pxc | 0.14.1 |
| python-offline-buildpack-lts | 1.6.28 |
| routing | 0.178.7 |
| ruby-offline-buildpack-lts | 1.7.31 |
| silk | 2.3.4 |
| staticfile-offline-buildpack-lts | 1.4.39 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.13 |

2.2.15

- **[Feature Improvement]** Reduce load on autoscaling database by adding indices to improve query efficiency
- **[Bug Fix]** Increase TLS Certificate verification depth in Apps Manager to allow for longer certificate chains
- **[Bug Fix]** Apps Manager correctly displays footer text when not set in Ops Manager
- Bump ubuntu-trusty stemcell to version 3586.96
- Bump capi to version 1.58.16
- Bump cf-autoscaling to version 201.11
- Bump cflinuxfs2 to version 1.280.0
- Bump push-apps-manager-release to version 665.0.32

| Component | Version |
|-----------------------------------|---------|
| ubuntu-trusty stemcell | 3586.96 |
| backup-and-restore-sdk | 1.12.0 |
| binary-offline-buildpack-lts | 1.0.30 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.16 |
| cf-autoscaling | 201.11 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.16.0 |
| cf-networking | 2.3.3 |
| cf-smoke-tests | 40.0.40 |
| cf-syslog-drain | 6.8 |
| cflinuxfs2 | 1.280.0 |
| consul | 195 |
| credhub | 1.9.9 |
| diego | 2.8.7 |
| dotnet-core-offline-buildpack-lts | 2.2.5 |
| garden-runc | 1.16.8 |
| go-offline-buildpack-lts | 1.8.33 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |

| Component | Version |
|----------------------------------|----------|
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.6 |
| nodejs-offline-buildpack-lts | 1.6.43 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.70 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.32 |
| push-usage-service-release | 666.0.12 |
| pxc | 0.14.1 |
| python-offline-buildpack-lts | 1.6.28 |
| routing | 0.178.7 |
| ruby-offline-buildpack-lts | 1.7.31 |
| silk | 2.3.4 |
| staticfile-offline-buildpack-lts | 1.4.39 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.13 |

2.2.14

- **[Security Fix]** Bump UAA to address CVE-2019-3775
- **[Feature Improvement]** Improve error messages when installing buildpacks
- **[Feature Improvement]** Increase performance for internal MySQL by setting the setting for `innodb_flush_log_at_trx_commit` from 1 to 2. This increases performance safely for clustered deployments. Single node might need to scale up to avoid the possibility of 1 second of data loss during deploys.
- **[Feature Improvement]** Add support for tcp hitless reloads in haproxy to avoid connection reset errors
- **[Feature Improvement]** Add ability to enable/disable gorouter hairpinning with **Bypass security checks for route service lookup**. This feature has potential security concerns, but may be needed for backwards compatibility. See [Configuring Route Service Lookup](#).
- **[Bug Fix]** Fix issue in which Apps Manager shows `Invalid User` as the username for space and organization members without usernames, such as UAA clients
- Bump ubuntu-trusty stemcell to version `3586.93`
- Bump capi to version `1.58.15`
- Bump cf-autoscaling to version `201.10`
- Bump cf-syslog-drain to version `6.8`
- Bump cflinuxfs2 to version `1.279.0`
- Bump push-apps-manager-release to version `665.0.30`
- Bump routing to version `0.178.7`
- Bump uaa to version `60.13`

| Component | Version |
|-------------------------------|---------|
| ubuntu-trusty stemcell | 3586.93 |
| backup-and-restore-sdk | 1.12.0 |
| binary-offline-buildpack-lts | 1.0.30 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.15 |
| cf-autoscaling | 201.10 |

| Component | Version |
|-----------------------------------|----------|
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.16.0 |
| cf-networking | 2.3.3 |
| cf-smoke-tests | 40.0.40 |
| cf-syslog-drain | 6.8 |
| cflinuxfs2 | 1.279.0 |
| consul | 195 |
| credhub | 1.9.9 |
| diego | 2.8.7 |
| dotnet-core-offline-buildpack-lts | 2.2.5 |
| garden-runc | 1.16.8 |
| go-offline-buildpack-lts | 1.8.33 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |
| loggregator | 102.8 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.6 |
| nodejs-offline-buildpack-lts | 1.6.43 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.70 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.30 |
| push-usage-service-release | 666.0.12 |
| pxc | 0.14.1 |
| python-offline-buildpack-lts | 1.6.28 |
| routing | 0.178.7 |
| ruby-offline-buildpack-lts | 1.7.31 |
| silk | 2.3.4 |
| staticfile-offline-buildpack-lts | 1.4.39 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.13 |

2.2.13

- **[Feature Improvement]** Operators can configure API Batch Size for the CF Syslog Drain Release
- Bump ubuntu-trusty stemcell to version `3586.79`
- Bump cf-syslog-drain to version `6.7`
- Bump cflinuxfs2 to version `1.267.0`

| Component | Version |
|------------------------------|---------|
| ubuntu-trusty stemcell | 3586.79 |
| backup-and-restore-sdk | 1.12.0 |
| binary-offline-buildpack-lts | 1.0.30 |

| Component | Version |
|-----------------------------------|----------|
| bosh-dns-allases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.11 |
| cf-autoscaling | 201.9 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.16.0 |
| cf-networking | 2.3.3 |
| cf-smoke-tests | 40.0.40 |
| cf-syslog-drain | 6.7 |
| cflinuxfs2 | 1.267.0 |
| consul | 195 |
| credhub | 1.9.9 |
| diego | 2.8.7 |
| dotnet-core-offline-buildpack-lts | 2.2.5 |
| garden-runc | 1.16.8 |
| go-offline-buildpack-lts | 1.8.33 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |
| loggregator | 102.8 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.6 |
| nodejs-offline-buildpack-lts | 1.6.43 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.70 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.27 |
| push-usage-service-release | 666.0.12 |
| pxc | 0.14.1 |
| python-offline-buildpack-lts | 1.6.28 |
| routing | 0.178.5 |
| ruby-offline-buildpack-lts | 1.7.31 |
| silk | 2.3.4 |
| staticfile-offline-buildpack-lts | 1.4.39 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.11 |

2.2.12

- **[Security Fix]** Apps Manager verifies SSL certificates for endpoints to which it proxies. For environments using untrusted certificates, this may cause Apps Manager to show no content. To resolve this issue, see [Apps Manager shows no content due to SSL validation issue](#).
- **[Feature Improvement]** Increase the maximum number of connections for internal MySQL to 3500
- **[Feature Improvement]** Change default lifetime of Apps Manager client UAA token to 1 hour

- [Feature Improvement] Improve auctioneer cell-state logs in Diego Auctioneer
- [Feature Improvement] Increase Tomcat max http header size to 14K
- [Bug Fix] Fix BBR failures when backing up large blobs to unversioned S3 blobstores
- [Bug Fix] Fix binding route services to apps
- [Bug Fix] Fix concurrency bug in the Router's route pool, which could manifest as a fatal error: "Unlock of unlocked RWMutex"
- [Bug Fix] Fix bug in Apps Manager where space page, services tab shows a 500 error if the last operation of a service is null
- [Bug Fix] Make header tabs focusable and clickable via keyboard navigation in Apps Manager
- [Bug Fix] Improve garden init process to avoid edge cases that can lead to zombies
- [Bug Fix] Add back Consul registration in PXC Proxy to fix issue that can cause API and Application downtime when upgrading from PAS 2.1.x.
- [Bug Fix] Show (Deleted User) in Apps Manager rather than empty row for Cloud Controller users that do not exist in UAA
- [Bug Fix] Fix failure to bind service to app with custom parameters in Apps Manager
- opsmanager failed to upgrade srt 2.1 to 2.2
- Bump ubuntu-trusty-stemcell to version 3586.71
- Bump backup-and-restore-sdk to version 1.12.0
- Bump binary-offline-buildpack-lts to version 1.0.30
- Bump capi to version 1.58.11
- Bump cflinuxfs2 to version 1.260.0
- Bump diego to version 2.8.7
- Bump dotnet-core-offline-buildpack-lts to version 2.2.5
- Bump garden-runc to version 1.16.8
- Bump go-offline-buildpack-lts to version 1.8.33
- Bump nodejs-offline-buildpack-lts to version 1.6.43
- Bump php-offline-buildpack-lts to version 4.3.70
- Bump push-apps-manager-release to version 665.0.27
- Bump pxc to version 0.14.1
- Bump python-offline-buildpack-lts to version 1.6.28
- Bump routing to version 0.178.5
- Bump ruby-offline-buildpack-lts to version 1.7.31
- Bump staticfile-offline-buildpack-lts to version 1.4.39
- Bump uaa to version 60.11

| Component | Version |
|-------------------------------|---------|
| ubuntu-trusty-stemcell | 3586.71 |
| backup-and-restore-sdk | 1.12.0 |
| binary-offline-buildpack-lts | 1.0.30 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.11 |
| cf-autoscaling | 201.9 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.16.0 |
| cf-networking | 2.3.3 |
| cf-smoke-tests | 40.0.40 |
| cf-syslog-drain | 6.6 |
| cflinuxfs2 | 1.260.0 |
| consul | 195 |
| credhub | 1.9.9 |
| diego | 2.8.7 |

| Component | Version |
|-----------------------------------|----------|
| dotnet-core-offline-buildpack-lts | 2.2.0 |
| garden-runc | 1.16.8 |
| go-offline-buildpack-lts | 1.8.33 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |
| loggregator | 102.8 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.6 |
| nodejs-offline-buildpack-lts | 1.6.43 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.70 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.27 |
| push-usage-service-release | 666.0.12 |
| pxc | 0.14.1 |
| python-offline-buildpack-lts | 1.6.28 |
| routing | 0.178.5 |
| ruby-offline-buildpack-lts | 1.7.31 |
| silk | 2.3.4 |
| staticfile-offline-buildpack-lts | 1.4.39 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.11 |

2.2.11

⚠ warning: Do not upgrade directly to this release from PAS v2.1.x. For more information, see [Downtime when Upgrading from v2.1 to v2.2.7 or Later](#).

- **[Security Fix]** Upgrade UAA to 60.9 to address CVE-2018-15754
- **[Feature Improvement]** Improved logging and error handling for Diego Sync job
- **[Feature Improvement]** Blobstore pre-start performance enhancement
- **[Bug Fix]** Remove log noise from Reverse Log Proxy and TrafficController
- **[Bug Fix]** Fix memory allocated to be multiplied by number of instances for each process on space page app tab
- **[Bug Fix]** Ensure that the encoding used by Credhub is UTF-8
- **[Bug Fix]** VXLAN-policy-agent now opens ports in non-ephemeral port range
- **[Bug Fix]** Fix help text for TCP router ports because comma separated lists of ports are not supported
- **[Bug Fix]** Ensure logs and metrics are forwarded by adding syslog_forwarder and loggregator_agent to VMs missing them
- Bump ubuntu-trusty-stemcell to version `3586.60`
- Bump capi to version `1.58.10`
- Bump cf-smoke-tests to version `40.0.40`
- Bump cflinuxfs2 to version `1.255.0`
- Bump credhub to version `1.9.9`
- Bump dotnet-core-offline-buildpack-lts to version `2.2.0`

- Bump go-offline-buildpack-lts to version `1.8.29`
- Bump loggregator to version `102.8`
- Bump nodejs-offline-buildpack-lts to version `1.6.34`
- Bump php-offline-buildpack-lts to version `4.3.64`
- Bump push-apps-manager-release to version `665.0.24`
- Bump python-offline-buildpack-lts to version `1.6.23`
- Bump ruby-offline-buildpack-lts to version `1.7.27`
- Bump silk to version `2.3.4`
- Bump staticfile-offline-buildpack-lts to version `1.4.35`
- Bump uaa to version `60.9`

| Component | Version |
|-----------------------------------|----------|
| ubuntu-trusty-stemcell | 3586.60 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack-lts | 1.0.27 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.10 |
| cf-autoscaling | 201.9 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.16.0 |
| cf-networking | 2.3.3 |
| cf-smoke-tests | 40.0.40 |
| cf-syslog-drain | 6.6 |
| cflinuxfs2 | 1.255.0 |
| consul | 195 |
| credhub | 1.9.9 |
| diego | 2.8.4 |
| dotnet-core-offline-buildpack-lts | 2.2.0 |
| garden-runc | 1.16.1 |
| go-offline-buildpack-lts | 1.8.29 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |
| loggregator | 102.8 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.6 |
| nodejs-offline-buildpack-lts | 1.6.34 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.64 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.24 |
| push-usage-service-release | 666.0.12 |
| pxc | 0.14.0 |
| python-offline-buildpack-lts | 1.6.23 |

| Component | Version |
|----------------------------------|---------|
| ruby-offline-buildpack-lts | 1.7.27 |
| silk | 2.3.4 |
| staticfile-offline-buildpack-lts | 1.4.35 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.9 |

2.2.10

⚠ warning: Do not upgrade directly to this release from PAS v2.1.x. For more information, see [Downtime when Upgrading from v2.1 to v2.2.7 or Later](#).

- [Security Fix] Update JDK to latest patch release for Autoscaler
- [Security Fix] Address leak of CF admin credentials into NFS broker bosh errand logs
- [Security Fix] Fix issue where policy server API responses did not contain X-Frame-Options and Content-Security-Policy
- [Security Fix] Rotate diego intermediate CA before current certificate expires
- [Feature Improvement] Improve performance of the system_report/service_usages endpoint in the `usages-service` to prevent potential 502 or 504 responses on larger deployments
- [Feature Improvement] Fix error handling to report NFS mount failures in CF application logs
- [Feature Improvement] Update version number in link to docs page for Apps Manager
- [Bug Fix] Show more helpful error message in Apps Manager when toggling on Autoscaler fails
- [Bug Fix] Allow scaling of individual processes in multiprocess app when some processes are scaled to zero
- [Bug Fix] Prevent container IPs from leaking by enforcing that TCP RST messages always have the cell ip as the source ip
- [Bug Fix] Fix issue where the CAPI sync job fails when TCP routes are being used
- [Bug Fix] Fix issue where configured database connection timeout for silk was not applied when using an external database
- [Bug fix] Fix race condition during installation of buildpacks
- Bump ubuntu-trusty stemcell to version `3586.57`
- Bump capi to version `1.58.8`
- Bump cf-autoscaling to version `201.9`
- Bump cf-mysql to version `36.16.0`
- Bump cf-networking to version `2.3.3`
- Bump cf-smoke-tests to version `40.0.17`
- Bump cflinuxfs2 to version `1.249.0`
- Bump nfs-volume to version `1.2.6`
- Bump push-apps-manager-release to version `665.0.22`
- Bump push-usage-service-release to version `666.0.12`
- Bump silk to version `2.3.3`

| Component | Version |
|-------------------------------|---------|
| ubuntu-trusty stemcell | 3586.57 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack-lts | 1.0.27 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.8 |
| cf-autoscaling | 201.9 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |

| Component | Version |
|-----------------------------------|----------|
| cf-networking | 2.3.3 |
| cf-smoke-tests | 40.0.17 |
| cf-syslog-drain | 6.6 |
| cflinuxfs2 | 1.249.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.4 |
| dotnet-core-offline-buildpack-lts | 2.1.5 |
| garden-runc | 1.16.1 |
| go-offline-buildpack-lts | 1.8.28 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |
| loggregator | 102.7 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.6 |
| nodejs-offline-buildpack-lts | 1.6.32 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.61 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.22 |
| push-usage-service-release | 666.0.12 |
| pxc | 0.14.0 |
| python-offline-buildpack-lts | 1.6.21 |
| routing | 0.178.4 |
| ruby-offline-buildpack-lts | 1.7.24 |
| silk | 2.3.3 |
| staticfile-offline-buildpack-lts | 1.4.32 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.8 |

2.2.9


⚠ warning: Do not upgrade directly to this release from PAS v2.1.x. For more information, see [Downtime when Upgrading from v2.1 to v2.2.7 or Later](#).

- **[Security Fix]** Bump UAA for CVEs
- **[Feature Improvement]** Improve router pruning behavior when route integrity is enabled
- **[Feature Improvement]** Operators can specify the Diego executor properties for memory usage and disk capacity in order to enable finer grained resource usage strategies
- **[Bug fix]** Enforce that max_valid_packages_stored and max_staged_droplets_stored be >= 1
- **[Bug Fix]** Do not produce duplicate schedules when updating a schedule in Apps Manager
- Bump ubuntu-trusty stemcell to version `3586.52`
- Bump cflinuxfs2 to version `1.245.0`

- Bump push-apps-manager-release to version `665.0.20`
- Bump routing to version `0.178.4`
- Bump uaa to version `60.8`

| Component | Version |
|-----------------------------------|----------|
| ubuntu-trusty-stemcell | 3586.52 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack-lts | 1.0.27 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.7 |
| cf-autoscaling | 201.8 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.1 |
| cf-smoke-tests | 40.0.10 |
| cf-syslog-drain | 6.6 |
| cflinuxfs2 | 1.245.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.4 |
| dotnet-core-offline-buildpack-lts | 2.1.5 |
| garden-runc | 1.16.1 |
| go-offline-buildpack-lts | 1.8.28 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |
| loggregator | 102.7 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.3 |
| nodejs-offline-buildpack-lts | 1.6.32 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.61 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.20 |
| push-usage-service-release | 666.0.11 |
| pxc | 0.14.0 |
| python-offline-buildpack-lts | 1.6.21 |
| routing | 0.178.4 |
| ruby-offline-buildpack-lts | 1.7.24 |
| silk | 2.3.0 |
| staticfile-offline-buildpack-lts | 1.4.32 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.8 |

2.2.8


warning: Do not upgrade directly to this release from PAS v2.1.x. For more information, see [Downtime when Upgrading from v2.1 to v2.2.7 or Later.](#)

- [Security Fix] log-cache no longer supports TLS 1.0 and TLS1.1
- [Feature Improvement] Split up networking policy server database migrations to reduce the risk of a failure causing a partial migration
- [Feature Improvement] Improve error messages logged by Cloud Controller when there are Azure blobstore failures
- [Feature Improvement] Update name of the Small Footprint PAS tile shown on the tile in Ops Manager UI
- [Feature Improvement] clock_global now defaults to 2 instances to be highly available
- [Feature Improvement] Allow disabling connection pooling for autoscaler API & escape special characters in external database passwords
- [Bug Fix] Prevent potential memory leak when Cloud Controller’s space summary endpoint is called under certain usage conditions
- [Bug Fix] Fix manual configuration of load balancers for SSH to application containers on Small Footprint PAS (SF-PAS)
- Bump ubuntu-trusty stemcell to version 3586.46
- Bump capi to version 1.58.7
- Bump cf-autoscaling to version 201.8
- Bump cf-networking to version 2.3.1
- Bump cf-smoke-tests to version 40.0.10
- Bump cflinuxfs2 to version 1.242.0
- Bump diego to version 2.8.4
- Bump go-offline-buildpack-lts to version 1.8.28
- Bump java-offline-buildpack-lts to version 4.16.1
- Bump log-cache to version 1.4.7
- Bump ruby-offline-buildpack-lts to version 1.7.24

| Component | Version |
|-----------------------------------|---------|
| ubuntu-trusty stemcell | 3586.46 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack-lts | 1.0.27 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.7 |
| cf-autoscaling | 201.8 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.1 |
| cf-smoke-tests | 40.0.10 |
| cf-syslog-drain | 6.6 |
| cflinuxfs2 | 1.242.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.4 |
| dotnet-core-offline-buildpack-lts | 2.1.5 |
| garden-runc | 1.16.1 |
| go-offline-buildpack-lts | 1.8.28 |
| haproxy | 8.7.0 |
| java-offline-buildpack-lts | 4.16.1 |
| log-cache | 1.4.7 |

| Component | Version |
|----------------------------------|----------|
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.3 |
| nodejs-offline-buildpack-lts | 1.6.32 |
| notifications-ui | 33 |
| notifications | 46 |
| php-offline-buildpack-lts | 4.3.61 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.19 |
| push-usage-service-release | 666.0.11 |
| pxc | 0.14.0 |
| python-offline-buildpack-lts | 1.6.21 |
| routing | 0.178.3 |
| ruby-offline-buildpack-lts | 1.7.24 |
| silk | 2.3.0 |
| staticfile-offline-buildpack-lts | 1.4.32 |
| statsd-injector | 1.3.0 |
| syslog | 11.3.2 |
| uaa | 60.2 |

2.2.7

⚠ warning: Do not upgrade directly to this release from PAS v2.1.x. For more information, see [Downtime when Upgrading from v2.1 to v2.2.7 or Later](#).

- **[Security Fix]** Bump garden-runc to prevent malicious users from causing a denial of service for other apps
- **[Feature Improvement]** Improve nfs blobstore pre-start performance
- **[Bug Fix]** space and org managers can now view app logs in apps manager
- **[Bug Fix]** Fix unsafe logic in NFS unmount and drain code that may lead to deletion of files on remote NFS shares.
- **[Bug Fix]** PAS 2.1.14 upgrade fails with `Error: release 'cf-networking/1.10.2' has already been uploaded`
- **[Bug Fix]** Fix issue in loggregator where AZ names with special characters could cause metron agent job to fail
- **[Bug Fix]** Fix issue where the PAS tile could be incorrectly downloaded when upgrading SF-PAS via PivNet
- **[Bug Fix]** Fix parse error for syslog rules when iptables logging is enabled
- Bump binary-offline-buildpack-lts to version `1.0.27`
- Bump capi to version `1.58.5`
- Bump cf-cli to version `1.5.0`
- Bump cf-smoke-tests to version `40.0.9`
- Bump cf-syslog-drain to version `6.6`
- Bump cflinuxfs2 to version `1.238.0`
- Bump dotnet-core-offline-buildpack-lts to version `2.1.5`
- Bump garden-runc to version `1.16.1`
- Bump go-offline-buildpack-lts to version `1.8.27`
- Bump java-offline-buildpack-lts to version `4.15.1`
- Bump loggregator to version `102.7`
- Bump nfs-volume to version `1.2.3`
- Bump nodejs-offline-buildpack-lts to version `1.6.32`
- Bump php-offline-buildpack-lts to version `4.3.61`

- Bump push-apps-manager-release to version `665.0.19`
- Bump pxc to version `0.14.0`
- Bump python-offline-buildpack-lts to version `1.6.21`
- Bump ruby-offline-buildpack-lts to version `1.7.23`
- Bump staticfile-offline-buildpack-lts to version `1.4.32`
- Bump stemcell ubuntu-trusty to version `3586.43`

| Component | Version |
|-------------------------------|----------|
| stemcell | 3586.43 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.27 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.5 |
| cf-autoscaling | 201.3 |
| cf-backup-and-restore | 0.0.11 |
| cf-cli | 1.5.0 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.9 |
| cf-syslog-drain | 6.6 |
| cflinuxfs2 | 1.238.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.2 |
| dotnet-core-offline-buildpack | 2.1.5 |
| garden-runc | 1.16.1 |
| go-offline-buildpack | 1.8.27 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.15.1 |
| log-cache | 1.4.4 |
| loggregator | 102.7 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.3 |
| nodejs-offline-buildpack | 1.6.32 |
| notifications | 46 |
| notifications-ui | 33 |
| php-offline-buildpack | 4.3.61 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.19 |
| push-usage-service-release | 666.0.11 |
| pxc | 0.14.0 |
| python-offline-buildpack | 1.6.21 |
| routing | 0.178.3 |
| ruby-offline-buildpack | 1.7.23 |
| staticfile-offline-buildpack | 1.4.32 |
| statsd-injector | 1.3.0 |

| Component | Version |
|---|---------|
| syslog | 11.3.2 |
| uua | 60.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.6

- **[Security Fix]** Prevent app developers from registering an NFS service broker that issues service bindings with uid and gid specified when LDAP is enabled
- **[Feature Improvement]** Update BOSH DNS configuration to allow resolving BBS and Auctioneer servers on unhealthy VMs
- **[Feature Improvement]** Operators can configure the maximum number of packages and droplets to store
- **[Feature Improvement]** Operators can override connection timeout values for the cloud controller database to prevent downtime when MySQL proxy VMs are recreated
- **[Feature Improvement]** Update PAS 2.2 with binary-buildpacks that have stack associations
- **[Bug Fix]** Fix issue where the SF-PAS tile could be incorrectly downloaded when upgrading PAS via PivNet
- **[Bug Fix]** Improve performance to reduce chance of failed database migrations during upgrades of usage service
- **[Bug Fix]** Fixes and improvements for Apps Manager
 - When the Autoscaler is not installed, prevent a crash that occurs on the app page
 - When creating a space as admin, make the admin a member of the corresponding organization
 - Improved the display of service plan costs when costs are not integers as expected
 - Prevent a page crash that occurs when there are no upcoming scheduled limit changes
- Bump binary-offline-buildpack to version [1.0.25](#)
- Bump push-apps-manager-release to version [665.0.18](#)
- Bump push-usage-service-release to version [666.0.11](#)
- Bump stemcell ubuntu-trusty to version [3586.42](#)

| Component | Version |
|---|---------|
| stemcell | 3586.42 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.25 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.4 |
| cf-autoscaling | 201.3 |
| cf-backup-and-restore | 0.0.11 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.8 |
| cf-syslog-drain | 6.5 |
| cflinuxfs2 | 1.235.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.2 |
| dotnet-core-offline-buildpack | 2.1.3 |
| garden-runc | 1.13.3 |
| go-offline-buildpack | 1.8.25 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.13.1 |
| log-cache | 1.4.4 |
| loggregator | 102.4 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

| Component | Version |
|---|----------|
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.2 |
| nodejs-offline-buildpack | 1.6.28 |
| notifications | 46 |
| notifications-ui | 33 |
| php-offline-buildpack | 4.3.57 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.18 |
| push-usage-service-release | 666.0.11 |
| python-offline-buildpack | 1.6.18 |
| pxc | 0.9.0 |
| routing | 0.178.3 |
| ruby-offline-buildpack | 1.7.21 |
| staticfile-offline-buildpack | 1.4.29 |
| statsd-injector | 1.3.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| uaa | 60.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.5

- **[Security Fix]** Bump usage service for CVE-2018-11086
- **[Security Fix]** Bump apps manager for CVE-2018-11088
 - Fix security vulnerability: CVE-2018-11088
 - Fix typo in autoscaling flyout
 - Text changes to improve actuator integration with Steeltoe
 - Steeltoe heap dumps should have extension .dmp
 - Fix Spring endpoints not appearing in app actions dropdown for Spring 2.0 apps
 - Fix Spring “View Raw JSON” feature not appearing when git info not present on app
 - Fix occasionally incorrect display of app processes when scaling app memory or disk
 - Fix app remaining in “Starting...” state after scaling
 - Fix autoscale instance limits not refreshing in flyout after applying changes
- **[Bug Fix]** Autoscaler uses https to communicate with log-cache instead of http
- **[Bug Fix]** Configure PXC MySQL to listen on port that will not conflict with processes that get a random port (Small Footprint Only)
 - Change MySQL from listening on port 33306 to 13306 for Small Footprint PAS
- **[Feature Improvement]** Do not back up resources bucket as it is not restored
 - The property `.properties.system_blobstore.external.resources_bucket.value` has been deprecated and will be removed in 2.3
- Bump bosh-system-metrics-forwarder to version `0.0.15`
- Bump cf-autoscaling to version `201.3`
- Bump cf-smoke-tests to version `40.0.8`
- Bump cflinuxfs2 to version `1.235.0`
- Bump log-cache to version `1.4.4`
- Bump pivotal-account to version `1.9.1`
- Bump push-apps-manager-release to version `665.0.17`
- Bump push-usage-service-release to version `666.0.10`
- Bump routing to version `0.178.3`

- Bump stemcell ubuntu-trusty to version 3586.40

| Component | Version |
|---|----------|
| stemcell | 3586.40 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.21 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.15 |
| capi | 1.58.4 |
| cf-autoscaling | 201.3 |
| cf-backup-and-restore | 0.0.11 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.8 |
| cf-syslog-drain | 6.5 |
| cflinuxfs2 | 1.235.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.2 |
| dotnet-core-offline-buildpack | 2.1.3 |
| garden-runc | 1.13.3 |
| go-offline-buildpack | 1.8.25 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.13.1 |
| log-cache | 1.4.4 |
| loggregator | 102.4 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.2 |
| nodejs-offline-buildpack | 1.6.28 |
| notifications | 46 |
| notifications-ui | 33 |
| php-offline-buildpack | 4.3.57 |
| pivotal-account | 1.9.1 |
| push-apps-manager-release | 665.0.17 |
| push-usage-service-release | 666.0.10 |
| python-offline-buildpack | 1.6.18 |
| pxc | 0.9.0 |
| routing | 0.178.3 |
| ruby-offline-buildpack | 1.7.21 |
| staticfile-offline-buildpack | 1.4.29 |
| statsd-injector | 1.3.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| uaa | 60.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.4

- [Feature Improvement] Improve performance for `nfs-experimental` readonly mounts and those that don't set the uid and gid parameters
- [Bug Fix] Fix autoscaler and smoke test failures when using database with timezone setting other than UTC
- [Bug Fix] Fixes BBS communication with Locket issue on startup when deploying with BOSH DNS enabled
- [Bug Fix] Apps manager: Fix spaces count on org page
- [Bug Fix] Apps manager: When the autoscaler service fails to toggle, show an error flash message
- [Bug Fix] Apps manager: A spacedeveloper can map a route without providing a hostname
- [Bug Fix] Apps manager: Fix crash on app page overview tab when spring health endpoint returns an array of objects instead of an array of strings
- Bump cf-autoscaling to version `201.1`
- Bump cf-smoke-tests to version `40.0.6`
- Bump cflinuxfs2 to version `1.229.0`
- Bump diego to version `2.8.2`
- Bump log-cache to version `1.3.0`
- Bump nfs-volume to version `1.2.2`
- Bump push-apps-manager-release to version `665.0.14`
- Bump routing to version `0.178.2`
- Bump stemcell to version `3586.27`

| Component | Version |
|--|---------|
| stemcell | 3586.27 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.21 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.11 |
| capi | 1.58.4 |
| cf-autoscaling | 201.1 |
| cf-backup-and-restore | 0.0.11 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.6 |
| cf-syslog-drain | 6.5 |
| cflinuxfs2 | 1.229.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.2 |
| dotnet-core-offline-buildpack | 2.1.3 |
| garden-runc | 1.13.3 |
| go-offline-buildpack | 1.8.25 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.13.1 |
| log-cache | 1.3.0 |
| loggregator | 102.4 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.2 |
| nodejs-offline-buildpack | 1.6.28 |
| notifications | 46 |
| notifications-ui | 33 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior | |

| Component | Version |
|---|----------|
| cha-offline-buildpack | 4.3.57 |
| pivotal-account | 1.9.0 |
| push-apps-manager-release | 665.0.14 |
| push-usage-service-release | 666.0.2 |
| python-offline-buildpack | 1.6.18 |
| pxc | 0.9.0 |
| routing | 0.178.2 |
| ruby-offline-buildpack | 1.7.21 |
| staticfile-offline-buildpack | 1.4.29 |
| statsd-injector | 1.3.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| uaa | 60.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.3

- **[Feature Improvement]** Loggregator agent egresses preferred tags instead of DeprecatedTags in loggregator envelopes. This fixes a high CPU issue in Doppler cluster.
- **[Feature Improvement]** Fix issue where fileserver assets were not correctly invalidated in Diego cell caches after an upgrade
- **[Feature Improvement]** `capi` `/v2/info` endpoint returns additional metadata for `name`, `build` and `description`
- **[Feature Improvement]** Add the `healthwatch_api_admin` UAA client to allows access to the Healthwatch API
- **[Feature Improvement]** Retry blobstore uploads when GCS returns transmission error
- **[Feature Improvement]** Allow operators to configure application health check timeout in PAS
- **[Feature Improvement]** Move encryption key field to the top of the Credhub page
- **[Bug Fix]** Fix TLS pruning behavior for Gorouter
- **[Bug Fix]** Apps using a Docker image from an insecure registry configured in the Private Docker Insecure Registry Whitelist can now be staged successfully.
- **[Bug Fix]** Fix option “HAProxy requests but does not require client certificates.”
- **[Bug Fix]** Bump apps manager with changes
 - When creating new services, no longer show org-scoped services from other organizations
 - Org Managers and Admins can leave organizations
 - When visiting Apps Manager on an environment where UAA has a self-signed SSL cert, do not blue screen, redirect to UAA login page.
- **[Bug Fix]** Fix performance and data consistency issues in Log Cache.
- **[Bug Fix]** Set cloud controller staging timeout value on all cloud controller jobs to allow large apps to stage before the timeout.
- Bump capi to version `1.58.4`
- Bump diego to version `2.8.1`
- Bump java-offline-buildpack to version `4.13.1`
- Bump log-cache to version `1.4.0`
- Bump loggregator to version `102.4`
- Bump mysql-monitoring to version `8.20.0`
- Bump push-apps-manager-release to version `665.0.13`
- Bump routing to version `0.178.1`
- Bump stemcell to version `3586.26`

| Component | Version |
|---|---------|
| stemcell | 3586.26 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.21 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

| Component | Version |
|---|----------|
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.11 |
| capi | 1.58.4 |
| cf-autoscaling | 201.0.0 |
| cf-backup-and-restore | 0.0.11 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.5 |
| cf-syslog-drain | 6.5 |
| cflinuxfs2 | 1.227.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.1 |
| dotnet-core-offline-buildpack | 2.1.3 |
| garden-runc | 1.13.3 |
| go-offline-buildpack | 1.8.25 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.13.1 |
| log-cache | 1.4.0 |
| loggregator | 102.4 |
| mysql-monitoring | 8.20.0 |
| nats | 24 |
| nfs-volume | 1.2.1 |
| nodejs-offline-buildpack | 1.6.28 |
| notifications | 46 |
| notifications-ui | 33 |
| php-offline-buildpack | 4.3.57 |
| pivotal-account | 1.9.0 |
| push-apps-manager-release | 665.0.13 |
| push-usage-service-release | 666.0.2 |
| python-offline-buildpack | 1.6.18 |
| pxc | 0.9.0 |
| routing | 0.178.1 |
| ruby-offline-buildpack | 1.7.21 |
| staticfile-offline-buildpack | 1.4.29 |
| statsd-injector | 1.3.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| uaa | 60.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.2

- **[Feature Improvement]** Add ability to configure HAProxy client certificate verification
- **[Security Fix]** Bump UAA for [CVE-2018-11047](<https://www.cloudfoundry.org/blog/cve-2018-11047/>)
- Bump cflinuxfs2 version 1.227.0
- Bump java-offline-buildpack version 4.13

- Bump uaa version 60.2

| Component | Version |
|---|----------|
| stemcell | 3586.24 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.21 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.11 |
| capi | 1.58.1 |
| cf-autoscaling | 201.0.0 |
| cf-backup-and-restore | 0.0.11 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.5 |
| cf-syslog-drain | 6.5 |
| cflinuxfs2 | 1.227.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.0 |
| dotnet-core-offline-buildpack | 2.1.3 |
| garden-runc | 1.13.3 |
| go-offline-buildpack | 1.8.25 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.13 |
| log-cache | 1.3.0 |
| loggregator | 102.2 |
| mysql-monitoring | 8.18.0 |
| nats | 24 |
| nfs-volume | 1.2.1 |
| nodejs-offline-buildpack | 1.6.28 |
| notifications | 46 |
| notifications-ui | 33 |
| php-offline-buildpack | 4.3.57 |
| pivotal-account | 1.9.0 |
| push-apps-manager-release | 665.0.11 |
| push-usage-service-release | 666.0.2 |
| python-offline-buildpack | 1.6.18 |
| pxc | 0.9.0 |
| routing | 0.178.0 |
| ruby-offline-buildpack | 1.7.21 |
| staticfile-offline-buildpack | 1.4.29 |
| statsd-injector | 1.3.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| uaa | 60.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.1

- **[Feature Improvement]** Allows PCF Metrics to be installed with both v1.5 and v1.4 versions to prevent dataloss.
- **[Bug Fix]** Bump cf-smoke-tests-release to 40.0.5 to fix some flakiness
- **[Security Fix]** Bump apps manager for CVE-2018-11044
 - When creating new services, no longer show org-scoped services from other organizations
 - Org Managers and Admins can leave organizations
- **[Security Fix]** Bump loggregator release for CVE-2018-1268 and CVE-2018-1269
- ***** [Bug Fix]**** bump consul to v195
 - Includes go 1.9.7, removes go 1.8.*.
 - Deploying v193 could fail on some deployments due to a conflict with other tiles that compiled the release differently
 - Fixes intermittent consul DNS issues on Windows Cells
- Bump binary-offline-buildpack to version 1.0.21
- Bump cf-smoke-tests to version 40.0.5
- Bump cflinuxfs2 to version 1.223.0
- Bump consul to version 195
- Bump dotnet-core-offline-buildpack to version 2.1.3
- Bump go-offline-buildpack to version 1.8.25
- Bump loggregator to version 102.2
- Bump nodejs-offline-buildpack to version 1.6.28
- Bump php-offline-buildpack to version 4.3.57
- Bump push-apps-manager-release to version 665.0.11
- Bump python-offline-buildpack to version 1.6.18
- Bump ruby-offline-buildpack to version 1.7.21
- Bump staticfile-offline-buildpack to version 1.4.29

| Component | Version |
|-------------------------------|---------|
| stemcell | 3586.24 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.21 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.11 |
| capi | 1.58.1 |
| cf-autoscaling | 201.0.0 |
| cf-backup-and-restore | 0.0.11 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.5 |
| cf-syslog-drain | 6.5 |
| cflinuxfs2 | 1.223.0 |
| consul | 195 |
| credhub | 1.9.3 |
| diego | 2.8.0 |
| dotnet-core-offline-buildpack | 2.1.3 |
| garden-runc | 1.13.3 |
| go-offline-buildpack | 1.8.25 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.12.1 |
| log-cache | 1.3.0 |

* Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior.

| Component | Version |
|--|----------|
| loggregator | 102.3 |
| mysql-monitoring | 8.18.0 |
| nats | 24 |
| nfs-volume | 1.2.1 |
| nodejs-offline-buildpack | 1.6.28 |
| notifications | 46 |
| notifications-ui | 33 |
| php-offline-buildpack | 4.3.57 |
| pivotal-account | 1.9.0 |
| push-apps-manager-release | 665.0.11 |
| push-usage-service-release | 666.0.2 |
| python-offline-buildpack | 1.6.18 |
| pxc | 0.9.0 |
| routing | 0.178.0 |
| ruby-offline-buildpack | 1.7.21 |
| staticfile-offline-buildpack | 1.4.29 |
| statsd-injector | 1.3.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| uaa | 60 |
| <i>* Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior.</i> | |

2.2.0

| Component | Version |
|--|---------|
| stemcell | 3586.24 |
| backup-and-restore-sdk | 1.7.1 |
| binary-offline-buildpack | 1.0.18 |
| bosh-dns-aliases | 0.0.2 |
| bosh-system-metrics-forwarder | 0.0.11 |
| capi | 1.58.1 |
| cf-autoscaling | 201.0.0 |
| cf-backup-and-restore | 0.0.11 |
| cf-mysql | 36.14.0 |
| cf-networking | 2.3.0 |
| cf-smoke-tests | 40.0.4 |
| cf-syslog-drain | 6.5 |
| cflinuxfs2 | 1.220.0 |
| consul | 194 |
| credhub | 1.9.3 |
| diego | 2.8.0 |
| dotnet-core-offline-buildpack | 2.0.7 |
| garden-runc | 1.13.3 |
| go-offline-buildpack | 1.8.23 |
| haproxy | 8.7.0 |
| java-offline-buildpack | 4.12.1 |
| log-cache | 1.3.0 |
| <i>* Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior.</i> | |

| Component | Version |
|---|---------|
| loggregator | 102.1 |
| mysql-monitoring | 8.18.0 |
| nats | 24 |
| nfs-volume | 1.2.1 |
| nodejs-offline-buildpack | 1.6.25 |
| notifications | 46 |
| notifications-ui | 33 |
| php-offline-buildpack | 4.3.56 |
| pivotal-account | 1.9.0 |
| push-apps-manager-release | 665.0.9 |
| push-usage-service-release | 666.0.2 |
| python-offline-buildpack | 1.6.17 |
| pxc | 0.9.0 |
| routing | 0.178.0 |
| ruby-offline-buildpack | 1.7.19 |
| staticfile-offline-buildpack | 1.4.28 |
| statsd-injector | 1.3.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| uua | 60 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

How to Upgrade

The procedure for upgrading to Pivotal Application Service (PAS) v2.2 is documented in the [Upgrading Pivotal Cloud Foundry](#) topic.

When upgrading to v2.2, be aware of the following upgrade considerations:

- If you previously used an earlier version of PAS, you must first upgrade to PAS v2.1 to successfully upgrade to PAS v2.2.
- Some partner service tiles may be incompatible with PCF v2.2. Pivotal is working with partners to ensure their tiles are updated to work with the latest versions of PCF.

For information about which partner service releases are currently compatible with PCF v2.2, review the appropriate partners services release documentation at <https://docs.pivotal.io>, or contact the partner organization that produces the tile.

New Features in PAS v2.2

More Secure Cipher Suites for CF SSH Proxy


The CF SSH proxy accepts a narrower range of ciphers, MACs, and key exchanges. This change improves the security of CF SSH sessions.

These SSH proxy settings are not configurable in the PAS tile.

Note: This change may be incompatible with SSH clients other than `cf ssh`. See [SSH Proxy Security Configuration](#) for more information about the supported ciphers, MACs, and key exchanges.

TLS-Encrypted Option for Internal System Databases

For internal system databases, PAS now supports a more secure [Percona Server](#) database with TLS-encrypted communication between server nodes, as well as the previous [MariaDB](#) option. See [Migrate to TLS Communication](#) for details.

 **Warning:** Migrating PAS internal databases to using TLS causes temporary downtime of PAS system functions. It does not interrupt apps hosted by PAS.

Support for AWS Instance Profiles

PAS now supports [AWS instance profiles](#) when you are configuring an S3 filestore. Either an instance profile or an access and secret key are required.

For more information, see the **External or S3 Filestore** section of the [PAS installation topic for your IaaS](#).

Unversioned S3 Buckets for Backups

PAS can now back up unversioned S3 buckets used for external file storage, saving backup artifacts to separate, dedicated backup buckets. For more information, see the **External or S3 Filestore** section of the [PAS installation topic for your IaaS](#).

Gorouter Logging Changes for GDPR Compliance

Operators can now disable logging of client IP addresses in the Gorouter to comply with the General Data Protection Regulation (GDPR).

This setting, **Logging of Client IPs in CF Router**, is configured in the **Networking** pane of the PAS tile. You can disable logging of the `X-Forwarded-For` HTTP header only or of both the source IP address and the `X-Forwarded-For` HTTP header. By default, the **Log client IPs** option is set in PAS.

For more information about configuring the **Logging of Client IPs in CF Router** field, see the **Configure Networking** section of the [PAS installation topic for your IaaS](#).


New Format for Timestamps in Diego Component Logs

The timestamps in the Diego component logs are now in a format compatible with [RFC 3339](#). Log-level identifiers are also formatted as strings instead of numeric codes.

RFC 3339 timestamps are enabled by default for new PAS v2.2 deployments. Upgrades from earlier PAS versions retain the previous component log format with Unix epoch timestamps.

You can enable the new timestamp format for Diego logs in the PAS tile.

For more information, see the **Configure Application Containers** section of the [PAS installation topic for your IaaS](#).

 **Breaking Change:** Before enabling RFC 3339 format for Diego logs, ensure that your log aggregation system anticipates the timestamp format change. If you experience issues, you can disable RFC 3339 format in the PAS tile.

Task Placement More Resilient to Resource Unavailability

When memory or disk resources are temporarily unavailable, PAS no longer fails application and staging tasks immediately. Instead, it attempts several times to place the task on a Diego cell with sufficient capacity.

This temporary unavailability may occur when many application instances or tasks are being created or destroyed simultaneously or when the Diego Bulletin Board System (BBS) or auctioneer fails to communicate to one or more Diego cells.

For more information about Diego task allocation, see [How Diego Balances App Processes](#).

Instance Identity Certificates Contain CF Org and Space IDs


The instance identity certificates provided to application instance and task containers now contain organizational units with their CF org and space IDs in the certificate subject name. Existing applications must be restarted after an upgrade to PAS v2.2 to receive these new identifiers.

For more information, see [Using Instance Identity Credentials](#).


BOSH DNS Enabled By Default

BOSH DNS is enabled by default for both app containers and PCF components in PCF v2.2.

In previous versions, Consul managed service discovery between PCF components, but Consul is being replaced by BOSH DNS.

 **Note:** In PCF v2.2, Consul and BOSH DNS are both available in PCF, but BOSH DNS is the only service used for DNS requests.

You can disable BOSH DNS if instructed to do so by Pivotal support. If you disabled BOSH DNS in PCF v2.1, reenable it before upgrading to PCF v2.2. For more information, see [BOSH DNS Enabled By Default For App Containers and PCF Components](#).

 **warning:** Do not disable BOSH DNS without instructions from Pivotal support. Disabling BOSH DNS will also disable PKS, NSX-T, and several PAS features.

Service Discovery for Container-to-Container Networking Enabled By Default

In PAS v2.1, service discovery for container-to-container networking was an experimental feature that you could opt in to use. In PAS v2.2, this feature is enabled by default, and you can opt out of using it.

For more information about disabling service discovery for container-to-container networking, see the **Configure Application Developer Controls** section of the [PAS installation topic for your IaaS](#).

DNS Search Domains


PAS v2.2 allows you to configure the DNS search domains to be used in containers by entering a comma-separated list.

For more information, see the **DNS Search Domains** configuration described in the **Container Networking** section of the [PAS installation topic for your IaaS](#).

Pivotal Account Replaced by UAA

Prior to PAS v2.2, you could use Pivotal Account to create and manage user accounts. In PAS v2.2, PAS stops using Pivotal Account, and you can now create and manage user accounts through the UAA UI instead.

The **Errands** pane in the PAS tile replaces **Pivotal Account Errand** with the **Delete Pivotal Account Application** errand, which is configured to run automatically. For more information, see the **Configure Errands** section of the [PAS installation topic for your IaaS](#).

 **Note:** The **Delete Pivotal Account Application** errand does not delete the `account` database used by the app.

You can manually delete the `account` database that remains as an artifact in PAS MySQL by following these steps:

1. Use `bosh ssh` to access one of the MySQL VMs in your deployment. See [Advanced Troubleshooting with the BOSH CLI](#) for instructions. For example:

```
bosh ssh mysql/0
```

2. Run the following command to start MySQL using the credentials in `mylogin.cnf`:

```
mysql --defaults-file=/var/vcap/jobs/mysql/config/mylogin.cnf
```

3. Run the following command to delete the `account` database:

```
DROP database account;
```


Loggregator Adds Log Cache in PAS Advanced Features


Loggregator adds an in-memory caching layer for logs and metrics and provides a RESTful interface for retrieving them. Use Log Cache to query and filter

logs.


Log Cache is colocated on the Doppler VMs. It speeds up the retrieval of data from the Loggregator system, especially for deployments with a large number of Dopplers. Log Cache uses the available memory on a device to store logs, and so may impact performance during periods of high memory contention.

For more information about Log Cache, see [Enable Log Cache](#).

 **Breaking Change:** If you use Pivotal Application Service's App Autoscaler, Pivotal strongly recommends enabling Log Cache. App Autoscaler relies on Log Cache's API endpoints to function properly. If you disable Log Cache, App Autoscaler will fail.

 **Breaking Change:** Because of the addition of the log-cache process to the Doppler VM, the memory requirement for the Doppler VM has been increased to 4GB.

Syslog Draining for Service Instances (Beta)

The `cf-drain-cli` plugin now enables app developers to bind user-provided syslog drains to service instances. For more information, see the [CF Drain CLI Plugin](#)  GitHub repository. If a service tile supports syslog drains, app developers can use this plugin to forward logs and metrics from their service instance to an external endpoint.

Forwarding of DEBUG Syslog Messages Disabled by Default

By default, PAS v2.2 does not forward DEBUG syslog messages to external services. The new **Don't Forward Debug Logs** checkbox is configurable in the **System Logging** pane of the PAS tile.

For more information about configuring this checkbox, see the **(Optional) Configure System Logging** section of the [PAS installation topic for your IaaS](#) .

If you currently have a custom rule to filter out DEBUG syslog messages, you can delete it. Before deleting your custom rule, ensure the **Don't Forward Debug Logs** checkbox is enabled in the PAS tile.

App Autoscaler UI Integrated into Apps Manager

The App Autoscaler UI is now integrated into Apps Manager. This enables users to configure autoscaling for their apps through Apps Manager. The new UI is based on the App Autoscaler API v2.0.

For more information about scaling apps using App Autoscaler, see [Scaling an Application Using App Autoscaler](#).


Improved App Autoscaler CLI

The App Autoscaler CLI now supports creating custom autoscaling rules and scheduled limit changes for apps bound to the App Autoscaler service.

For more information about the App Autoscaler CLI, see [Using the App Autoscaler CLI](#).

Updated App Autoscaler Metrics Collection Interval Values

This release updates the minimum, maximum, and default values for the Metrics Collection Interval used by the App Autoscaler in PAS. Updated minimum: 60 seconds. Updated maximum: 3600 seconds. Updated default: 120 seconds.

To configure this value, see the **(Optional) Configure App Autoscaler** section of the [PAS installation topic for your IaaS](#) .

App Autoscaler Verbose Logging

Verbose logs are now available for App Autoscaler. Verbose logs show specific reasons why App Autoscaler scaled the app, information on minimum and maximum instance limits, App Autoscaler's status, and more. Verbose logs result in more detailed logs, but do not otherwise impact performance.

To enable verbose logs, select the **Verbose Logging** checkbox in the App Autoscaler pane.

For more information, see the **(Optional) Configure App Autoscaler** section of the [PAS installation topic for your IaaS](#).

Improved Session Management Behavior in Apps Manager

Users are now logged out of Apps Manager when they log out of UAA or their UAA session expires. You can configure the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** values in the **UAA** pane of the PAS tile.

Health Check Invocation Timeout is Configurable via Cloud Controller V3 API

This V3 API endpoint allows users to change the duration of a health check invocation timeout. An invocation timeout is a period of time within a standard timeout period, during which a healthcheck assess the health of your app. A responsive app is marked as alive, but an unresponsive app is marked as dead.

By default, the health check invocation timeout is set to one second. Increasing the invocation timeout period allows health checks to perform complex actions that may exceed the default timeout setting. A longer invocation timeout period may prevent your app from being marked as dead when it is actually healthy.

Change the invocation timeout period with the `invocation_timeout` flag in the healthcheck API.

For more information, see [The health_check object](#).

Selector-Based Subscription Model and Reference Nozzles

You can request Firehose subscriptions that filter out all unspecified content using the Loggregator v2 API endpoint from the Reverse Log Proxy.

For examples of nozzles that use the Loggregator V2 API and consume only specified whitelisted metrics, see `rlpreader` and `rlptypereader` in the [loggregator-tools](#) repository.

For more information about this feature, see the *V2 Subscriptions* page of the [loggregator-release](#) repository.

Known Issues

Downtime when Upgrading from v2.1 to v2.2.7 or Later

Upgrading directly from PAS v2.1.x to v2.2.7 or later may cause significant app downtime. If you are upgrading from v2.1.x, Pivotal recommends that you upgrade to v2.2.6 or an earlier patch release of v2.2.x. Once you are on v2.2.6 or an earlier patch release of v2.2.x, you can then upgrade to v2.2.7.

A fix for this issue is planned for v2.2.12.

For more information, see the following article in the Pivotal Knowledge Base: [How to avoid app downtime while upgrading from PAS v2.1.x to v2.2.7](#).

CredHub Database Cannot be External on GCP

If your PAS deployment is on GCP and you want to use Runtime CredHub, you must select **Internal** for both your system databases and CredHub database. If you are using external system databases, you cannot use CredHub.

CredHub is not compatible with the external database option on GCP. GCP Cloud SQL presents its certificate in a way that CredHub refuses to connect to it.

App Autoscaler Smoke Test Errand Failure

When deploying PAS v2.2.x, the App Autoscaler smoke test errand may fail with the following error:

Autoscaler did not receive any metrics for disk_quota during the scaling window. Scaling down will be deferred until these metrics are available.

For a workaround, see the following KB article: [App Autoscaler Smoke Test Errand fails to retrieve any metrics from logcache](#).

Apps Serve Routes After App Deletion Due to MySQL Errors

After an app is deleted, the app instances are not always cleaned up on Diego cells. Those instances continue to serve routes.

This error occurs when the Cloud Controller and Diego cells fall out of sync. You can resolve this issue by restarting the `cloud_controller_clock` process in the `clock_global` VM.

For more information, see the Knowledge Base article [Apps Serve Routes Even After App Deletion Due To MySQL Errors](#).

Timeouts Connecting to GCS Blobstores Using Service Account Key Authentication

Pushing large apps may fail if you use Google Cloud Storage (GCS) as an external blobstore, and you authenticate to it with a GCS Service Account. This option is configured in the PAS tile **File Storage** pane, under **Configure your Cloud Controller's filesystem**.

For more information, see the Knowledge Base article [Timeouts connecting to GCS blobstores when configured to use service account key authentication](#).

Deploying PAS Runtime for Windows Results in an Access is Denied Error

This rare issue can occur when you deploy the PAS Runtime for Windows v2.2.

The error reads:

```
Action Failed get_task: Task 5b085f4a-b56a-42e3-5974-f3876879397d result: Compiling package certspliter_windows: Removing packages: Uninstalling package bundle: remove /var/vcap/data/packages/golang-windows/83bf1f4181665d2ee2c0118a56bd04764b8f56b0/go/bin/go.exe: Access is denied.
```

If you encounter this error, Pivotal recommends retrying the deployment until the error does not occur.

For more information, see the Knowledge Base article [Deploying PAS for Windows Tile Results in an Access is Denied Error](#).

PAS Deployment Fails with Spring Cloud Services v1.5.5 and Earlier

If you are running Spring Cloud Services, you need to upgrade to Spring Cloud Services v1.5.6 or later before you can upgrade PCF to v2.2.

For more information, see the Knowledge Base article [Spring Cloud Services Deployment fails with can't resolve link error in PAS 2.2](#).

Some Components Use Go v1.9 to Avoid x.509 Cert Errors in v1.10

x509 certificate parsing in the Go language is [stricter in v1.10](#) than it is in v1.9. As a result, certificates that many Pivotal customers generated with open-source tools and continue to use could cause errors if parsed by Go v1.10. To avoid this, some PAS v2.2 components use Go v1.9. PAS v2.2 includes both versions of the language.

Configuring a List of TCP Routing Ports

This section describes an issue and workaround related to configuring a list of TCP Routing Ports in the PAS tile UI.

Issue

You cannot enter a comma-separated list of ports in the **TCP Routing Ports** field of the PAS tile. If you enter a comma-separated list, the Routing API does not start. The **TCP Routing Ports** field allows entries in the following formats:

- A single value, such as `1234`

- A range of values, such as `1234-5678`

Workaround

If you want to configure a list of ports, Pivotal recommends following these steps:



Note: This procedure causes brief downtime for TCP apps listening on ports that you open after deploying PAS.

1. Configure PAS with **Enable TCP Routing** selected.
2. Enter one port you want to use in the **TCP Routing Ports** field.
3. Deploy PAS.
4. Use the Routing API to add all desired TCP ports by following the instructions in the [Modify your TCP ports](#) section of the *Enabling TCP Routing* topic. When using the Routing API, you can include a comma separated list of ports.

Loggregator Component Horizontal Scaling Thresholds

Above approximately 40 Doppler instances and 25 Traffic Controller instances, horizontal scaling is no longer useful for improving Loggregator Firehose performance. To improve performance, increase CPU resources for the existing Doppler and Traffic Controller instances to add vertical scale.

The Syslog Adapter now enforces a hard limit on how many application syslog drains it can service, therefore it is important to follow the [scaling recommendations](#) to ensure that all syslog drains can be serviced.

Apps Manager SSL Validation Cannot Be Disabled in v2.2.12–v2.2.15

In v2.2.12–v2.2.15, Apps Manager ignores the **Disable SSL certificate verification for this environment** PAS tile setting. For environments using SSL certificates signed by an untrusted certificate authority (CA), this may cause Apps Manager to show no content.

To resolve this issue, see [Apps Manager shows no content due to SSL validation issue](#).

Apps Manager Only Allows One Intermediate Certificate Authority in v2.2.12–v2.2.14

In v2.2.12, v2.2.13, and v2.2.14, Apps Manager does not accept SSL certificates that have a signing chain with more than one intermediate certificate authority between the SSL certificate and the root certificate authority. This includes certificates from backend services such as the Cloud Controller API.

If there is more than one intermediate certificate authority, not counting the root certificate authority, the following happens:

- Apps Manager does not show content.
- The logs for Apps Manager include the text `certificate chain too long`.

If you must use an SSL certificate chain with more than one intermediate certificate authority in your environment, contact Pivotal Support to discuss options for working around this issue.

Cloud Controller Error Causes PCF Upgrade to Fail

With buildpacks now having stack associations, additional validation must be added while upgrading to PAS v2.2 and later. This can generate a new

`StacklessAndStackfulMatchingBuildpacksError` error in the post-start scripts.

For more information and instructions for fixing this error, see [Pivotal Cloud Foundry upgrade fails with a StacklessAndStackfulMatchingBuildpacksExistError Cloud Controller Error](#) in the Pivotal Knowledge Base.

PAS for Windows v2.2 Release Notes

This topic contains release notes for Pivotal Application Service (PAS) for Windows.

How to Upgrade

The PAS for Windows v2.2 tile is available with the release of Pivotal Cloud Foundry (PCF) v2.2. To use the PAS for Windows v2.2 tile, you must install Ops Manager v2.2 or later and PAS v2.2 or later.

Releases

2.2.9

- Bump windows2016 stemcell to version 1709.19
- Bump hwc-offline-buildpack to version 3.1.6
- Bump windows2016fs-release to version 2.2.0

| Component | Version |
|-----------------------|---------|
| windows2016 stemcell | 1709.19 |
| consul | 195 |
| diego | 2.8.7 |
| event-log | 0.7.0 |
| garden-runc | 1.16.8 |
| hwc-offline-buildpack | 3.1.6 |
| loggregator | 102.8 |
| winc | 1.8.0 |
| windows-utilities | 0.10.0 |
| windows2016fs-release | 2.2.0 |

2.2.8

- **[Feature]** Operators can provide trusted certs in OpsMgr for .NET apps to use automatically
- Bump hwc-offline-buildpack to version 3.1.5
- Bump winc to version 1.8.0

| Component | Version |
|-----------------------|---------|
| windows2016 stemcell | 1709.17 |
| consul | 195 |
| diego | 2.8.7 |
| event-log | 0.7.0 |
| garden-runc | 1.16.8 |
| hwc-offline-buildpack | 3.1.5 |
| loggregator | 102.8 |
| winc | 1.8.0 |
| windows-utilities | 0.10.0 |
| windows2016fs-release | 2.0.0 |

2.2.7

- Bump windows2016 stemcell to version 1709.17
- Bump diego to version 2.8.7
- Bump garden-runc to version 1.16.8
- Bump hwc-offline-buildpack to version 3.1.4
- Bump windows2016fs-release to version 2.0.0

| Component | Version |
|-----------------------|---------|
| windows2016 stemcell | 1709.17 |
| consul | 195 |
| diego | 2.8.7 |
| event-log | 0.7.0 |
| garden-runc | 1.16.8 |
| hwc-offline-buildpack | 3.1.4 |
| loggregator | 102.8 |
| winc | 1.7.0 |
| windows-utilities | 0.10.0 |
| windows2016fs-release | 2.0.0 |

2.2.6

- Bump windows2016 stemcell to version 1709.15
- Bump hwc-offline-buildpack to version 3.1.2
- Bump loggregator to version 102.8
- Bump windows2016fs-release to version 1.12.0

| Component | Version |
|-----------------------|---------|
| windows2016 stemcell | 1709.15 |
| consul | 195 |
| diego | 2.8.4 |
| event-log | 0.7.0 |
| garden-runc | 1.16.1 |
| hwc-offline-buildpack | 3.1.2 |
| loggregator | 102.8 |
| winc | 1.7.0 |
| windows-utilities | 0.10.0 |
| windows2016fs-release | 1.12.0 |

2.2.5

- [Security Fix] Rotate diego intermediate CA before current certificate expires
- [Feature Improvement] Operators can specify the Diego executor properties for memory usage and disk capacity in order to enable finer grained resource usage strategies.
- [Feature Improvement] Smoke tests for PASW are run as a post-deploy errand
- [Bug Fix] Fix issue that could cause application deployments to fail on some infrastructure due to incorrect MTU detection
- Bump to hwc-offline-buildpack compatible with PAS 2.2
- Bump windows2016 stemcell to version 1709.14
- Bump diego to version 2.8.4
- Bump hwc-offline-buildpack to version 3.1.1

- Bump winc to version `1.7.0`
- Bump windows2016fs-release to version `1.10.0`

| Component | Version |
|-----------------------|---------|
| windows2016 stemcell | 1709.14 |
| consul | 195 |
| diego | 2.8.4 |
| event-log | 0.7.0 |
| garden-runc | 1.16.1 |
| hwc-offline-buildpack | 3.1.1 |
| loggregator | 102.7 |
| winc | 1.7.0 |
| windows-utilities | 0.10.0 |
| windows2016fs-release | 1.10.0 |

2.2.4

- **[Security Fix]** Bump garden-runc to prevent malicious users from causing a denial of service for other apps
- **[Bug Fix]** Fix issue in loggregator where AZ names with special characters could cause metron agent job to fail
- Bump garden-runc to version `1.16.1`
- Bump hwc-offline-buildpack to version `3.0.2`
- Bump loggregator to version `102.7`
- Bump windows2016fs to version `1.8.0`
- Bump stemcell windows2016 to version `1709.13`

| Component | Version |
|-----------------------|---------|
| Stemcell | 1709.13 |
| consul | 195 |
| diego | 2.8.2 |
| event_log | 0.7.0 |
| garden-runc | 1.16.1 |
| hwc-offline-buildpack | 3.0.2 |
| loggregator | 102.7 |
| winc | 1.3.0 |
| windows2016fs | 1.8.0 |
| windows-utilities | 0.10.0 |

2.2.3

- Bump stemcell windows2016 version `1709.12`

| Component | Version |
|-----------------------|---------|
| Stemcell | 1709.12 |
| consul | 195 |
| diego | 2.8.2 |
| event_log | 0.7.0 |
| garden-runc | 1.13.3 |
| hwc-offline-buildpack | 2.3.19 |
| loggregator | 102.4 |
| | |

| Component | Version |
|-------------------|---------|
| winc | 1.3.0 |
| windows-utilities | 0.10.0 |

2.2.2

- **[Bug Fix]** Fix intermittent consul DNS issues on Windows Cells
- Bump consul to version `195`
- Bump diego to version `2.8.2`
- Bump event-log to version `0.7.0`
- Bump hwc-offline-buildpack to version `2.3.19`
- Bump loggregator to version `102.4`
- Bump stemcell windows2016 to version `1709.11`

| Component | Version |
|-----------------------|---------|
| Stemcell | 1709.11 |
| consul | 195 |
| diego | 2.8.2 |
| event_log | 0.7.0 |
| garden-runc | 1.13.3 |
| hwc-offline-buildpack | 2.3.19 |
| loggregator | 102.4 |
| winc | 1.3.0 |
| windows-utilities | 0.10.0 |

2.2.0

| Component | Version |
|---|---------|
| Stemcell | 1709.8 |
| consul | 193 |
| diego | 2.8.0 |
| event_log | 0.2 |
| garden-runc | 1.13.3 |
| hwc-offline-buildpack | 2.3.17* |
| loggregator | 102.1 |
| winc | 1.3.0 |
| windows-utilities | 0.10.0 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

New Features in PAS for Windows v2.2


New Format for Timestamps in Diego Component Logs

The timestamps in the Diego component logs are now in a format compatible with [RFC 3339](#). Log-level identifiers are also formatted as strings instead of numeric codes.

RFC 3339 timestamps are enabled by default for new v2.2 deployments. Upgrades from earlier versions retain the previous component log format with Unix epoch timestamps.

You can enable the new timestamp format for Diego logs in the PAS tile.

For more information, see the **Configure Application Containers** section of any IaaS-specific PAS configuration topic, such as [Deploying PAS on AWS](#).

 **Breaking Change:** Before enabling RFC 3339 format for Diego logs, ensure that your log aggregation system anticipates the timestamp format change. If you experience issues, you can disable RFC 3339 format in the PAS tile.

Known Issues

Deploying PAS Runtime for Windows Results in an Access is Denied Error

This rare issue can occur when you deploy the PAS Runtime for Windows v2.2.

The error reads:

```
Action Failed get_task: Task 5b085f4a-b56a-42e3-5974-f3876879397d result: Compiling package certsplitter_windows: Removing packages: Uninstalling package bundle: remove /var/vcap/data/packages/golang-windows/83bf1f4181665d2ee2c0118a56bd04764b8f56b0go\bin\go.exe: Access is denied.
```

If you encounter this error, Pivotal recommends retrying the deployment until the error does not occur.

For more information, see the Knowledge Base article [Deploying PAS for Windows Tile Results in an Access is Denied Error](#).

Consul Agent Job Does Not Prestart on Windows Diego Cells

In PAS for Windows v2.2, the `consul_agent_windows` job may fail to prestart when a Diego cell VM is created. The `Cannot index into a null array` error message typically indicates that your Diego cell VM is affected. To workaround this issue, you can recreate the VM.

PCF Isolation Segment v2.2 Release Notes

Known Issues

- **[Known Issue]** The NSX-T tile versions 2.3.1 and lower are not compatible with IST. Upcoming release NSX-T 2.3.2 will address this issue.

Releases

NOTE: BREAKING CHANGE You must upgrade to PAS 2.2.3 or greater prior to installing IST 2.2.4 or higher

2.2.15

- Bump ubuntu-trusty stemcell to version 3586.96
- Bump cflinuxfs2 to version 1.281.0

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.96 |
| cf-networking | 2.3.3 |
| cflinuxfs2 | 1.281.0 |
| consul | 195 |
| diego | 2.8.7 |
| garden-runc | 1.16.8 |
| haproxy | 8.7.0 |
| loggregator | 102.8 |
| nfs-volume | 1.2.6 |
| routing | 0.178.7 |
| silk | 2.3.4 |
| syslog | 11.3.2 |

2.2.14 ***[Feature Improvement]** Add support for TCP hitless reloads in haproxy to avoid connection reset errors ***[Feature Improvement]**
Add ability to enable/disable gorouter hairpinning * Bump ubuntu-trusty stemcell to version `3586.93` * Bump cflinuxfs2 to version `1.279.0` * Bump
routing to version `0.178.7`

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.93 |
| cf-networking | 2.3.3 |
| cflinuxfs2 | 1.279.0 |
| consul | 195 |
| diego | 2.8.7 |
| garden-runc | 1.16.8 |
| haproxy | 8.7.0 |
| loggregator | 102.8 |
| nfs-volume | 1.2.6 |
| routing | 0.178.7 |
| silk | 2.3.4 |
| syslog | 11.3.2 |

2.2.13

- Bump ubuntu-trusty stemcell to version 3586.79
- Bump cflinuxfs2 to version 1.267.0
- Bump diego to version 2.8.7

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.79 |
| cf-networking | 2.3.3 |
| cflinuxfs2 | 1.267.0 |
| consul | 195 |
| diego | 2.8.7 |
| garden-runc | 1.16.8 |
| haproxy | 8.7.0 |
| loggregator | 102.8 |
| nfs-volume | 1.2.6 |
| routing | 0.178.5 |
| silk | 2.3.4 |
| syslog | 11.3.2 |

2.2.12

- [Bug Fix] Fix concurrency bug in the Router's route pool, which could manifest as a fatal error: "Unlock of unlocked RWMutex"
- [Bug Fix] Improve garden init process to avoid edge cases that can lead to zombies
- Bump ubuntu-trusty stemcell to version 3586.71
- Bump cflinuxfs2 to version 1.261.0
- Bump garden-runc to version 1.16.8
- Bump routing to version 0.178.5

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.71 |
| cf-networking | 2.3.3 |
| cflinuxfs2 | 1.261.0 |
| consul | 195 |
| diego | 2.8.5 |
| garden-runc | 1.16.8 |
| haproxy | 8.7.0 |
| loggregator | 102.8 |
| nfs-volume | 1.2.6 |
| routing | 0.178.5 |
| silk | 2.3.4 |
| syslog | 11.3.2 |

2.2.11

- Bump ubuntu-trusty stemcell to version 3586.65
- Bump cflinuxfs2 to version 1.258.0
- Bump diego to version 2.8.5

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.65 |
| | |

| Component | Version |
|---------------|---------|
| cf-networking | 2.3.3 |
| cflinuxfs2 | 1.255.0 |
| consul | 195 |
| diego | 2.8.5 |
| garden-runc | 1.16.1 |
| haproxy | 8.7.0 |
| loggregator | 102.8 |
| nfs-volume | 1.2.6 |
| routing | 0.178.4 |
| silk | 2.3.4 |
| syslog | 11.3.2 |

2.2.10

- Bump ubuntu-trusty stemcell to version 3586.60
- Bump cflinuxfs2 to version 1.255.0
- Bump loggregator to version 102.8
- Bump silk to version 2.3.4

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.60 |
| cf-networking | 2.3.3 |
| cflinuxfs2 | 1.255.0 |
| consul | 195 |
| diego | 2.8.4 |
| garden-runc | 1.16.1 |
| haproxy | 8.7.0 |
| loggregator | 102.8 |
| nfs-volume | 1.2.6 |
| routing | 0.178.4 |
| silk | 2.3.4 |
| syslog | 11.3.2 |

2.2.9

- [Security Fix] Address leak of CF admin credentials into NFS broker bosh errand logs
- [Security Fix] Rotate diego intermediate CA before current certificate expires
- [Feature Improvement] Fix error handling to report NFS mount failures in CF application logs
- [Bug Fix] Prevent container IPs from leaking by enforcing that TCP RST messages always have the cell ip as the source ip
- Bump ubuntu-trusty stemcell to version 3586.57
- Bump cf-networking to version 2.3.3
- Bump cflinuxfs2 to version 1.249.0
- Bump nfs-volume to version 1.2.6
- Bump silk to version 2.3.3

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.57 |
| cf-networking | 2.3.3 |
| cflinuxfs2 | 1.249.0 |
| consul | 195 |

| Component | Version |
|-------------|---------|
| diego | 2.8.4 |
| garden-runc | 1.16.1 |
| haproxy | 8.7.0 |
| loggregator | 102.7 |
| nfs-volume | 1.2.6 |
| routing | 0.178.4 |
| silk | 2.3.3 |
| syslog | 11.3.2 |

2.2.8

- **[Feature Improvement]** Improve router pruning behavior when route integrity is enabled
- Bump ubuntu-trusty stemcell to version 3586.52
- Bump cflinuxfs2 to version 1.245.0
- Bump routing to version 0.178.4

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.52 |
| cf-networking | 2.3.1 |
| cflinuxfs2 | 1.245.0 |
| consul | 195 |
| diego | 2.8.4 |
| garden-runc | 1.16.1 |
| haproxy | 8.7.0 |
| loggregator | 102.7 |
| nfs-volume | 1.2.3 |
| routing | 0.178.4 |
| silk | 2.3.0 |
| syslog | 11.3.2 |

2.2.7

- **[Bug Fix]** Logs marked as “DEBUG” are no longer forwarded by default
- Bump ubuntu-trusty stemcell to version 3586.46
- Bump cf-networking to version 2.3.1
- Bump cflinuxfs2 to version 1.242.0
- Bump diego to version 2.8.4

| Component | Version |
|------------------------|---------|
| ubuntu-trusty stemcell | 3586.46 |
| cf-networking | 2.3.1 |
| cflinuxfs2 | 1.242.0 |
| consul | 195 |
| diego | 2.8.4 |
| garden-runc | 1.16.1 |
| haproxy | 8.7.0 |
| loggregator | 102.7 |
| nfs-volume | 1.2.3 |
| | |

| Component | Version |
|-----------|---------|
| routing | 0.178.3 |
| silk | 2.3.0 |
| syslog | 11.3.2 |

2.2.6

- **[Security Fix]** Bump garden-runc to prevent malicious users from causing a denial of service for other apps
- **[Bug Fix]** Fix unsafe logic in NFS unmount and drain code that may lead to deletion of files on remote NFS shares.
- **[Bug Fix]** Fix issue in loggregator where AZ names with special characters could cause metron agent job to fail
- **[Bug Fix]** Fix parse error for syslog rules when iptables logging is enabled
- Bump cflinuxfs2 to version 1.238.0
- Bump garden-runc to version 1.16.1
- Bump loggregator to version 102.7
- Bump nfs-volume to version 1.2.3
- Bump stemcell ubuntu-trusty to version 3586.43

| Component | Version |
|---|---------|
| stemcell | 3586.43 |
| cf-networking | 2.3.0 |
| cflinuxfs2 | 1.238.0 |
| consul | 195 |
| diego | 2.8.2 |
| garden-runc | 1.16.1 |
| haproxy | 8.7.0 |
| loggregator | 102.7 |
| nfs-volume | 1.2.3 |
| routing | 0.178.3 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.5

- Bump cflinuxfs2 to version 1.235.0
- Bump routing to version 0.178.3
- Bump stemcell ubuntu-trusty to version 3586.42

| Component | Version |
|---|---------|
| stemcell | 3586.42 |
| cf-networking | 2.3.0 |
| cflinuxfs2 | 1.235.0 |
| consul | 195 |
| diego | 2.8.2 |
| garden-runc | 1.13.3 |
| haproxy | 8.7.0 |
| loggregator | 102.4 |
| nfs-volume | 1.2.2 |
| routing | 0.178.3 |
| silk | 2.3.0 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

| Component | Version |
|---|---------|
| syslog | 11.3.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.4

NOTE: BREAKING CHANGE You must upgrade to PAS 2.2.3 or greater prior to installing IST 2.2.4 or higher

- **[Bug Fix]** Applications can use internal service discovery
- Bump cflinuxfs2 to version [1.228.0](#)
- Bump diego to version [2.8.2](#)
- Bump nfs-volume to version [1.2.2](#)
- Bump routing to version [0.178.2](#)
- Bump stemcell to version [3586.27](#)

| Component | Version |
|---|---------|
| stemcell | 3586.27 |
| cf-networking | 2.3.0 |
| cflinuxfs2 | 1.228.0 |
| consul | 195 |
| diego | 2.8.2 |
| garden-runc | 1.13.3 |
| haproxy | 8.7.0 |
| loggregator | 102.4 |
| nfs-volume | 1.2.2 |
| routing | 0.178.2 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

2.2.3

- **[Bug Fix]** Fix TLS pruning behavior for Gorouter
- Bump diego to version [2.8.1](#)
- Bump loggregator to version [102.4](#)
- Bump routing to version [0.178.1](#)
- Bump stemcell to version [3586.26](#)

| Component | Version |
|---|---------|
| stemcell | 3586.26 |
| cf-networking | 2.3.0 |
| cflinuxfs2 | 1.227.0 |
| consul | 195 |
| diego | 2.8.0 |
| garden-runc | 1.13.3 |
| haproxy | 8.7.0 |
| loggregator | 102.4 |
| nfs-volume | 1.2.1 |
| routing | 0.178.1 |
| silk | 2.3.0 |
| * Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior. | |

| Component | Version |
|--|---------|
| syslog | 11.3.2 |
| <i>* Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior.</i> | |

2.2.2

- **[Feature Improvement]** Add ability to configure HAproxy client certificate verification
- Bump cflinuxfs2 version [1.227.0](#)

| Component | Version |
|--|---------|
| Stemcell | 3586.24 |
| cf-networking | 2.3.0 |
| cflinuxfs2 | 1.227.0 |
| consul | 195 |
| diego | 2.8.0 |
| garden-runc | 1.13.3 |
| haproxy | 8.7.0 |
| loggregator | 102.2 |
| nfs-volume | 1.2.1 |
| routing | 0.178.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| <i>* Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior.</i> | |

2.2.1

- **[Security Fix]** Bump loggregator release for CVE-2018-1268 and CVE-2018-1269
- **[Bug Fix]** bump consul to v195
 - Includes go lang 1.9.7, removes go lang 1.8.*.
 - Deploying v193 could fail on some deployments due to a conflict with other tiles that compiled the release differently
 - Fixes intermittent consul DNS issues on Windows Cells
- Bump cflinuxfs2 to version [1.223.0](#)
- Bump consul to version [195](#)
- Bump loggregator to version [102.2](#)

| Component | Version |
|--|---------|
| Stemcell | 3586.24 |
| cf-networking | 2.3.0 |
| cflinuxfs2 | 1.223.0 |
| consul | 195 |
| diego | 2.8.0 |
| garden-runc | 1.13.3 |
| haproxy | 8.7.0 |
| loggregator | 102.2 |
| nfs-volume | 1.2.1 |
| routing | 0.178.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| <i>* Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior.</i> | |

2.2.0

| Component | Version |
|--|---------|
| Stemcell | 3586.24 |
| cf-networking | 2.3.0 |
| cflinuxfs2 | 1.220.0 |
| consul | 194 |
| diego | 2.8.0 |
| garden-runc | 1.13.3 |
| haproxy | 8.7.0 |
| loggregator | 102.1 |
| nfs-volume | 1.2.1 |
| routing | 0.178.0 |
| silk | 2.3.0 |
| syslog | 11.3.2 |
| <i>* Components marked with an asterisk have been patched to resolve security vulnerabilities or fix component behavior.</i> | |

About PCF Isolation Segment

The PCF Isolation Segment v2.2 tile is available for installation with PCF v2.2.

[Isolation segments](#) provide dedicated pools of resources where you can deploy apps and isolate workloads. Using isolation segments separates app resources as completely as if they were in different CF deployments but avoids redundant management and network complexity.

For more information about using isolation segments in your deployment, see the [Managing Isolation Segments](#) topic.

How to Install

The procedure for installing PCF Isolation Segment v2.2 is documented in the [Installing PCF Isolation Segment](#) topic.

To install a PCF Isolation Segment, you must first install PCF v2.2.

New Features in PCF Isolation Segment v2.2

Gorouter Logging Changes for GDPR Compliance

Operators can now disable logging of client IP addresses in the Gorouter to comply with the General Data Protection Regulation (GDPR).

This setting, **Logging of Client IPs in CF Router**, is configured in the **Networking** pane of the PCF Isolation Segment tile. You can disable logging of the `X-Forwarded-For` HTTP header only or of both the source IP address and the `X-Forwarded-For` HTTP header. By default, the **Log client IPs** option is set in PCF Isolation Segment.

For more information about configuring the **Logging of Client IPs in CF Router** field, see [Networking](#) in the *Installing PCF Isolation Segment* topic.


New Format for Timestamps in Diego Component Logs

The timestamps in the Diego component logs are now in a format compatible with [RFC 3339](#). Log-level identifiers are also formatted as strings instead of numeric codes.

RFC 3339 timestamps are enabled by default for new v2.2 deployments. Upgrades from earlier versions retain the previous component log format with Unix epoch timestamps.

You can enable the new timestamp format for Diego logs in the Pivotal Application Service (PAS) tile.

For more information, see the **Configure Application Containers** section of any IaaS-specific PAS configuration topic, such as [Deploying PAS on AWS](#).

 **Breaking Change:** Before enabling RFC 3339 format for Diego logs, ensure that your log aggregation system anticipates the timestamp format change. If you experience issues, you can disable RFC 3339 format in the PAS tile.

DNS Search Domains

PCF Isolation Segment allows you to configure the DNS search domains used in containers by entering a comma-separated list.

For more information, see the **DNS Search Domains** configuration described in the **Container Networking** section of any IaaS-specific PAS configuration topic, such as [Deploying PAS on AWS](#).

Known issues

NSX-T v2.3.1 and Earlier Not Compatible with PCF Isolation Segment

The NSX-T tiles v2.3.1 and earlier are not compatible with PCF Isolation Segment. The Gorouters in an Isolation Segment are not given access in the firewall rules for NSX-T v2.3.1 and earlier, which prevents them from communicating with apps.

NSX-T v2.3.2 and later give access to the Gorouters in an Isolation Segment, and thus are compatible with PCF Isolation Segment.

About Advanced Features

The Advanced Features section of the PCF Isolation Segment v2.2 tile includes new functionality that may have certain constraints.

Although these features are fully supported, Pivotal recommends caution when using them in production.


Stemcell Release Notes

This topic provides an overview of the Stemcell versions used by Pivotal Cloud Foundry (PCF).

Stemcells are available for download on Pivotal Network. Once downloaded, you can upload them to your deployment using the **Stemcell** configuration pane of a given tile or by navigating to the **Stemcell Library** page in Ops Manager v2.1 or later.

Before you upgrade PCF, always verify that any tiles that you have installed, either from Pivotal or a partner, are compatible with the version of PCF you are deploying and its supported stemcells. For more information on checking PCF and stemcell compatibility, see [Tile Compatibility](#) in the Upgrade Checklist.

To find out which stemcell version is used by which tile version, check the release notes or the Pivotal Network download page for the tile.

 **Note:** A stemcell is a versioned OS image that BOSH uses to create VMs for the BOSH Director, Pivotal Application Service (PAS), and other PCF Service tiles, such as MySQL for PCF. For more information, see [What is a Stemcell?](#) in the BOSH documentation.

Ubuntu Linux Stemcell Lines

This section lists Linux-based stemcells used in Pivotal Cloud Foundry.

Trusty Stemcells

Each stemcell line has a corresponding release notes section. See the links below:

- [Stemcell 3586.x Release Notes](#)
- [Stemcell 3541.x Release Notes](#)
- [Stemcell 3468.x Release Notes](#)
- [Stemcell 3445.x Release Notes](#)
- [Stemcell 3421.x Release Notes](#)
- [Stemcell 3363.x Release Notes](#)

Trusty End-of-Support

Ubuntu 14.04 LTS (Trusty) stemcells are reaching end-of-support in April 2019. Starting in September 2018, Pivotal and its partners will begin releasing product tiles for PCF that support Ubuntu 16.04 LTS (Xenial) stemcells instead. Using supported stemcells is necessary to avoid exposure to security vulnerabilities.

Xenial Stemcells

Each stemcell line has a corresponding release notes section. See the links below:

- [Stemcell 97.x Release Notes](#)
- [Stemcell 87.x Release Notes](#)
- [Stemcell 81.x Release Notes](#)
- [Stemcell 60.x Release Notes](#)
- [Stemcell 50.x Release Notes](#)
- [Stemcell 40.x Release Notes](#)

Add-on Support for Xenial Stemcells

If you are using any of the following PCF add-ons, you must update the add-on and its configuration to be compatible with the Ubuntu Xenial 16.04 stemcell before deploying any tiles that use Xenial. The following add-on versions support the Xenial stemcell:

- ClamAV Add-on for PCF v1.2.22 or later. For information on how to update this add-on, see [Updating ClamAV Add-on for PCF to Run with Xenial Stemcells](#).
- File Integrity Monitoring (FIM) Add-on for PCF v1.4.28 or later. For information on how to update this add-on, see [Updating FIM Add-on for PCF to Run with Xenial Stemcells](#).
- IPSec Add-on for PCF v1.9.9 or later. For information on how to update this add-on, see [Updating IPSec Add-on for PCF to Run with Xenial Stemcells](#).

For information on which PCF tile releases now use Xenial, see [Tiles Using Xenial Stemcells in PCF](#).

Windows Stemcell Lines

This section lists Windows-based stemcells used in Pivotal Cloud Foundry. Each stemcell line has a corresponding release notes section. See the links below:

- [Stemcell 2019.x \(Windows Server version 2019\) Release Notes](#)
- [Stemcell 1803.x \(Windows Server version 1803\) Release Notes](#)
- [Stemcell 1709.x \(Windows Server version 1709\) Release Notes](#)
- [Stemcell 1200.x \(Windows2012R2\) Release Notes](#)

Stemcell (Linux) Release Notes

This topic includes release notes for Linux stemcells used with Pivotal Cloud Foundry (PCF).

Xenial Stemcells

The following sections describe each Xenial stemcell release.

315.x

This section includes release notes for the 315 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

315.41

✔ Available in Pivotal Network

Release Date: June 17, 2019

CVE fixes for <https://usn.ubuntu.com/4017-1/> [↗](#)

250.x

This section includes release notes for the 250 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

250.63

✔ Available in Pivotal Network

Release Date: June 17, 2019

CVE fixes for <https://usn.ubuntu.com/4017-1/> [↗](#)

250.56

✔ Available in Pivotal Network

Release Date: May 22, 2019

USN 3977-2

250.29

✔ Available in Pivotal Network

Release Date: April 08, 2019

Periodic stemcell bump (Apr 9, 2019)

250.25

✔ Available in Pivotal Network

Release Date: March 25, 2019

Periodic stemcell bump (Mar 26, 2019)

250.23

✔ Available in Pivotal Network

Release Date: March 21, 2019

Periodic stemcell bump (Mar 22, 2019)

250.21

✔ Available in Pivotal Network

Release Date: March 12, 2019

Periodic stemcell bump (Mar 15, 2019)

250.17

✔ Available in Pivotal Network

Release Date: February 25, 2019

Periodic stemcell bump (Mar 06, 2019)

250.9

Release Date: February 12, 2019

Periodic Ubuntu Xenial stemcell bump (Feb 13, 2019)

250.4

Release Date: January 29, 2019

First published xenial 250. stemcell.

170.x

This section includes release notes for the 170 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

170.82

✔ Available in Pivotal Network

Release Date: June 17, 2019

CVE fixes for <https://usn.ubuntu.com/4017-1/> [↗](#)

170.48

✔ Available in Pivotal Network

Release Date: April 08, 2019

Periodic stemcell bump (Apr 8, 2019)

170.45

✔ Available in Pivotal Network

Release Date: March 25, 2019

Periodic stemcell bump (Mar 26, 2019)

170.43

Release Date: March 21, 2019

Periodic stemcell bump (Mar 22, 2019)

170.39

✔ Available in Pivotal Network

Release Date: March 11, 2019

Periodic stemcell bump (Mar 15, 2019)

170.38

✔ Available in Pivotal Network

Release Date: February 25, 2019

Periodic stemcell bump (Mar 06, 2019)

170.30

✔ Available in Pivotal Network

Release Date: February 12, 2019

Periodic Ubuntu Xenial stemcell bump (Feb 12, 2019)

170.25

✔ Available in Pivotal Network

Release Date: January 28, 2019

Periodic Ubuntu Xenial stemcell bump (Jan 28, 2019)

170.24

✔ Available in Pivotal Network

Release Date: January 23, 2019

Addresses “USN-3866-1: Ghostscript vulnerability”

170.23

✔ Available in Pivotal Network

Release Date: January 22, 2019

Addresses “USN-3863-1: APT vulnerability”

170.21

Release Date: January 15, 2019

Periodic Ubuntu Xenial stemcell bump (Jan 15, 2019)

170.19

✔ Available in Pivotal Network

Release Date: January 11, 2019

Addresses “USN-3855-1: systemd vulnerabilities”

170.15

✔ Available in Pivotal Network

Release Date: December 20, 2018

Periodic Ubuntu Xenial stemcell bump (Dec 26, 2018)

170.14

✔ Available in Pivotal Network

Release Date: December 17, 2018

Periodic Ubuntu Xenial stemcell bump (Dec 17, 2018)

170.13

Release Date: December 11, 2018

Fixes

- *Google:* hostname should always be BOSH Agent ID ([#57](#), [#162225262](#))

170.12

Release Date: December 04, 2018

Periodic Ubuntu Xenial stemcell bump (Dec 05, 2018)

170.9

Release Date: November 19, 2018

Periodic Ubuntu Xenial stemcell bump (Nov 19, 2018)

170.6

Release Date: November 15, 2018

Includes updates to address:

- [USN-3820-2](#) [↗](#): Linux kernel (HWE) vulnerabilities

170.5

Release Date: November 05, 2018

Periodic Ubuntu Xenial stemcell bump (Nov 05, 2018)

97.x

This section includes release notes for the 97 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

97.113

✔ Available in Pivotal Network

Release Date: June 17, 2019

CVE fixes for <https://usn.ubuntu.com/4017-1/> [↗](#)

97.74

✔ Available in Pivotal Network

Release Date: April 08, 2019

Periodic stemcell bump (Apr 8, 2019)

97.71

✔ Available in Pivotal Network

Release Date: March 25, 2019

Periodic stemcell bump (Mar 26, 2019)

97.67

✔ Available in Pivotal Network

Release Date: March 15, 2019

Periodic stemcell bump (Mar 22, 2019)

97.66

✔ Available in Pivotal Network

Release Date: March 11, 2019

Periodic stemcell bump (Mar 15, 2019)

97.65

✔ Available in Pivotal Network

Release Date: February 25, 2019

Periodic stemcell bump (Mar 06, 2019)

97.57

✔ Available in Pivotal Network

Release Date: February 12, 2019

Periodic Ubuntu Xenial stemcell bump (Feb 13, 2019)

97.53

✔ Available in Pivotal Network

Release Date: January 28, 2019

Periodic Ubuntu Xenial stemcell bump (Jan 28, 2019)

97.52

✔ Available in Pivotal Network

Release Date: January 23, 2019

Addresses “USN-3866-1: Ghostscript vulnerability”

97.51

✔ Available in Pivotal Network

Release Date: January 22, 2019

Addresses “USN-3863-1: APT vulnerability”

97.49

Release Date: January 15, 2019

Periodic Ubuntu Xenial stemcell bump (Jan 15, 2019)

97.47

✔ Available in Pivotal Network

Release Date: January 11, 2019

Addresses “USN-3855-1: systemd vulnerabilities”

97.43

✔ Available in Pivotal Network

Release Date: December 20, 2018

Periodic Ubuntu Xenial stemcell bump (Dec 26, 2018)

97.42

✔ Available in Pivotal Network

Release Date: December 17, 2018

Periodic Ubuntu Xenial stemcell bump (Dec 17, 2018)

97.41

✔ Available in Pivotal Network

Release Date: December 11, 2018

- *Google*: hostname should always be BOSH Agent ID ([#57](#), [#162225262](#))
- Unpin rsyslog (was v8.22; backported from 170.x; [#162514665](#))
- Periodic Ubuntu Xenial updates

97.39

✔ Available in Pivotal Network

Release Date: December 04, 2018

Periodic Ubuntu Xenial stemcell bump (Dec 05, 2018)

97.34

✔ Available in Pivotal Network

Release Date: November 19, 2018

Periodic Ubuntu Xenial stemcell bump (Nov 19, 2018)

97.33

✔ Available in Pivotal Network

Release Date: November 15, 2018

Includes updates to address:

- [USN-3820-2](#): Linux kernel (HWE) vulnerabilities

97.32

✔ Available in Pivotal Network

Release Date: November 05, 2018

Periodic Ubuntu Xenial stemcell bump (Nov 08, 2018)

This stemcell addresses a bug introduced in the 97.31 release. The bug impacts AWS light stemcell users only.

97.31

✔ Available in Pivotal Network

Release Date: November 05, 2018

Do not use - this release has a bug that impacts the light stemcells Periodic Ubuntu Xenial stemcell bump (Nov 05, 2018)

97.22

Release Date: October 04, 2018

Addresses “USN-3777-2: Linux kernel (HWE) vulnerabilities” (Oct 04, 2018)

97.19

✔ Available in Pivotal Network

Release Date: October 02, 2018

(Oct 02, 2018)

97.18

✔ Available in Pivotal Network

Release Date: September 24, 2018

Periodic Ubuntu Xenial stemcell bump (Sep 25, 2018)

97.17

✔ Available in Pivotal Network

Release Date: September 18, 2018

Fixes mounting persistent disk issue with bosh-agent. (Sep 19, 2018)

97.16

✔ Available in Pivotal Network

Release Date: September 10, 2018

Periodic Ubuntu Xenial stemcell bump (Sep 11, 2018)

97.15

✔ Available in Pivotal Network

Release Date: August 27, 2018

Bump Ubuntu Xenial stemcells for “USN-3756-1: Intel Microcode vulnerabilities”

97.12

✔ Available in Pivotal Network

Release Date: August 14, 2018

Bump Ubuntu Xenial stemcells for “USN-3740-2: Linux kernel (HWE) vulnerabilities”

97.10

Release Date: August 13, 2018

Periodic Ubuntu Xenial stemcell bump (Aug 14, 2018)

97.5

Release Date: August 08, 2018

Bump Ubuntu Xenial stemcells for “USN-3732-2: Linux kernel (HWE) vulnerability”

97.3

Release Date: July 30, 2018

Periodic Ubuntu Xenial stemcell bump (July 31, 2018)

87.x

This section includes release notes for the 87 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

87.4

Release Date: July 16, 2018

Periodic Ubuntu Xenial stemcell bump (July 16, 2018)

87.3

Release Date: July 11, 2018

Periodic Ubuntu Xenial stemcell bump (July 12, 2018)

87

Release Date: July 02, 2018

Periodic Ubuntu Xenial stemcell bump (July 2, 2018)

81.x

This section includes release notes for the 81 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

81

Release Date: June 19, 2018

- Periodic Ubuntu Xenial stemcell bump (June 18, 2018)

60.x

This section includes release notes for the 60 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

60

Release Date: June 04, 2018

- Periodic Ubuntu Xenial stemcell bump (June 4, 2018)

50.x

This section includes release notes for the 50 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

50

Release Date: May 23, 2018

- Light stemcells are available

40.x

This section includes release notes for the 40 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

40

Release Date: May 22, 2018

- First release of Ubuntu Xenial stemcells
- Notable differences from Ubuntu Trusty
 - Includes systemd instead of upstart
 - Includes 4.15 Linux Kernel instead of 4.4
 - Uses chronyd to sync time (runs as a daemon) instead of ntpdate
 - Does not include NFS utils by default

Warning: Do not *downgrade* instances from Ubuntu Xenial to Ubuntu Trusty stemcells as it may corrupt persistent disk content since Trusty stemcells may decide to use sfdisk partitioner instead of parted partitioner selected by Xenial stemcells.

7.x

This section includes release notes for the 7 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

7

Release Date: June 03, 2019

Periodic stemcell bump (Jun 4, 2019)

7

Release Date: April 08, 2019

Periodic stemcell bump (Apr 8, 2019)

7

Release Date: February 14, 2019

Periodic CentOS 7 stemcell bump (Feb 14, 2019)

7

Release Date: January 28, 2019

Periodic CentOS 7 stemcell bump (Jan 28, 2019)

7

Release Date: January 16, 2019

Periodic CentOS 7 stemcell bump (Jan 17, 2019)

Trusty Stemcells

The following sections describe each Trusty stemcell release.

3763.x

This section includes release notes for the 3763 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3763.14

Release Date: March 11, 2019

Periodic stemcell bump (Mar 14, 2019)

3763.13

Release Date: February 25, 2019

Periodic stemcell bump (Mar 08, 2019)

3586.x

This section includes release notes for the 3586 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3586.93

Release Date: March 25, 2019

Periodic stemcell bump (Mar 26, 2019)

3586.91

Release Date: March 12, 2019

Periodic stemcell bump (Mar 15, 2019)

3586.86

Release Date: February 25, 2019

Periodic stemcell bump (Mar 06, 2019)

3586.79

Release Date: February 12, 2019

Periodic Ubuntu Trusty stemcell bump (Feb 14, 2019)

3586.71

Release Date: January 28, 2019

Periodic Ubuntu Trusty stemcell bump (Jan 28, 2019)

3586.70

Release Date: January 23, 2019

Addresses “USN-3866-1: Ghostscript vulnerability” and “USN-3863-1: APT vulnerability”

3586.67

Release Date: January 14, 2019

Periodic Ubuntu Trusty stemcell bump (Jan 15, 2019)

3586.65

Release Date: December 21, 2018

Periodic Ubuntu Trusty stemcell bump (Dec 21, 2018)

3586.63

Release Date: December 19, 2018

Periodic Ubuntu Trusty stemcell bump (Dec 19, 2018)

3586.60

Release Date: December 03, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Dec 05, 2018)

3586.57

Release Date: November 19, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Nov 19, 2018)

3586.56

Release Date: November 15, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Nov 15, 2018)

3586.54

Release Date: November 05, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Nov 05, 2018)

3586.52

Release Date: October 22, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Oct 23, 2018)

3586.48

Release Date: October 08, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Oct 11, 2018)

3586.46

Release Date: October 02, 2018

Addresses “USN-3776-2: Linux kernel (Xenial HWE) vulnerabilities” (Oct 02, 2018)

3586.43

Release Date: September 24, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Sep 25, 2018)

3586.42

Release Date: September 10, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Sep 11, 2018)

3586.40

Release Date: August 27, 2018

Bump Ubuntu Trusty stemcells for “USN-3756-1: Intel Microcode vulnerabilities”

Known Issue

- On GCP, writing moderate amounts of data to a persistent disk and then migrating the disk will fail with:

Error: Timed out sending 'update_settings'. See [#159511884](#) ↗

3586.36

Release Date: August 14, 2018

Bump Ubuntu Trusty stemcells for “USN-3741-2: Linux kernel (Xenial HWE) vulnerabilities”

3586.35

Release Date: August 13, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Aug 14, 2018)

3586.27

Release Date: July 30, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (July 31, 2018)

3586.26

Release Date: July 16, 2018

Periodic Ubuntu Trusty stemcell bump (July 16, 2018)

3586.25

Release Date: July 02, 2018

- Periodic Ubuntu Trusty stemcell bump (July 2, 2018)

3586.24

Release Date: June 18, 2018

- Periodic Ubuntu Trusty stemcell bump (June 18, 2018)

3586.23

Release Date: June 13, 2018

- We are continuing to investigate GCP stemcell compatibility issue from earlier version, but we did roll back BOSH Agent to an earlier version that seems to not trigger this problem
 - Note: This build does not include fixes to recently published CVE-2018-3665

3586.18

Release Date: June 04, 2018

WARNING: We are currently investigating `unresponsive agent` issues when using the Google Cloud Platform version of this stemcell. In the meantime, please use `3586.16` when deploying to GCP.

- Periodic Ubuntu Trusty stemcell bump (June 4, 2018)

3586.16

Release Date: May 24, 2018

- Bump Ubuntu Trusty stemcells for “USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities”

TLS for Internal Blobstore Supported

For Ops Manager v2.2 and later, you can enable TLS for your internal blobstore. Make sure you configured all tiles with a stemcell v3586 or later before enabling TLS for your internal blobstore.

For more information, see [TLS for Internal Blobstore Supported](#) in the Ops Manager release notes.

3586.8

Release Date: May 21, 2018

- Periodic Ubuntu Trusty stemcell bump (May 21, 2018)

3586.7

Release Date: May 09, 2018

- Bump Ubuntu Trusty stemcells for “USN-3641-1: Linux kernel vulnerabilities”

3586.5

Release Date: May 08, 2018

- Bump s3cli to include AliCloud support
- Bump bosh-agent
 - Support network aliases (used by Softlayer CPI)
 - Support static routes for networks (used by Softlayer CPI)
 - Support iSCSI for persistent disks (used by Softlayer CPI)
 - Use parted when GPT partitions are detected
 - Refactor retryable strategy usages

3541.x

This section includes release notes for the 3541 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3541.65

Release Date: December 07, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Dec 07, 2018)

3541.64

Release Date: December 03, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Dec 05, 2018)

3541.61

Release Date: November 19, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Nov 19, 2018)

3541.60

Release Date: November 15, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Nov 15, 2018)

3541.57

Release Date: October 22, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Oct 23, 2018)

3541.54

Release Date: October 08, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Oct 11, 2018)

3541.52

Release Date: October 02, 2018

Addresses “USN-3776-2: Linux kernel (Xenial HWE) vulnerabilities” (Oct 02, 2018)

3541.49

Release Date: September 24, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Sep 25, 2018)

3541.48

Release Date: September 10, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Sep 11, 2018)

3541.46

Release Date: August 27, 2018

Bump Ubuntu Trusty stemcells for “USN-3756-1: Intel Microcode vulnerabilities”

3541.44

Release Date: August 14, 2018

Bump Ubuntu Trusty stemcells for “USN-3741-2: Linux kernel (Xenial HWE) vulnerabilities”

3541.43

Release Date: August 13, 2018

Periodic Ubuntu Trusty/CentOS stemcell bump (Aug 14, 2018)

3541.37

Release Date: July 30, 2018

Periodic Ubuntu Trusty stemcell bump (July 31, 2018)

3541.36

Release Date: July 16, 2018

Periodic Ubuntu Trusty stemcell bump (July 16, 2018)

3541.35

Release Date: July 02, 2018

- Periodic Ubuntu Trusty stemcell bump (July 2, 2018)

3541.34

Release Date: June 18, 2018

- Periodic Ubuntu Trusty stemcell bump (June 18, 2018)

3541.31

Release Date: June 04, 2018

- Periodic Ubuntu Trusty stemcell bump (June 4, 2018)

3541.25

Release Date: May 09, 2018

- Bump Ubuntu Trusty stemcells for “USN-3641-1: Linux kernel vulnerabilities”

3541.30

Release Date: May 23, 2018

- Bump Ubuntu Trusty stemcells for “USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities”

3541.26

Release Date: May 21, 2018

- Periodic Ubuntu Trusty stemcell bump (May 21, 2018)

3541.24

Release Date: May 07, 2018

- Ubuntu Trusty stemcells periodic update (May 7, 2018)

3541.12

Release Date: April 06, 2018

- Bump Ubuntu Trusty stemcells for USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities

3541.10

Release Date: March 26, 2018

- Periodic Ubuntu and CentOS stemcell bump (March 26/27, 2018)

3541.9

Release Date: March 12, 2018

- Periodic Ubuntu and CentOS stemcell bump (March 12, 2018)

3541.8

Release Date: March 08, 2018

- Bump bosh-agent to 2.67.1
 - Agent will now respect previously set permissions and owner on `sys/run`, `sys/log` and data job directories
 - This should fix stemcell compatibility with Diego/Garden if Agent restarts
 - If you were using 3541.x stemcell for any of your deployments, it's recommended to update your deployments to this version before updating Director since that would cause Agent restart

3541.5

Release Date: February 22, 2018

- Bump Ubuntu Trusty stemcells for USN-3582-2: Linux kernel (Xenial HWE) vulnerabilities

3541.4

Release Date: February 14, 2018

- Rolled back custom umask configuration as we found out it was different in some cases (depends on how processes were started)
 - Hardening of `/var/vcap/jobs/*` is still applied by the agent

3541.2

Release Date: February 08, 2018

- [breaking] Set default umask to 077 and further harden several `/var/vcap/*` directories
 - Note that you may have to change your release to adapt to this change
- [breaking] Renamed `/var/vcap/bosh/bin/ntpdate` to `/var/vcap/bosh/bin/sync-time`
- [breaking] Stop forwarding SSH events to bosh-agent
 - Agent no longer receives and forwards such events to HM. This should remove a lot of noisy generated by releases that expect a lot of SSH sessions (eg Gitlab). This information will continue to be available in logs forwarded to remote destinations (and locally `/var/log/auth.log`).
- Fixes `env.bosh.swap_size: 0` to work on more clouds (including GCP)

Misc

- Order stemcell tarballs so that upload-stemcell command can execute faster
- Generate `packages.txt` within stemcell tarball that includes list of installed packages (previously known under different name)

3469.x

This section includes release notes for the 3469 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3469.1

Release Date: February 27, 2018

- Stemcell produced for testing rsyslog bump to the latest version
 - Unless testing rsyslog, use 3468.x or 3541.x stemcell lines

3468.x

This section includes release notes for the 3468 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3468.78

Release Date: October 22, 2018

Periodic Ubuntu Trusty stemcell bump (Oct 23, 2018)

3468.75

Release Date: October 08, 2018

Periodic Ubuntu Trusty stemcell bump (Oct 11, 2018)

3468.73

Release Date: October 02, 2018

Addresses “USN-3776-2: Linux kernel (Xenial HWE) vulnerabilities” (Oct 02, 2018)

3468.71

Release Date: September 24, 2018

Periodic Ubuntu Trusty stemcell bump (Sep 25, 2018)

3468.69

Release Date: September 10, 2018

Periodic Ubuntu Trusty stemcell bump (Sep 11, 2018)

3468.67

Release Date: August 27, 2018

Bump Ubuntu Trusty stemcells for “USN-3756-1: Intel Microcode vulnerabilities”

3468.64

Release Date: August 14, 2018

Bump Ubuntu Trusty stemcells for “USN-3741-2: Linux kernel (Xenial HWE) vulnerabilities”

3468.63

Release Date: August 13, 2018

Periodic Ubuntu Trusty stemcell bump (Aug 14, 2018)

3468.55

Release Date: July 30, 2018

Periodic Ubuntu Trusty stemcell bump (July 31, 2018)

3468.54

Release Date: July 16, 2018

Periodic Ubuntu Trusty stemcell bump (July 16, 2018)

3468.53

Release Date: July 02, 2018

- Periodic Ubuntu Trusty stemcell bump (July 2, 2018)

3468.51

Release Date: June 18, 2018

- Periodic Ubuntu Trusty stemcell bump (June 18, 2018)

3468.47

Release Date: June 04, 2018

- Periodic Ubuntu Trusty stemcell bump (June 4, 2018)

3468.42

Release Date: May 09, 2018

- Bump Ubuntu Trusty stemcells for “USN-3641-1: Linux kernel vulnerabilities”

3468.46

Release Date: May 23, 2018

- Bump Ubuntu Trusty stemcells for “USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities”

3468.44

Release Date: May 21, 2018

- Periodic Ubuntu Trusty stemcell bump (May 21, 2018)

3468.41

Release Date: May 07, 2018

- Ubuntu Trusty stemcells periodic update (May 7, 2018)

3468.30

Release Date: April 06, 2018

- Bump Ubuntu Trusty stemcells for USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities

3468.28

Release Date: March 26, 2018

- Periodic Ubuntu and CentOS stemcell bump (March 26/27, 2018)

3468.27

Release Date: March 12, 2018

- Periodic Ubuntu and CentOS stemcell bump (March 12, 2018)

3468.26

Release Date: March 01, 2018

- Includes updated `ixgbevf 4.3.4`

3468.25

Release Date: February 22, 2018

- Bump Ubuntu Trusty stemcells for USN-3582-2: Linux kernel (Xenial HWE) vulnerabilities

3468.22

Release Date: February 05, 2018

- [Feb 5] Periodic stemcell bump

3468.21

Release Date: January 23, 2018

- No functional change from 3468.20, except version number

3468.20

Release Date: January 23, 2018

- Bump Ubuntu Trusty stemcells for [USN-3540-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#) (This flaw is known as Spectre.)

3468.19

Release Date: January 17, 2018

- Bump Ubuntu Trusty stemcells for USN-3534-1: GNU C Library vulnerabilities

3468.17

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-4: Linux kernel \(Xenial HWE\) regression](#) [↗](#)
- Configure vSphere stemcells to use VM hardware version 9 (requires ESXi 5.1) to be compatible with <https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html> [↗](#)

3468.16

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-2: Linux \(Xenial HWE\) vulnerability](#) [↗](#) (This flaw is known as Meltdown.)

3468.15

Release Date: December 15, 2017

- Bump Ubuntu Trusty stemcells for USN-3509-4: Linux kernel (Xenial HWE) regression

3468.13

Release Date: December 08, 2017

- Bump Ubuntu Trusty stemcell USN-3509-2: Linux kernel (Xenial HWE) vulnerabilities

3468.12

Release Date: December 06, 2017

- Bump Ubuntu Trusty stemcells for USN-3505-1: Linux firmware vulnerabilities

3468.11

Release Date: November 21, 2017

- Periodic Ubuntu stemcells update
- Includes Agent changes to support IPv6 on vSphere (manual networking)

3468.5

Release Date: October 26, 2017

- Configure `/tmp` to have sticky bit set

3468.1

Release Date: October 23, 2017

- Periodic stemcell bump

3468

Release Date: October 05, 2017

- Removed password authentication for Warden stemcells
- Various minor tweaks that were already backported to older lines

Upcoming features on this stemcell line:

- IPv6 support for vSphere

3445.x

This section includes release notes for the 3445 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3445.76

Release Date: October 22, 2018

Periodic Ubuntu Trusty stemcell bump (Oct 23, 2018)

3445.73

Release Date: October 08, 2018

Periodic Ubuntu Trusty stemcell bump (Oct 11, 2018)

3445.71

Release Date: October 02, 2018

Addresses “USN-3776-2: Linux kernel (Xenial HWE) vulnerabilities” (Oct 02, 2018)

3445.68

Release Date: September 24, 2018

Periodic Ubuntu Trusty stemcell bump (Sep 25, 2018)

3445.67

Release Date: September 10, 2018

Periodic Ubuntu Trusty stemcell bump (Sep 10, 2018)

3445.66

Release Date: August 27, 2018

Bump Ubuntu Trusty stemcells for “USN-3756-1: Intel Microcode vulnerabilities”

3445.64

Release Date: August 14, 2018

Bump Ubuntu Trusty stemcells for “USN-3741-2: Linux kernel (Xenial HWE) vulnerabilities”

3445.63

Release Date: August 13, 2018

Periodic Ubuntu Trusty stemcell bump (Aug 14, 2018)

3445.55

Release Date: July 30, 2018

Periodic Ubuntu Trusty stemcell bump (July 31, 2018)

3445.54

Release Date: July 16, 2018

Periodic Ubuntu Trusty stemcell bump (July 16, 2018)

3445.53

Release Date: July 02, 2018

- Periodic Ubuntu Trusty stemcell bump (July 2, 2018)

3445.51

Release Date: June 18, 2018

- Periodic Ubuntu Trusty stemcell bump (June 18, 2018)

3445.49

Release Date: June 04, 2018

- Periodic Ubuntu Trusty stemcell bump (June 4, 2018)

3445.48

Release Date: May 23, 2018

- Bump Ubuntu Trusty stemcells for “USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities”

3445.42

Release Date: May 01, 2018

- Ubuntu Trusty stemcells periodic update (Apr 30, 2018)

3445.46

Release Date: May 21, 2018

- Periodic Ubuntu Trusty stemcell bump (May 21, 2018)

3445.45

Release Date: May 09, 2018

- Bump Ubuntu Trusty stemcells for “USN-3641-1: Linux kernel vulnerabilities”

3445.44

Release Date: May 07, 2018

- Ubuntu Trusty stemcells periodic update (May 7, 2018)

3445.32

Release Date: April 06, 2018

- Bump Ubuntu Trusty stemcells for USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities

3445.30

Release Date: March 26, 2018

- Periodic Ubuntu Trusty stemcell bump (March 26/27, 2018)

3445.29

Release Date: March 12, 2018

- Periodic Ubuntu Trusty stemcell bump (March 12, 2018)

3445.28

Release Date: February 22, 2018

- Bump Ubuntu Trusty stemcells for USN-3582-2: Linux kernel (Xenial HWE) vulnerabilities

3445.25

Release Date: February 05, 2018

- [Feb 5] Periodic stemcell bump

3445.24

Release Date: January 23, 2018

- Bump Ubuntu Trusty stemcells for [USN-3540-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#) (This flaw is known as Spectre.)

3445.23

Release Date: January 17, 2018

- Bump Ubuntu Trusty stemcells for USN-3534-1: GNU C Library vulnerabilities

3445.22

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-4: Linux kernel \(Xenial HWE\) regression](#) [↗](#)
- Configure vSphere stemcells to use VM hardware version 9 (requires ESXi 5.1) to be compatible with <https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html> [↗](#)

3445.21

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-2: Linux \(Xenial HWE\) vulnerability](#) [↗](#) (This flaw is known as Meltdown.)

3445.19

Release Date: December 08, 2017

- Bump Ubuntu Trusty stemcell USN-3509-2: Linux kernel (Xenial HWE) vulnerabilities

3445.18

Release Date: December 06, 2017

- Bump Ubuntu Trusty stemcells for USN-3505-1: Linux firmware vulnerabilities

3445.17

Release Date: November 21, 2017

- Periodic Ubuntu stemcells update

3445.11

Release Date: September 19, 2017

- Bump Ubuntu stemcells for USN-3420-2: Linux kernel (Xenial HWE) vulnerabilities

3445.7

Release Date: August 30, 2017

- Logrotate /var/log/wtmp and utmp more aggressively
- Updated BOSH agent to include aggressive 5 minute timeout on NATS connection failure
- Set auditd rules to be mutable by default
 - Please use `auditd` job from os-conf-release to make rules immutable

3445.2

Release Date: August 16, 2017

- Bump Ubuntu stemcells for [USN-3392-2: Linux kernel \(Xenial HWE\) regression](#) [↗](#)

3445

Release Date: August 11, 2017

- Bump Ubuntu stemcells for [USN-3385-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#)
- Include gcscli for native GCS support
- Bump bosh-agent to include support for colocated errand jobs
- Fix occasional rsyslog hang on startup (as a workaround for <https://github.com/rsyslog/rsyslog/issues/1188> [↗](#))

3431.x

This section includes release notes for the 3431 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3431.13

Release Date: August 03, 2017

- Bump version (no change)

3431.11

Release Date: August 03, 2017

- Bump Ubuntu Trusty stemcells for [USN-3378-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#)
- Fix occasional rsyslog hang on startup
 - Workaround for <https://github.com/rsyslog/rsyslog/issues/1188> [↗](#)

3431.10

Release Date: July 31, 2017

- Periodic Ubuntu stemcells update

3422.x

This section includes release notes for the 3422 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3422.7

Release Date: November 22, 2017

- Test stemcell for umask changes (based on 3468.x stemcell line)

3421.x

This section includes release notes for the 3421 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3421.88

Release Date: October 08, 2018

Periodic Ubuntu Trusty stemcell bump (Oct 11, 2018)

3421.86

Release Date: October 02, 2018

Addresses “USN-3776-2: Linux kernel (Xenial HWE) vulnerabilities” (Oct 02, 2018)

3421.83

Release Date: September 24, 2018

Periodic Ubuntu Trusty stemcell bump (Sep 25, 2018)

3421.82

Release Date: September 10, 2018

Periodic Ubuntu Trusty stemcell bump (Sep 10, 2018)

3421.81

Release Date: August 27, 2018

Bump Ubuntu Trusty stemcells for “USN-3756-1: Intel Microcode vulnerabilities”

3421.79

Release Date: August 14, 2018

Bump Ubuntu Trusty stemcells for “USN-3741-2: Linux kernel (Xenial HWE) vulnerabilities”

3421.78

Release Date: August 13, 2018

Periodic Ubuntu Trusty stemcell bump (Aug 14, 2018)

3421.70

Release Date: July 30, 2018

Periodic Ubuntu Trusty stemcell bump (July 31, 2018)

3421.69

Release Date: July 16, 2018

Periodic Ubuntu Trusty stemcell bump (July 16, 2018)

3421.68

Release Date: July 02, 2018

- Periodic Ubuntu Trusty stemcell bump (July 2, 2018)

3421.66

Release Date: June 18, 2018

- Periodic Ubuntu Trusty stemcell bump (June 18, 2018)

3421.64

Release Date: June 04, 2018

- Periodic Ubuntu Trusty stemcell bump (June 4, 2018)

3421.63

Release Date: May 23, 2018

- Bump Ubuntu Trusty stemcells for “USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities”

3421.56

Release Date: May 01, 2018

- Ubuntu Trusty stemcells periodic update (Apr 30, 2018)

3421.60

Release Date: May 21, 2018

- Periodic Ubuntu Trusty stemcell bump (May 21, 2018)

3421.59

Release Date: May 09, 2018

- Bump Ubuntu Trusty stemcells for “USN-3641-1: Linux kernel vulnerabilities”

3421.58

Release Date: May 07, 2018

- Ubuntu Trusty stemcells periodic update (May 7, 2018)

3421.46

Release Date: April 06, 2018

- Bump Ubuntu Trusty stemcells for USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities

3421.44

Release Date: March 26, 2018

- Periodic Ubuntu Trusty stemcell bump (March 26/27, 2018)

3421.43

Release Date: March 12, 2018

- Periodic Ubuntu Trusty stemcell bump (March 12, 2018)

3421.42

Release Date: February 22, 2018

- Bump Ubuntu Trusty stemcells for USN-3582-2: Linux kernel (Xenial HWE) vulnerabilities

3421.39

Release Date: February 05, 2018

- [Feb 5] Periodic stemcell bump

3421.38

Release Date: January 23, 2018

- Bump Ubuntu Trusty stemcells for [USN-3540-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#) (This flaw is known as Spectre.)

3421.37

Release Date: January 17, 2018

- Bump Ubuntu Trusty stemcells for USN-3534-1: GNU C Library vulnerabilities

3421.36

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-4: Linux kernel \(Xenial HWE\) regression](#) [↗](#)
- Configure vSphere stemcells to use VM hardware version 9 (requires ESXi 5.1) to be compatible with <https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html> [↗](#)

3421.35

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-2: Linux \(Xenial HWE\) vulnerability](#) [↗](#) (This flaw is known as Meltdown.)

3421.34

Release Date: December 08, 2017

- Bump Ubuntu Trusty stemcell USN-3509-2: Linux kernel (Xenial HWE) vulnerabilities

3421.33

Release Date: December 06, 2017

- Bump Ubuntu Trusty stemcells for USN-3505-1: Linux firmware vulnerabilities

3421.32

Release Date: November 21, 2017

- Periodic Ubuntu stemcells update

3421.20

Release Date: August 16, 2017

- Bump Ubuntu stemcells for [USN-3392-2: Linux kernel \(Xenial HWE\) regression](#) [↗](#)

3421.19

Release Date: August 11, 2017

- Bump Ubuntu stemcells for [USN-3385-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#)

3421.18

Release Date: August 03, 2017

- Bump Ubuntu Trusty stemcells for [USN-3378-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#)
- Fix occasional rsyslog hang on startup
 - Workaround for <https://github.com/rsyslog/rsyslog/issues/1188> [↗](#)

3421.11

Release Date: June 29, 2017

- Bump Ubuntu stemcells for USN-3344-2: Linux kernel (Xenial HWE) vulnerabilities

3421.9

Release Date: June 21, 2017

- Bump Ubuntu stemcells for USN-3334-1: Linux kernel (Xenial HWE) vulnerabilities

3421.6

Release Date: June 09, 2017

- Bump Ubuntu stemcells for USN-3312-2 - Linux kernel vulnerabilities

3421.4

Release Date: June 01, 2017

- Bump CentOS stemcells for CESA-2017:1382 - sudo vulnerability

3421.3

Release Date: May 30, 2017

- Bump Ubuntu stemcells for USN-3304-1: Sudo vulnerability

3421

Release Date: May 22, 2017

New:

- Added `env.bosh.remove_static_libraries` (bool) to remove static libraries
 - Useful to enable this option when exporting compiled releases
- Added `env.bosh.ipv6.enable` (bool) to remove ipv6.disable kernel functionality at bootup time

Fixes:

- Fixed sysstat logging
- Fixed anacron's RANDOM_DELAY configuration

Bumps:

- Bumped s3cli v0.0.60
 - Updated aws-sdk-go to solve network timeout edge case
- Bumped davcli v0.0.19
 - Use TCP keep alive to solve network timeout edge case
- Bumped bosh-agent v0.0.35
 - Add `-v` to the Agent binary
 - Prepared `sync_dns` action to work with future Director's DNS integration

3363.x

This section includes release notes for the 3363 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3363.65

Release Date: June 18, 2018

- Periodic Ubuntu Trusty stemcell bump (July 18, 2018)

3363.64

Release Date: June 04, 2018

- Periodic Ubuntu Trusty stemcell bump (June 4, 2018)

3363.63

Release Date: May 23, 2018

- Bump Ubuntu Trusty stemcells for “USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities”

3363.62

Release Date: May 21, 2018

- Periodic Ubuntu Trusty stemcell bump (May 21, 2018)

3363.61

Release Date: May 09, 2018

- Bump Ubuntu Trusty stemcells for “USN-3641-1: Linux kernel vulnerabilities”

3363.60

Release Date: May 07, 2018

- Ubuntu Trusty stemcells periodic update (May 7, 2018)

3363.53

Release Date: April 06, 2018

- Bump Ubuntu Trusty stemcells for USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities

3363.52

Release Date: March 26, 2018

- Periodic Ubuntu Trusty stemcell bump (March 26/27, 2018)

3363.51

Release Date: March 12, 2018

- Periodic Ubuntu Trusty stemcell bump (March 12, 2018)

3363.50

Release Date: February 22, 2018

- Bump Ubuntu Trusty stemcells for USN-3582-2: Linux kernel (Xenial HWE) vulnerabilities

3363.49

Release Date: February 05, 2018

- [Feb 5] Periodic stemcell bump

3363.48

Release Date: January 23, 2018

- Bump Ubuntu Trusty stemcells for [USN-3540-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#) (This flaw is known as Spectre.)

3363.47

Release Date: January 17, 2018

- Bump Ubuntu Trusty stemcells for USN-3534-1: GNU C Library vulnerabilities

3363.46

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-4: Linux kernel \(Xenial HWE\) regression](#) [↗](#)
- Configure vSphere stemcells to use VM hardware version 9 (requires ESXi 5.1) to be compatible with <https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html> [↗](#)

3363.45

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-2: Linux \(Xenial HWE\) vulnerability](#) [↗](#) (This flaw is known as Meltdown.)

3363.44

Release Date: December 08, 2017

- Bump Ubuntu Trusty stemcell USN-3509-2: Linux kernel (Xenial HWE) vulnerabilities

3363.43

Release Date: December 06, 2017

- Bump Ubuntu Trusty stemcells for USN-3505-1: Linux firmware vulnerabilities

3363.42

Release Date: November 21, 2017

- Periodic Ubuntu stemcells update

3363.24

Release Date: May 17, 2017

- Periodic Ubuntu stemcells update

3363.22

Release Date: May 11, 2017

- Periodic Ubuntu stemcells update
- Run `cron` in BOSH Lite stemcells so that logrotation is performed

3363.20

Release Date: April 25, 2017

- Bump Ubuntu stemcells for USN-3265-2: Linux kernel (Xenial HWE) vulnerabilities

3363.19

Release Date: April 17, 2017

- Periodic bump for CentOS stemcells to include CESA-2017:0933
- Disable IPv6 through `/proc/cmdline` to eliminate possibility of listening on tcp6/udp6

3363.15

Release Date: April 05, 2017

- Bump Ubuntu stemcells for USN-3256-2: Linux kernel (HWE) vulnerability

Misc:

- Made AWS AMI backing snapshot public to support encryption of boot disks

3363.14

Release Date: March 30, 2017

- Bump Ubuntu stemcells for USN-3249-2: Linux kernel (Xenial HWE) vulnerability

3363.10

Release Date: March 08, 2017

- Bumps Ubuntu stemcells for USN-3220-2: Linux kernel (Xenial HWE) vulnerability

3363.9

Release Date: February 22, 2017

Changes: - Bumps Ubuntu stemcells for USN-3208-2: Linux kernel (Xenial HWE) vulnerabilities - Fixes excessive “out of memory” errors in kernel - <https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1655842> - Fixes regression to rsyslog by locking it down again to rsyslog 8.22.0

Agent: - Fixes Azure stemcell persistent disk formatting - Fixes Warden stemcells SSH access

3363.1

Release Date: February 15, 2017

Reported Problems: - DO NOT USE *azure* stemcell as it may cause data loss. - [Out of memory errors still exists in Kernel 4.4.0.62](#) - will be fixed around Feb 20.

Changes: - Fixes double -hvm- suffix problem for AWS Light stemcells

3363

Release Date: February 15, 2017

Reported Problems: - DO NOT USE *azure* stemcell as it may cause data loss. - [Out of memory errors still exists in Kernel 4.4.0.62](#) - will be fixed around Feb 20. - rsyslog version updated to 8.24.0, regressing on issue #1537 - AWS Light stemcell has incorrect name once imported - BOSH SSH does not work on BOSH Lite

Changes: - Add more auditd rules - Fix CentOS initramfs to load necessary kernel modules - Disable boot loader login - Increasing tcp_max_sync_backlog - Disabling any DSA host keys - Add `bosh_sshers` group and assign it to vcap user - Only allow users in `bosh_sshers` group to SSH

Agent: - Log Agent API access events in CEF format to syslog (vcap.agent topic) - Allow configuring swap size through `env.bosh.swap_size` (example: `env.bosh.swap_size: 0`) - Prepare for SHA2 releases - Allow setting fetching to work with base64 encoded user data - Do not delaycompress in logrotate

3312.x

This section includes release notes for the 3312 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3312.51

Release Date: January 23, 2018

- Bump Ubuntu Trusty stemcells for [USN-3540-2: Linux kernel \(Xenial HWE\) vulnerabilities](#) [↗](#) (This flaw is known as Spectre.)

3312.50

Release Date: January 10, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-4: Linux kernel \(Xenial HWE\) regression](#) [↗](#)
- Configure vSphere stemcells to use VM hardware version 9 (requires ESXi 5.1) to be compatible with <https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html> [↗](#)

3312.49

Release Date: January 09, 2018

- Bump Ubuntu Trusty stemcells for [USN-3522-2: Linux \(Xenial HWE\) vulnerability](#) [↗](#) (This flaw is known as Meltdown.)

3312.48

Release Date: December 08, 2017

- Bump Ubuntu Trusty stemcell USN-3509-2: Linux kernel (Xenial HWE) vulnerabilities

3312.47

Release Date: December 06, 2017

- Bump Ubuntu Trusty stemcells for USN-3505-1: Linux firmware vulnerabilities

3312.46

Release Date: November 21, 2017

- Periodic Ubuntu stemcells update

3312.17

Release Date: January 31, 2017

Reported Problems: - [Memory leak bug in Kernel 4.4.0-59](#) [↗](#)

Changes: - Periodic stemcell update

3312.15

Release Date: January 12, 2017

Reported Problems: - [Memory leak bug in Kernel 4.4.0-59](#) [↗](#)

Changes: - Periodic stemcell update

3312.12

Release Date: December 20, 2016

- Lock down rsyslog to 8.22.0 to avoid high memory usage issue <https://github.com/cloudfoundry/bosh/issues/1537> ↗

3312.9

Release Date: December 15, 2016

- Updates Azure Ubuntu stemcells to use parted partitioner to fix slow disk partitioning
 - Related issue: <https://github.com/cloudfoundry-incubator/bosh-azure-cpi-release/issues/227> ↗

3312.8

Release Date: December 14, 2016

- Bumps Ubuntu stemcells for USN-3156-1: APT vulnerability

3312.7

Release Date: December 06, 2016

- Bump Ubuntu stemcells for [USN-3151-2: Linux kernel \(Xenial HWE\) vulnerability](#) ↗

3312.6

Release Date: December 02, 2016

- Periodic stemcell update

3312.3

Release Date: November 30, 2016

- Periodic stemcell update
 - Includes [USN-3134-1](#) ↗ as requested by a community member

3312

Release Date: November 16, 2016

- Properly includes `libpam_cracklib.so` to avoid errors in `/var/log/auth.log`

3309.x

This section includes release notes for the 3309 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3309

Release Date: November 10, 2016

- Fixes persistent disk mounting on OpenStack described in [Stemcell 3308](#) ↗

3308.x

This section includes release notes for the 3308 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3308

Release Date: November 09, 2016

Reported Problems: - On OpenStack: Mounting persistent disks not working when using `config-drive: disk` while nova is configured to use a `cdrom` config-drive due to <https://github.com/cloudfoundry/bosh/issues/1503>

Fixes: - Fixes SSH key installation issue introduced in [Stemcell 3306](#)

3306.x

This section includes release notes for the 3306 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3306

Release Date: November 08, 2016

Reported Problems - `bosh-init` doesn't work with this stemcell on OpenStack and AWS due to <https://github.com/cloudfoundry/bosh/issues/1500> - Booting the stemcell image directly in you IaaS (without using BOSH/bosh-init) does no longer provision the ssh key for user `vcap`, so you need to login differently

Changes - Agent will now wait for monit to complete stop all processes before carrying on - Added google stemcells - Default `dmesg_restrict` to 1 - Disable all IPv6 configurations - Reenabled UDF kernel module for Azure - Increase `root_maxkeys` and `maxkeys` kernel configurations - Changed default hostname to `bosh-stemcell` instead of `localhost` to avoid boot problems on GCP - Lower TCP keepalive configuration by default - Mount `/var/log` directory to `/var/vcap/data/root_log` - Restrict Access to the `su` command - Add `pam_cracklib` requirements to `common-password` and `password-auth` - Enable auditing for processes that start prior to `auditd` - Set log rotation interval to 15 min in stemcell - Made ownership & permissions for `/etc/cron*` files more restrictive - Customize shell prompt to show instance name and ID - Removed floppy drives from vSphere stemcells - Removed `bosh micro` assets hence

making `bosh micro` unsupported

Misc: - Stemcells are now built through Concourse via <https://main.bosh-ci.cf-app.com/teams/main/pipelines/bosh:stemcells>

3263.x

This section includes release notes for the 3263 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3263.10

Release Date: November 03, 2016

- Updates CentOS kernel to the latest version for "Dirty COW"
 - Ubuntu stemcells were updated in previous versions at the time of Ubuntu USN updates
- Includes fix to the bosh-agent to better support 1TB+ disk partitioning

3263.8

Release Date: October 21, 2016

- Bump Ubuntu stemcells for USN-3106-2: Linux kernel (Xenial HWE) vulnerability
- Includes a fix to the bosh-agent to work more reliably with 2TB+ persistent disks

3263.7

Release Date: October 12, 2016

- Bump Ubuntu stemcells for USN-3099-2: Linux kernel (Xenial HWE) vulnerabilities

3263.5

Release Date: September 30, 2016

- Periodic bump
- Delay start of rsyslogd using systemd on CentOS

3263.4

Release Date: September 28, 2016

- google-kvm: improve the `google-*` daemon configurations
 - fixes `ssh: handshake failed` errors on boot

3263.3

Release Date: September 26, 2016

- Bumps Ubuntu stemcells for [USN-3087-2](#) (OpenSSL regression)

3263

Release Date: September 19, 2016

- Bumps Ubuntu to Linux kernel to 4.4

Based on 3262 stemcells. **Note:** OpenStack stemcells series 3263 is broken due to <https://github.com/cloudfoundry/bosh-agent/issues/98> and should not be used

3262.x

This section includes release notes for the 3262 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3262.21

Release Date: October 13, 2016

- Bump Ubuntu stemcells for USN-3099-2: Linux kernel (Xenial HWE) vulnerabilities

3262.19

Release Date: September 28, 2016

- google-kvm: improve the `google-*` daemon configurations
 - fixes `ssh: handshake failed` errors on boot

3262.16

Release Date: September 26, 2016

- Bumps Ubuntu stemcells for [USN-3087-2](#) (OpenSSL regression)

3262.15

Release Date: September 23, 2016

- Bumps Ubuntu stemcells for USN-3087-1: OpenSSL vulnerabilities

3233.x

This section includes release notes for the 3233 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3233.1

Release Date: September 27, 2016

- Bumps Ubuntu stemcells for [USN-3087-2](#) (OpenSSL regression)

USN-3522-2 Addresses Meltdown Vulnerabilities

Meltdown exploits critical vulnerabilities in modern processors. For more information about Meltdown, see the [Meltdown and Spectre Attacks](#) blog post. [USN-3522-2](#) addresses the critical vulnerability in Ubuntu associated with Meltdown.

This update may include degradations to performance if your VM's CPU and memory usage are currently at near-capacity levels. Prior to upgrading to this stemcell, monitor your PCF VM's current CPU and memory usage and scale those components if necessary. If any of your VMs are currently operating at 60% or above, Pivotal recommends scaling that VM. For more information about the performance impact of Meltdown-related stemcell patches on PCF components and guidance on scaling, see this [KB article](#).

For more information about monitoring and scaling PCF, see the [Monitoring PCF VMs from Ops Manager](#), [Key Capacity Scaling Indicators](#), and [Scaling PAS](#) topics. Performance degradation is likely to vary by workload type, IaaS, and other factors. Pivotal recommends testing your deployment thoroughly after upgrading to this stemcell.

3232.x

This section includes release notes for the 3232 line of Linux stemcells used with Pivotal Cloud Foundry (PCF).

3232.21


Release Date: September 26, 2016

- Bumps Ubuntu stemcells for [USN-3087-2](#) (OpenSSL regression)

Stemcell v1709.x (Windows Server version 1709) Release Notes

This topic includes release notes for Windows stemcells used with Pivotal Application Service for Windows (PASW).

To download a stemcell, see [Stemcells for PCF \(Windows\)](#) on Pivotal Network.

 **Note:** The Windows stemcell v1709.x line is compatible with PASW v2.1 and v2.2.

1709.21

Release Date: May 30, 2019

Security Fix

- Based on [Microsoft's guidance](#), additional fixes to protect against speculative execution side-channel vulnerabilities

1709.21

Release Date: May 23, 2019

Features

- Platform Engineers can deploy Windows Stemcells on a BOSH Director with Google Cloud Storage as their external Blobstore.
- Improved Troubleshooting of Windows VMs, with ssh enabled by default for all Windows VMs. You can still disable SSH in the PASW tile.

1709.20

Features

- Intended for use with [April 2019 Microsoft Security Updates](#)

1709.19

Features

- Includes [March 2019 Microsoft Security Updates](#).

Bug Fix

- Disabled additional configuration related to NetBios. See the Pivotal Tracker [story](#).

1709.18

Release Date: March 1, 2019

- [Patches] Included [February Patch Tuesday Microsoft Security Updates](#).

1709.17

Release Date: January 24, 2019

- [Patches] Included [January Patch Tuesday Microsoft Security Updates](#).
- Added [fix](#) for mitigating CVE-2018-3639.

1709.16

Release Date: December 24, 2018

Features

- [Patches] Included [December Patch Tuesday Microsoft Security Updates](#).
- Added the BOSH API version in the stemcell to surface more information about the compatibility of the stemcell with BOSH.

Bug Fix

- BOSH release job symlinks were not getting cleaned up when a target folder was removed. This issue is resolved.

1709.15

Release Date: November 28, 2018

Features

- [Security] Disabled use of TLS 1.0 by SSL/TLS server and client.
- [Security] Disabled RC4.
- [Security] Disabled triple-DES cipher to mitigate against Sweet32: Birthday attacks on 64-bit block ciphers in TLS.
- [Patches] Intended for use with [November 2018 Patch Tuesday Microsoft Security Updates](#).
- [New IaaS Support] Added support for AWS GovCloud.

1709.14

Release Date: October 30, 2018

Features

- Intended for use with [October 2018 Microsoft Security Updates](#).
- Disables RDP by default to improve security of the 1709 stemcells. You can still enable RDP through the PASW Tile Configuration.

Bug Fix

- Intermittent “Access denied” errors occur during the compilation phase of PASW deployments. We have added a fix to potentially resolve them.
- Fixed the Ephemeral Disk Provisioning for Azure enabling compatibility of PASW’s ephemeral disk functionality with OpsMgr on Azure.

1709.13

Release Date: September 24, 2018

Features

- Includes ephemeral disk support. This enables you to configure the size of your Windows cells in the PAS for Windows tile. For more information, see the [Configure Tile Resources](#) section in *Installing and Configuring PAS for Windows*.
- Intended for use with [September 2018](#) Microsoft Security Updates.

Bug Fix

- Previously, the `os_version` argument was mandatory during the `Invoke-Sysprep` step. The OS is now detected by default, and the `os_version` argument is optional.

Known Issues

- For Google Cloud Platform (GCP) users, a bug in PASW causes outbound connections from applications deployed on PASW with this stemcell version to fail. The resolution will come in patch versions of PASW v2.1, v2.2 and v2.3.

1709.12

Release Date: August 27, 2018

Features

- Intended for use with the [August 2018](#) Microsoft Security Updates.
- Includes an important Microsoft Security Update that provides protections against a new speculative execution side-channel vulnerability known as L1 Terminal Fault (L1TF). For more information, see [Windows Support](#).
- Compatible with the latest stable OpenSSH version, `OpenSSH_for_Windows_v7.7.2.0p1-Beta`. This version fixed the issue of OpenSSH logs filling up the disk.

Bug Fix

- Deployment of PASW fails due to “Access is Denied” error during compilation of packages on the Windows VM.

1709.11

Release Date: August 2, 2018

Features

This is the first official release of the 1709 stemcell for Amazon Web Services (AWS). PASW can be deployed on AWS going forward.

Improvements

This release incorporates [Patch Tuesday July 2018](#) security updates.

Bug Fix

Previously, when operators selected the **Encrypt Linux EBS Volumes** checkbox in the IaaS-specific configuration section of the BOSH Director tile, the deployment of PASW would fail.

This release enables operators to select the **Encrypt Linux EBS Volumes** checkbox without the deployment of PASW failing. However, only Linux VMs will be encrypted, not Windows VMs.

vSphere Stemcell

The source code and other assets are available on [GitHub](#).

1709.10

Release Date: June 27, 2018

Bug Fix

- Updated the bosh-davcli and the bosh-s3cli to the latest.
- Repairs NTP. Specifically, run time sync command via Powershell to strip quotes from NTP server. See the Pivotal Tracker [story](#).

The source code and other assets are available on [GitHub](#).

1709.8

Release Date: June 1, 2018

Bug Fix

- Includes a fix to support syncing as stated by Microsoft even when the time is drastically off.

The source code and other assets are available on [GitHub](#).

1709.7

Release Date: May 24, 2018

Improvements

- Disabled root disk resizing for the 1709 AWS stemcell.

The source code and other assets are available on [GitHub](#).

1709.6

Release Date: May 18, 2018

Improvements

- Intended for use with [May 2018](#) Microsoft security updates.

The source code and other assets are available on [GitHub](#).

1709.5

Release Date: May 8, 2018

Improvements

- Intended for use with [April 2018](#) [Microsoft security updates](#).
- Disabled root disk resizing and provided large root disks by default. For more information, see [Windows Stemcells v1709.5-v1709.12](#) [in *Installing and Configuring PAS for Windows*](#).

The source code and other assets are available on [GitHub](#) [.](#)

1709.4

Release Date: March 20, 2018

Note

- You must **enable** the Meltdown and Spectre patch for it to function. See [Creating a vSphere Stemcell by Hand](#) [in GitHub](#) for instruction to enable the patch.

Improvements

- Intended for use with March 2018 Microsoft security updates.
- Intended for use with [KB4056892](#) [that addresses Microsoft's guidance for protection against speculative execution side-channel vulnerabilities](#) [.](#) See Microsoft's *Known Issues* listed in the [KB article](#) [for the patch](#).

Source code and other assets on [GitHub](#) [.](#)

1709.3

Release Date: February 21, 2018

Note

- You must **enable** the Meltdown and Spectre patch for it to function. See [Creating a vSphere Stemcell by Hand](#) [in GitHub](#) for instruction to enable the patch.

Improvements

- Intended for use with February 2018 Microsoft security updates.
- Intended for use with [KB4056892](#) [that addresses Microsoft's guidance for protection against speculative execution side-channel vulnerabilities](#) [.](#) See Microsoft's *Known Issues* listed in the [KB article](#) [for the patch](#).

Fixes

- Fix BOSH ssh when stemcell is operating as a Diego Cell.













Source code and other assets on [GitHub](#) [.](#)

Tiles Using Xenial Stemcells in PCF

This table provides a quick reference of PCF product versions that are now using Xenial stemcells.

Products Using Xenial Stemcells


If a product is not yet listed, the product still uses Trusty stemcells.

| Product/Component | Starting Version | Release Notes Link |
|-----------------------------------|------------------|---|
| PCF Operations Manager | v2.3 | Release Notes  |
| Pivotal Application Service (PAS) | v2.3 | Release Notes  |
| Pivotal Container Service (PKS) | v1.2 | Release Notes  |
| PCF Event Alerts | v1.2.3 | Release Notes  |
| Metrics Forwarder for PCF | v1.11.3 | Release Notes  |
| MySQL for PCF | v2.4 | Release Notes  |
| RabbitMQ for PCF | v1.14.1 | Release Notes  |
| Redis for PCF | v1.14.0 | Release Notes  |
| Scheduler for PCF | v1.2.3 | Release Notes  |
| Single Sign-On (SSO) for PCF | v1.7.1 | Release Notes  |
| Spring Cloud Data Flow | v1.2.0 | Release Notes  |
| Spring Cloud Services for PCF | v2.0.2 | Release Notes  |

Xenial Stemcell Support in Ops Manager

You can import and use Xenial stemcell-based tiles in the following versions of Ops Manager:

- v2.1.15 and later
- v2.2.2 and later
- v2.3.x and later

For more information about the introduction of Xenial stemcells to your PCF deployment, see [Updates for Xenial Stemcell Support](#)  in the *Pivotal Cloud Foundry v2.3 Breaking Changes Release Notes*.

Platform Architecture and Planning

This documentation describes reference architectures and other plans for installing Pivotal Cloud Foundry (PCF) on any infrastructure to support the runtime environments Pivotal Application Service (PAS) and Pivotal Container Service (PKS).

Overview

A Pivotal Cloud Foundry (PCF) reference architecture describes a proven approach for deploying PCF on a specific IaaS, such as AWS, Azure, GCP, OpenStack, or vSphere. PCF reference architectures meet the following requirements:

- Secure
- Publicly-accessible
- Includes common PCF-managed services such as MySQL, RabbitMQ, and Spring Cloud Services
- Can host at least 100 app instances, or far more
- Have been deployed and validated by Pivotal to support Ops Manager, PAS, and PKS

You can use PCF reference architectures to help plan the best configuration for your PCF deployment on your IaaS.

Reference Architecture and Planning Topics

All PCF reference architectures start with the [Base PAS Architecture](#) and [Base PKS Architecture](#), below.

The following infrastructure-specific topics build on these two common base architectures:

- [AWS Reference Architecture](#)
- [Azure Reference Architecture](#)
- [GCP Reference Architecture](#)
- [OpenStack Reference Architecture](#)
- [vSphere Reference Architecture](#)

The following topic describes a broader architecture that automates the installation and updating of multiple PCF foundations, multiple instances of each architecture above:

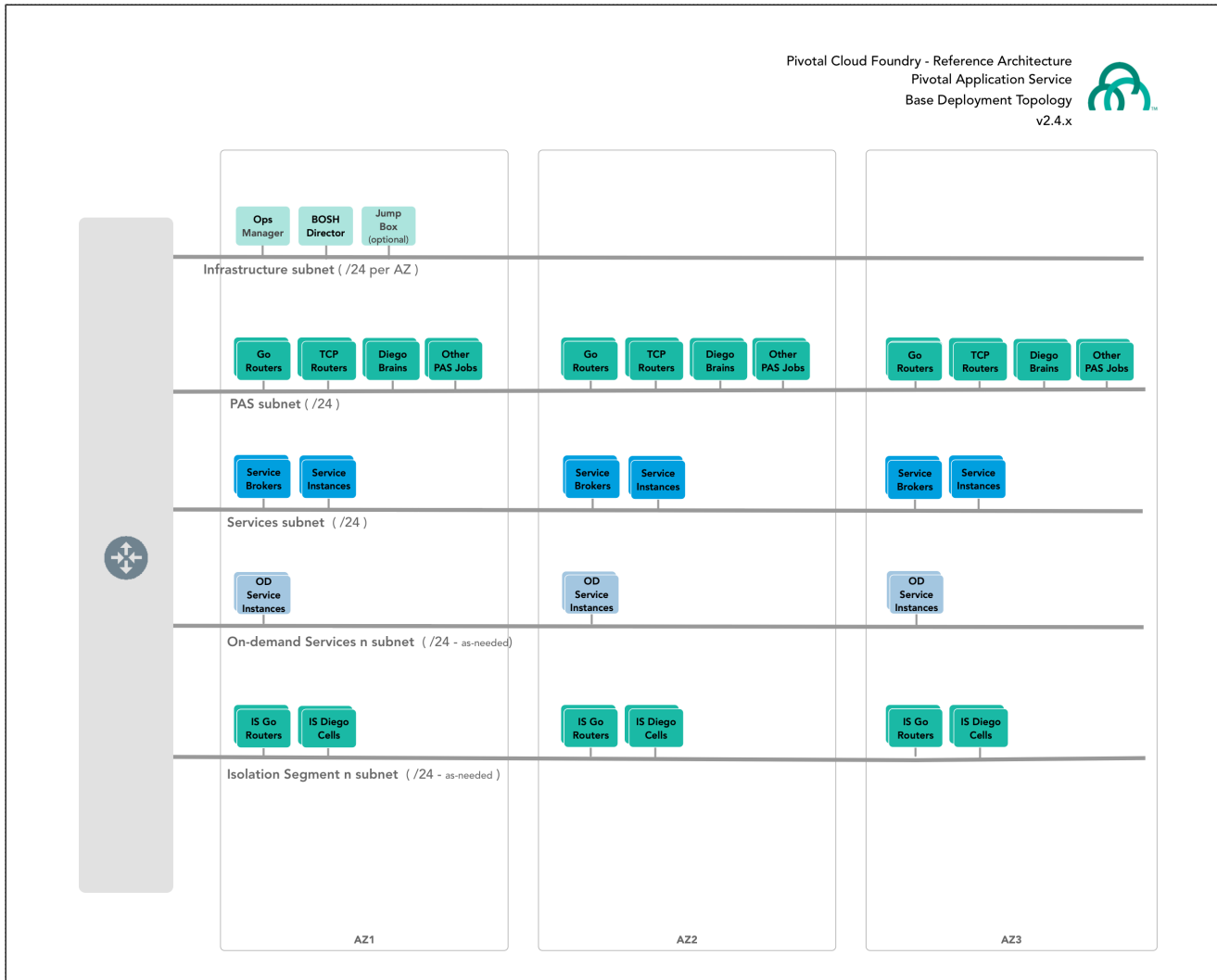
- [Control Plane Reference Architectures](#)

The following topics address aspects of platform architecture and planning that the PCF reference architectures do not cover:

- [Implementing a Multi-Foundation PKS Deployment](#)
- [Using Global DNS Load Balancers for Multi-Foundation](#)

PAS Architecture

The following diagram shows a base architecture for PAS, and how its network topology places and replicates PCF and PAS components across subnets and Availability Zones.



[View a larger version of this diagram](#)

Internal Components

The following table describes the internal component placements shown in the diagram above:

| Component | Placement and Access Notes |
|--------------------------------|---|
| Ops Manager | Deployed on one of the three public subnets. Accessible by FQDN or through an optional jumpbox. |
| BOSH Director | Deployed on the infrastructure subnet. |
| Jumpbox | Optional. Deployed on the infrastructure subnet for accessing PAS management components such as Ops Manager and the Cloud Foundry command-line interface (cf CLI). |
| Gorouters (HTTP routers in CF) | Deployed on all three PAS subnets, one per Availability Zone (AZ). Accessed through the HTTP, HTTPS, and SSL load balancers. |
| Diego Brain | Deployed on all three PAS subnets, one per AZ. The Diego Brain component is required, but SSH container access support through the Diego Brain is optional, and enabled through the SSH load balancers. |
| TCP Routers | Optional. Deployed on all three PAS subnets, one per AZ, to support TCP routing. |
| Service Tiles | Service brokers and shared services instances are deployed to the Services subnet. Dedicated on-demand service instances are deployed to an On-demand services subnet. |
| Isolation Segments | Deployed on an Isolation Segment subnet. Includes Diego Cells and Gorouters for running and accessing apps hosted within isolation segments. |

Networks

Pivotal recommends defining your networks and load-balancing their incoming requests as follows:

Required Subnets

PAS requires the following statically-defined networks to host its main component systems.

- Infrastructure subnet - `/24` segment This subnet contains VMs that require access only for Platform Administrators, for example Ops Manager, the BOSH Director, and an optional jumpbox.
- PAS subnet - `/24` segment This subnet contains PAS runtime VMs, such as Gorouters, Diego Cells and Cloud Controllers.
- Services subnet - `/24` segment The Services and On-Demand Services networks support Ops Manager tiles that you might add in addition to PAS. You can think of them as the “everything not PAS” networks. Some services tiles can call for additional network capacity to grow into on-demand. If you use services with this capability, Pivotal recommends that you add an On-Demand Services network for each on-demand service, as described below.
- On-Demand Services subnet(s) - `/24` segments This is for services that can allocate network capacity on-demand from BOSH for their worker VMs; see the Services subnet above. Pivotal recommends allocating a dedicated subnet to each on-demand service. For example, you can configure the Redis tile as follows:
 - **Network:** enter the existing `Services` network, to host the service broker
 - **Services Network:** deploy a new network `OD-Services1`, to host the Redis worker VMs

Another on-demand service tile can then also use `Services` for its broker and a new `OD-Services2` network for its workers, and so on.

- Isolation Segments subnet(s) - `/24` segments You can add one or more Isolation Segment tiles to an PAS installation to compartmentalize hosting and routing resources. For each Isolation Segment you deploy, you should designate a `/24` network for its range of address space.

Load Balancing

Any PAS installation needs a suitable load balancer to send incoming HTTP, HTTPS, SSH, and SSL traffic to its Gorouters and application containers. All installations approaching production-level use rely on external load balancing from hardware appliance vendors or other network-layer solutions.

The load balancer can also perform Layer 4 or Layer 7 load balancing functions. SSL can be terminated at the load balancer or used as a pass-through to the Gorouter.

Common deployments of load balancing in PAS are:

- HTTP/HTTPS traffic to and from Gorouters
- TCP traffic to and from TCP routers
- Traffic from the Diego Brain, when developers access app containers via SSH

To balance load across multiple PAS foundations, use an IaaS- or vendor-specific Global Traffic Manager or Global DNS load balancer.

For additional information, see [Global DNS Load Balancers for Multi-Foundation Environments](#).

High Availability

PAS is not considered High Availability (HA) until it runs across at least two Availability Zones (AZs). Pivotal recommends defining three AZs.

On IaaSes with their own HA capabilities, using the IaaS HA in conjunction with a PCF HA topology provides the best of both worlds. Multiple AZs give PCF redundancy, so that losing an AZ is not catastrophic. The BOSH Resurrector can then replace lost VMs as needed to repair a foundation.

To back up and restore a foundation externally, use BOSH Backup and Restore (BBR). For more information, see the [BOSH Backup and Restore](#) documentation.

Storage

PAS requires disk storage for each component, for both persistent data and to allocate to ephemeral data. You size these disks in the **Resource Config** pane of the PAS tile. For details on storage configuration and capacity planning, see the corresponding chapter for the specific IaaS.

The platform also requires you to configure file storage for large shared objects. These blobstores can be external or internal. For details, see the

Configure File Storage step in the *Deploying PAS* topic for your IaaS, and the [Configure File Storage](#) section in the *Configuring PAS for Upgrade* topic.

Security

See the topics below for how PAS implements security:

- [PCF Infrastructure Security](#) 
- [Security Concepts](#) 
- [Certificates and TLS in PCF](#)
- [Network Communication Paths in PCF](#)  - includes firewall ports

Domain Names

PAS requires following domain names to be registered:

- System domain, for PAS and other tiles: `sys.domain.name`
- App domain, for your applications: `app.domain.name`

You must also define the following wildcard domain names and include them when creating certificates that access PAS and its hosted apps:

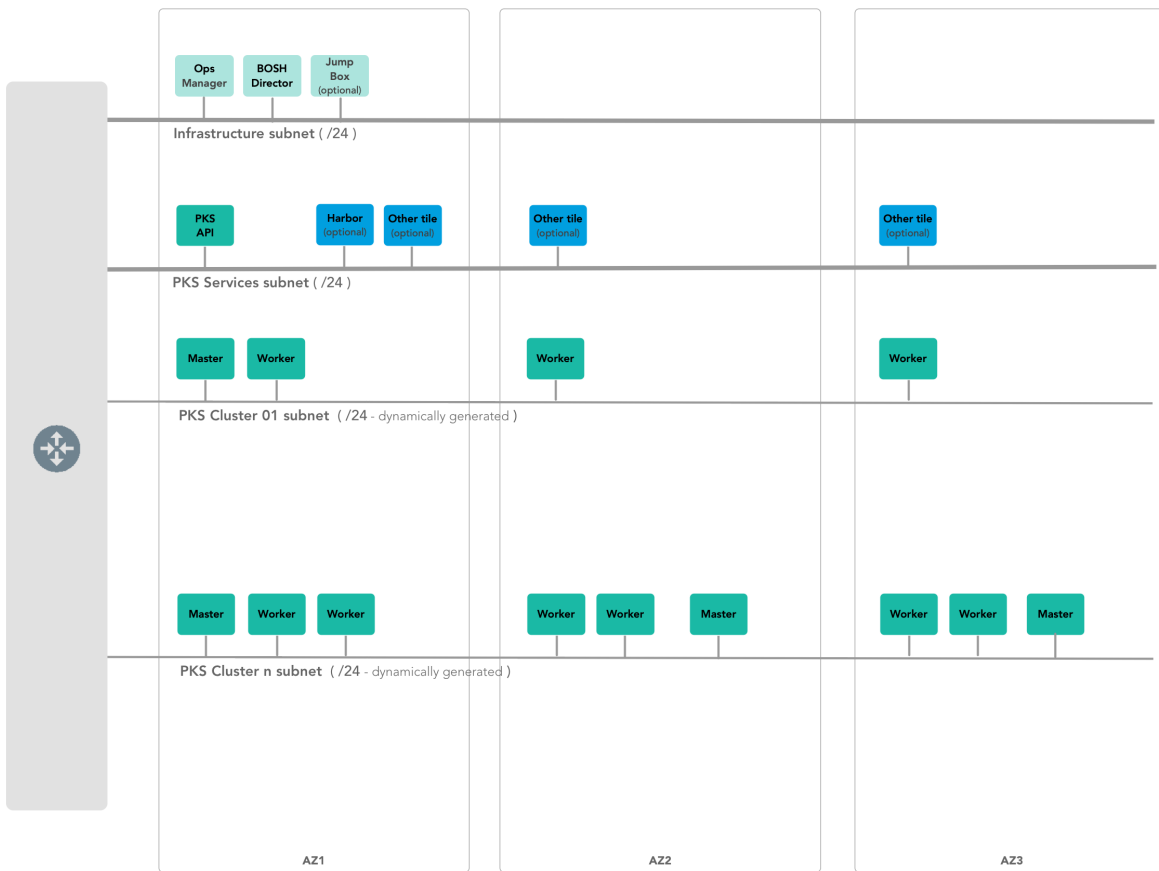
- *.SYSTEM-DOMAIN
- *.APPS-DOMAIN
- *.login.SYSTEM-DOMAIN
- *.uaa.SYSTEM-DOMAIN

Component Scaling

See [Scaling PAS](#) for recommendations on how to scale PAS for different deployment scenarios.

PKS Architecture

The following diagram shows a base architecture for PKS, and how its network topology places and replicates PCF and PKS components across subnets and Availability Zones.



[View a larger version of this diagram](#)

Internal Components

The following table describes the internal component placements shown in the diagram above:

| Component | Placement and Access Notes |
|---------------|---|
| Ops Manager | Deployed on one of the subnets. Accessible by fully-qualified domain name (FQDN) or through an optional jumpbox. |
| BOSH Director | Deployed on the infrastructure subnet. |
| Jumpbox | Optional. Deployed on the infrastructure subnet for accessing PKS management components such as Ops Manager and the PKS + Kubectl command-line interface. |
| PKS API | Deployed as a service broker VM on the PKS Services subnet. Handles PKS API and service adapter requests, and manages PKS clusters. For more information, see Pivotal Container Service (PKS) . |
| Harbor Tile | Optional container images registry, typically deployed to the Services subnet. |
| PKS Cluster | Deployed to a dynamically-created, dedicated PKS cluster subnet. Each cluster consists of worker nodes that run the workloads (applications) and one or more master nodes. |

Networks

Pivotal recommends defining your networks and load-balancing their incoming requests as follows:

Subnets Requirements

PKS requires two defined networks to host the main elements that compose it.

- Infrastructure subnet - `/24` Contains VMs that require access only for Platform Administrators, for example Ops Manager, BOSH Director and an optional jumpbox.
- PKS Services subnet - `/24` Hosts PKS API VM and other optional service tiles such as Harbor.
- PKS Clusters subnets - each one a `/24` from a pool of pre-allocated IPs Hosts PKS clusters.

Load Balancing

Load balancers can be used to manage traffic across master nodes of a PKS cluster or for deployed workloads. For more information on how to configure load balancers for PKS, refer to the corresponding documentation for the specific IaaS.

High Availability

PKS has no inherent HA capabilities to design for. Make the best efforts to have HA design at the IaaS, storage, power and access layers to support PKS.

Storage

PKS requires shared storage across all Availability Zones for the deployed workloads to appropriately allocate their required storage.

Security

See the topics below for how PKS implements security:


- [Enterprise PKS Security](#) 
- [Firewall Ports](#) 

Domain Names

PKS requires the following domain names to be registered when creating a wildcard certificate and PKS tile configurations: `*.pks.domain.name`

The wildcard certificate covers both the PKS API domain e.g. `api.pks.domain.name` and the PKS Clusters domains e.g. `mycluster.pks.domain.name`.

Cluster Management

See [Managing Clusters](#)  for recommendations on managing Enterprise PKS clusters.

| Component | Reference Architecture Notes |
|---|---|
| Domains & DNS | <p>CF Domain Zones and routes in use by the reference architecture include:</p> <ul style="list-style-type: none"> domains for *.apps and *.sys (required) a route for Ops Manager (required) a route for ssh access to app containers (optional) <p>Using Route 53 to manage domains is optional.</p> |
| Ops Manager | Deployed on one of the three public subnets and accessible by FQDN or through an optional jumpbox. |
| BOSH Director | Deployed on the infrastructure subnet. |
| Elastic Load Balancers - HTTP, HTTPS, and SSL | Required. Load balancer that handles incoming HTTP, HTTPS, and SSL traffic and forwards them to the Gorouters. Deployed on all three public subnets. |
| Elastic Load Balancers - SSH | Optional. Load balancer that provides SSH access to app containers. Deployed on all three public subnets, one per AZ. |
| Gorouters | Accessed through the HTTP, HTTPS, and SSL Elastic Load Balancers. Deployed on all three Pivotal Application Service (PAS) subnets, one per AZ. |
| Diego Brains | Required. However, the SSH container access functionality is optional and enabled through the SSH Elastic Load Balancers. Deployed on all three PAS subnets, one per AZ. |
| TCP Routers | Optional feature for TCP routing. Deployed on all three PAS subnets, one per AZ. |
| CF Database | Reference architecture uses AWS RDS. Deployed on all three RDS subnets, one per AZ. |
| Storage Buckets | Reference architecture uses 4 S3 buckets: buildpacks, droplets, packages, and resources. |
| Service Tiles | Deployed on all three service subnets, one per AZ. |
| Service User & Roles | <p>One IAM role and one IAM user are recommended: the IAM role for Terraform, and the IAM user for Ops Manager and BOSH. Consult the following list:</p> <ul style="list-style-type: none"> Admin Role: Terraform uses this IAM role to provision required AWS resources as well as an IAM user. IAM User: This IAM user with IAM security credentials (access key ID and secret access key) is automatically provisioned with restrict access only to resources needed by PCF. |
| EC2 Instance Quota | The default EC2 instance quota on a new AWS subscription only has around 20 EC2 instances, which is not enough to host a multi-AZ deployment. The recommended quota for EC2 instances is 100. AWS requires the instances quota tickets to include Primary Instance Types, which should be t2.micro. |

Network Objects

The following table lists the network objects in this reference architecture.

| Network Object | Notes | Estimated Number |
|-------------------------------|--|------------------|
| External Public IPs | One per deployment, assigned to Ops Manager. | 1 |
| Virtual Private Network (VPC) | One per deployment. A PCF deployment exists within a single VPC and a single AWS region, but should distribute PCF jobs and instances across 3 AWS AZs to ensure a high degree of availability. | 1 |
| Subnets | <p>The reference architecture requires the following subnets:</p> <ul style="list-style-type: none"> 1 x (/24) infrastructure (BOSH Director) subnet 3 x (/24) public subnets (Ops Manager, Elastic Load Balancers, NAT instances), one per AZ 3 x (/20) PAS subnets (Gorouters, Diego Cells, Cloud Controllers, etc.), one per AZ 3 x (/20) services subnets (RabbitMQ, MySQL, Spring Cloud Services, etc.), one per AZ 3 x (/24) RDS subnets (Cloud Controller DB, UAA DB, etc.), one per AZ. | 13 |
| | This reference architecture requires 4 route tables: one for the public subnet, and one each for all 3 private subnets across 3 AZs. Consult the following list: | |

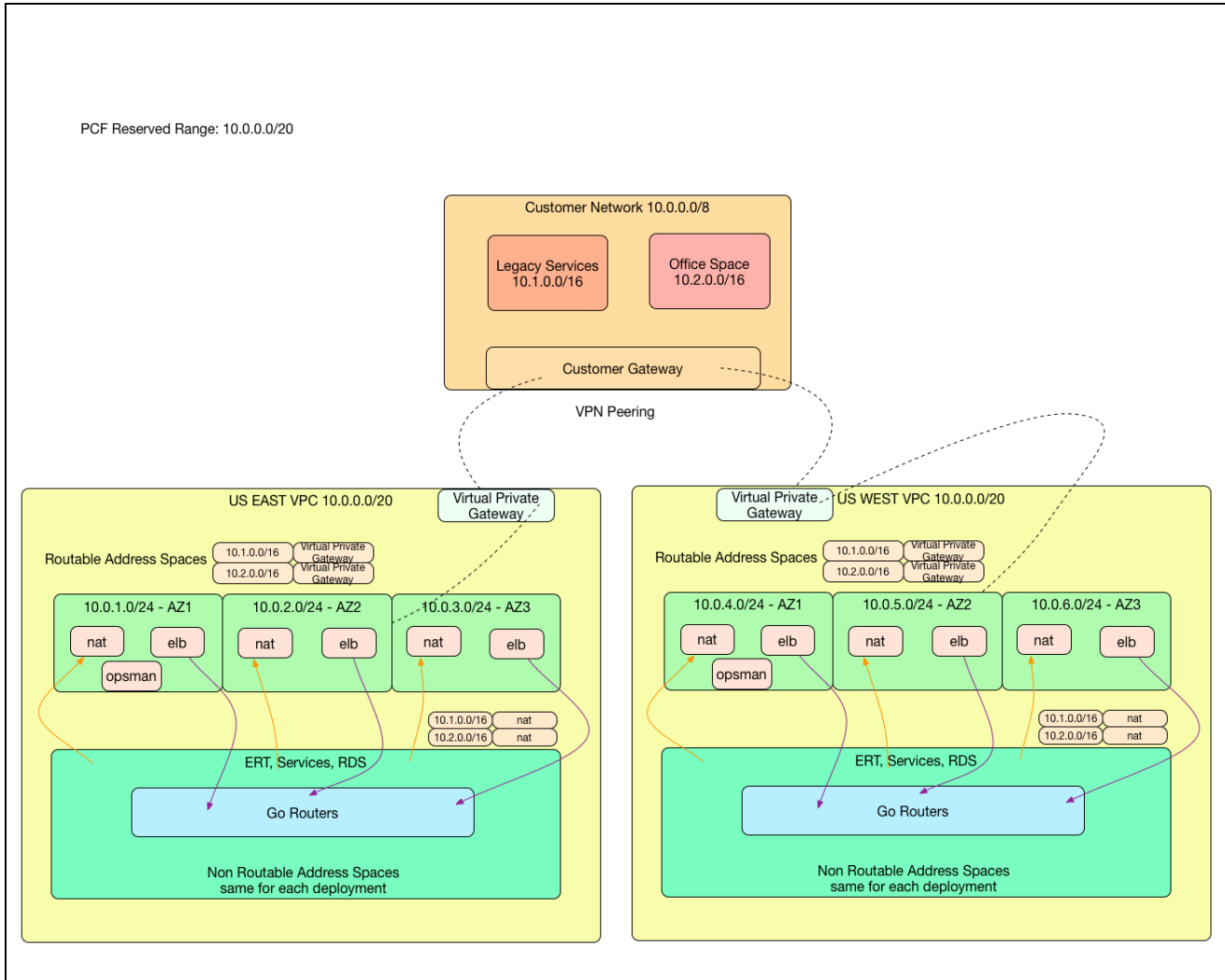
| Route Tables | <ul style="list-style-type: none">PublicSubnetRouteTable: This routing table enables the ingress/egress routes from/to Internet through the Internet gateway for Ops Manager and the NAT Gateway.PrivateSubnetRouteTable: This routing table enables the egress routing to the Internet through the NAT Gateway for the BOSH Director and PAS. <p>For more information, see the Terraform script that creates the route tables and the script that performs the route table association.</p> <div><p>Note: If an EC2 instance sits on a subnet with an Internet gateway attached as well as a public IP address, it is accessible from the Internet through the public IP address; for example, Ops Manager. PAS needs Internet access due to the access needs of using an S3 bucket as a blobstore.</p></div> | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|---|----------------|---------------|--|----------|-------------|----------|-------------|-----------|------|------------------------------|----------|-------------|-----------|-------|--|--------|-------------|----------|-----|--|-----------|------------------|----------|-----|--|-------|----|-----------|-----|-------------|-------|-----|-----------|-----|--------------|-------|------|-----------|-----|--|----------|------|-----------|-----|------------------------------|---|
| Security Groups | <p>The reference architecture requires 5 Security Groups. For more information, see the Terraform Security Group rules script. The following table describes the Security Group ingress rules:</p> <div><p>Note: The extra port of 4443 with the Elastic Load Balancer is due to the limitation that the Elastic Load Balancer does not support WebSocket connections on HTTP/HTTPS.</p></div> <table><thead><tr><th>Security Group</th><th>Port</th><th>From CIDR</th><th>Protocol</th><th>Description</th></tr></thead><tbody><tr><td>OpsMgrSG</td><td>22</td><td>0.0.0.0/0</td><td>TCP</td><td>Ops Manager SSH access</td></tr><tr><td>OpsMgrSG</td><td>443</td><td>0.0.0.0/0</td><td>TCP</td><td>Ops Manager HTTP access</td></tr><tr><td>VmsSG</td><td>ALL</td><td>VPC_CIDR</td><td>ALL</td><td>Open up connections among BOSH-deployed VMs</td></tr><tr><td>MysqlSG</td><td>3306</td><td>VPC_CIDR</td><td>TCP</td><td>Enable network access to RDS</td></tr><tr><td>ElbSG</td><td>80</td><td>0.0.0.0/0</td><td>TCP</td><td>HTTP to PAS</td></tr><tr><td>ElbSG</td><td>443</td><td>0.0.0.0/0</td><td>TCP</td><td>HTTPS to PAS</td></tr><tr><td>ElbSG</td><td>4443</td><td>0.0.0.0/0</td><td>TCP</td><td>WebSocket connection to Loggregator endpoint</td></tr><tr><td>SshElbSG</td><td>2222</td><td>0.0.0.0/0</td><td>TCP</td><td>SSH connection to containers</td></tr></tbody></table> | Security Group | Port | From CIDR | Protocol | Description | OpsMgrSG | 22 | 0.0.0.0/0 | TCP | Ops Manager SSH access | OpsMgrSG | 443 | 0.0.0.0/0 | TCP | Ops Manager HTTP access | VmsSG | ALL | VPC_CIDR | ALL | Open up connections among BOSH-deployed VMs | MysqlSG | 3306 | VPC_CIDR | TCP | Enable network access to RDS | ElbSG | 80 | 0.0.0.0/0 | TCP | HTTP to PAS | ElbSG | 443 | 0.0.0.0/0 | TCP | HTTPS to PAS | ElbSG | 4443 | 0.0.0.0/0 | TCP | WebSocket connection to Loggregator endpoint | SshElbSG | 2222 | 0.0.0.0/0 | TCP | SSH connection to containers | 5 |
| Security Group | Port | From CIDR | Protocol | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OpsMgrSG | 22 | 0.0.0.0/0 | TCP | Ops Manager SSH access | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OpsMgrSG | 443 | 0.0.0.0/0 | TCP | Ops Manager HTTP access | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| VmsSG | ALL | VPC_CIDR | ALL | Open up connections among BOSH-deployed VMs | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MysqlSG | 3306 | VPC_CIDR | TCP | Enable network access to RDS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ElbSG | 80 | 0.0.0.0/0 | TCP | HTTP to PAS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ElbSG | 443 | 0.0.0.0/0 | TCP | HTTPS to PAS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ElbSG | 4443 | 0.0.0.0/0 | TCP | WebSocket connection to Loggregator endpoint | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SshElbSG | 2222 | 0.0.0.0/0 | TCP | SSH connection to containers | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Load Balancers | <p>PCF on AWS requires the Elastic Load Balancer, which can be configured with multiple listeners to forward HTTP/HTTPS/TCP traffic. Two Elastic Load Balancers are recommended: one to forward the traffic to the Gorouters, <code>PcfElb</code>, the other to forward the traffic to the Diego Brain SSH proxy, <code>PcfSshElb</code>. For more information, see the Terraform load balancers script.</p> <p>The following table describes the required listeners for each load balancer:</p> <table><thead><tr><th>ELB</th><th>Instance/Port</th><th>LB Port</th><th>Protocol</th><th>Description</th></tr></thead><tbody><tr><td>PcfElb</td><td>gorouter/80</td><td>80</td><td>HTTP</td><td>Forward traffic to Gorouters</td></tr><tr><td>PcfElb</td><td>gorouter/80</td><td>443</td><td>HTTPS</td><td>SSL termination and forward traffic to Gorouters</td></tr><tr><td>PcfElb</td><td>gorouter/80</td><td>4443</td><td>SSL</td><td>SSL termination and forward traffic to Gorouters</td></tr><tr><td>PcfSshElb</td><td>diego-brain/2222</td><td>2222</td><td>TCP</td><td>Forward traffic to Diego Brain for container SSH connections</td></tr></tbody></table> <p>Each ELB binds with a health check to check the health of the back-end instances:</p> <ul style="list-style-type: none"><code>PcfElb</code> checks the health on Gorouter port 80 with TCP<code>PcfSshElb</code> checks the health on Diego Brain port 2222 with TCP | ELB | Instance/Port | LB Port | Protocol | Description | PcfElb | gorouter/80 | 80 | HTTP | Forward traffic to Gorouters | PcfElb | gorouter/80 | 443 | HTTPS | SSL termination and forward traffic to Gorouters | PcfElb | gorouter/80 | 4443 | SSL | SSL termination and forward traffic to Gorouters | PcfSshElb | diego-brain/2222 | 2222 | TCP | Forward traffic to Diego Brain for container SSH connections | 2 | | | | | | | | | | | | | | | | | | | | |
| ELB | Instance/Port | LB Port | Protocol | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PcfElb | gorouter/80 | 80 | HTTP | Forward traffic to Gorouters | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PcfElb | gorouter/80 | 443 | HTTPS | SSL termination and forward traffic to Gorouters | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PcfElb | gorouter/80 | 4443 | SSL | SSL termination and forward traffic to Gorouters | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PcfSshElb | diego-brain/2222 | 2222 | TCP | Forward traffic to Diego Brain for container SSH connections | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Jumpbox | <p>Optional. Provides a way of accessing different network components. For example, you can configure it with your own permissions and then set it up to access to Pivotal Network to download tiles. Using a jumpbox is particularly useful in IaaS where Ops Manager does not have a public IP address. In these cases, you can SSH into Ops Manager or any other component through the jumpbox.</p> | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Integrate PCF with Customer Data Center through VPN

At times, applications on PCF need to access on-premise data. The connection between an AWS VPC and an on-premise datacenter is made through [VPN peering](#). When employing non-VPN peering, there are several points to consider:

- Assign routable IP addresses with the following in mind:
 - It may not be realistic to request multiple routable /22 address spaces, due to IP exhaustion.
 - Using different VPC address spaces can cause snowflakes deployments and present difficulties in automation.
 - Only make the load balancer, NAT devices, and Ops Manager routable.

- PCF components can route egress through a NAT instance. As a result, operators do not need to assign routable IP addresses to PCF components.
- Inbound traffic from the datacenter should come through an [internal load balancer](#).
 - Outbound traffic to the datacenter should go through AWS NAT instances.



[View a larger version of this diagram](#).

Azure Reference Architecture

This guide presents a reference architecture for Pivotal Cloud Foundry (PCF) on Azure.

Azure does not provide resources in a way that translates directly to PCF availability zones. Instead, Azure provides high availability through fault domains and [availability sets](#).

All reference architectures described in this topic are validated for production-grade PCF deployments using fault domains and availability sets that include multiple job instances.

See [Azure on PCF Requirements](#) for general requirements for running PCF and specific requirements for running PCF on Azure.

PCF Reference Architectures

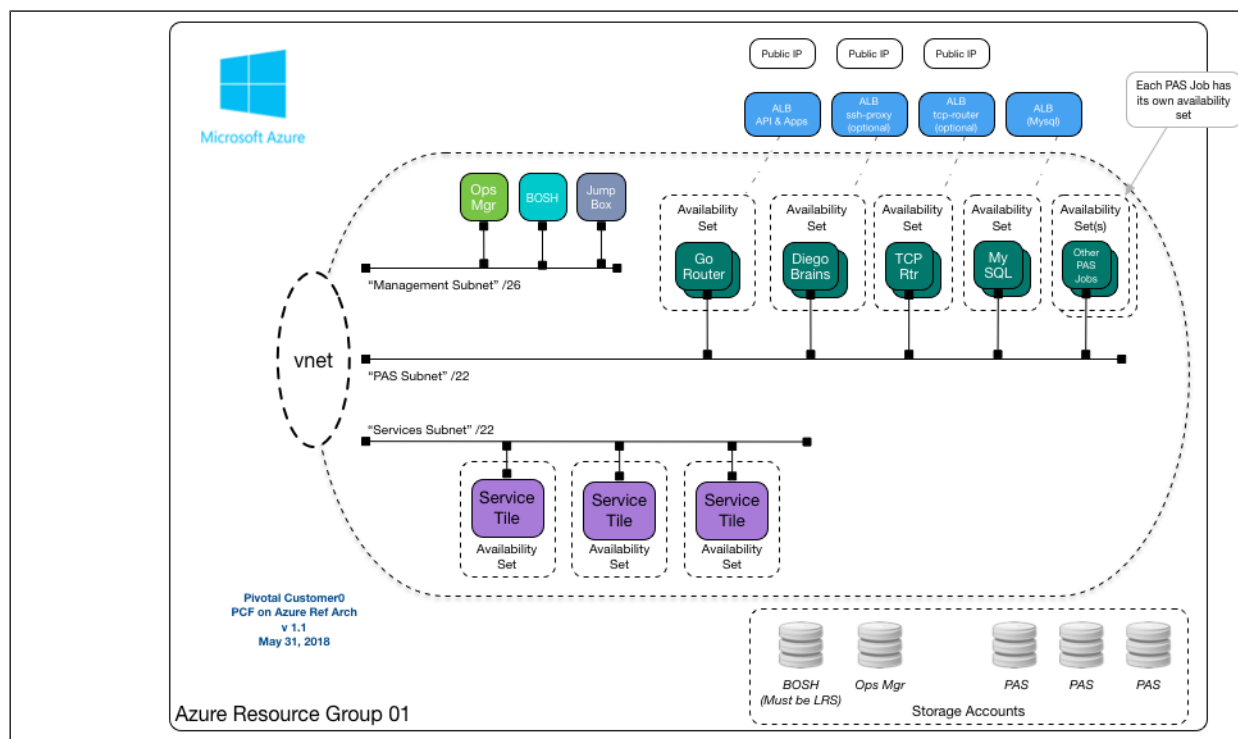
A PCF reference architecture describes a proven approach for deploying PCF on a specific IaaS, such as Azure, that meets the following requirements:

- Secure
- Publicly-accessible
- Includes common PCF-managed services such as MySQL, RabbitMQ, and Spring Cloud Services
- Can host at least 100 app instances, or far more

Pivotal provides reference architectures to help you determine the best configuration for your PCF deployment.

Base Azure Reference Architecture

The following diagram provides an overview of a reference architecture deployment of PCF on Azure.



[View a larger version of this diagram](#).

Base Reference Architecture Components

The following table lists the components that are part of a base reference architecture deployment on Azure using a single resource group.

| Component | Reference Architecture Notes |
|------------------------------------|--|
| Domains and DNS | CF Domain Zones and routes in use by the reference architecture include: <ul style="list-style-type: none"> domains for *.apps and *.system (required), a route for Ops Manager (required), a route for Doppler (required), a route for Loggregator (required), a route for SSH access to app containers (optional), and a route for TCP routing to apps (optional). |
| Ops Manager | Deployed on the management subnet and accessible by FQDN or through an optional jumpbox. |
| BOSH | Deployed on the management subnet. |
| Azure Load Balancer - API and Apps | Required. Load balancer that handles incoming API and apps requests and forwards them to the Gorouters. |
| Azure Load Balancer - ssh-proxy | Optional. Load balancer that provides SSH access to app containers. |
| Azure Load Balancer - tcp-router | Optional. Load balancer that handles TCP routing requests for apps. |
| Azure Load Balancer - MySQL | Required to provide high availability for MySQL backend to Pivotal Application Service (PAS). |
| Gorouters | Accessed through the API and Apps load balancer. Deployed on the PAS subnet, one job per Azure availability set. |
| Diego Brains | Required. However, the SSH container access functionality is optional and enabled through the SSH Proxy load balancer. Deployed on the PAS subnet, one job per Azure availability set. |
| TCP Routers | Optional feature for TCP routing. Deployed on the PAS subnet, one job per availability zone. |
| MySQL | Reference architecture uses internal MySQL provided with PCF. Deployed on the PAS subnet, one job per Azure availability set. |
| PAS | Required. Deployed on the PAS subnet, one job per Azure availability set. |
| Storage Accounts | PCF on Azure requires 5 standard storage accounts: BOSH, Ops Manager, and three PAS storage accounts. Each account comes with a set amount of disk. Reference architecture recommends using 5 storage accounts because Azure Storage Accounts have an IOPs limit of approximately 20k per account, which generally relates to a BOSH JOB/VM limit of approximately 20 VMs each. |
| Service Tiles | Deployed on the Services subnet. Each service tile is deployed to an availability set. |

Alternative Network Layouts for Azure

This section describes the possible network layouts for PCF deployments as covered by the reference architecture of PCF on Azure.

At a high level, there are currently two possible ways of deploying PCF as described by the reference architecture:

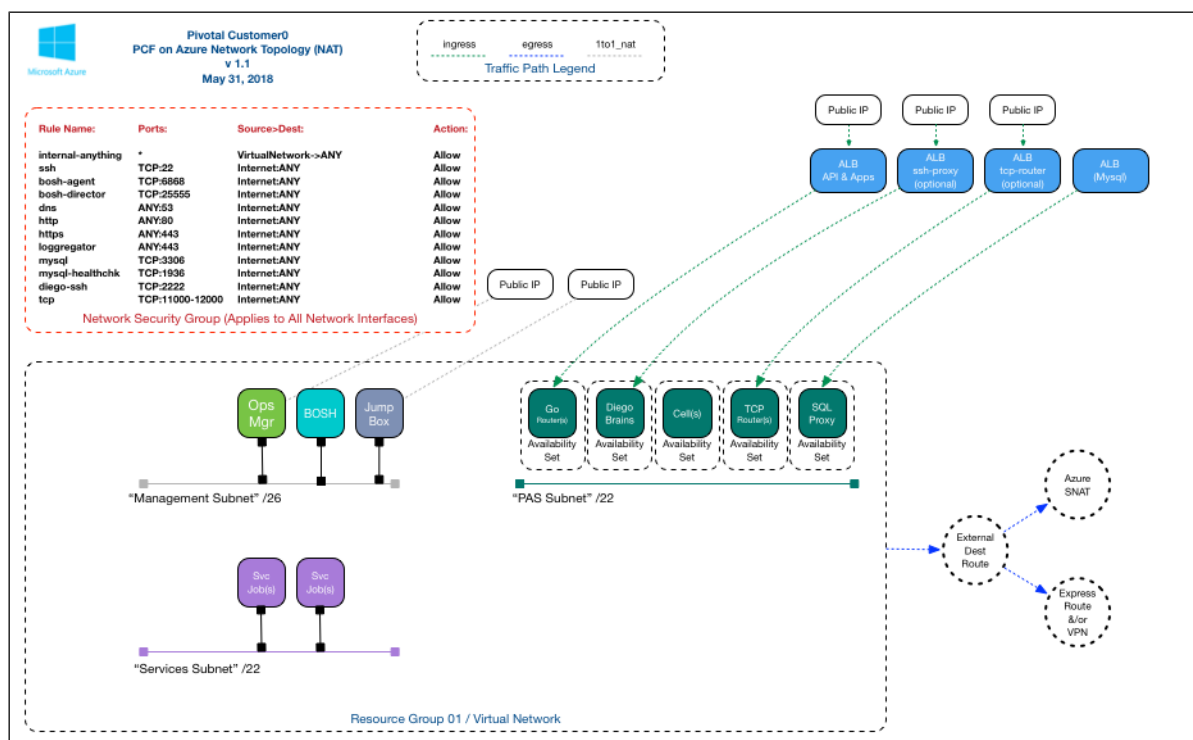
1. Single resource group, or
2. Multiple resource groups.

The first scenario is outlined in [Installing PCF on Azure](#). It models a single PCF deployment in a single Azure Resource Group.

If you require multiple resource groups, refer to the [Multiple Resource Group deployment](#) section of this topic.

Network Layout

This diagram illustrates the network topology of the base reference architecture for PCF on Azure. In this deployment, you expose only a minimal number of public IP addresses and deploy only one resource group.



[View a larger version of this diagram](#)

Network Objects

The following table lists the network objects in PCF on Azure reference architecture.

| Network Object | Notes | Estimated Number |
|------------------------------|---|------------------|
| External Public IP addresses | <p>Use</p> <ol style="list-style-type: none"> 1. global IP address for apps and system access 2. Ops Manager or optional jumpbox. <p>Optionally, you can use a public IP address for the ssh-proxy and tcp-router load balancers.</p> | 1-4 |
| Virtual Network | One per deployment. Azure virtual network objects allow multiple subnets with multiple CIDRs, so a typical deployment of PCF will likely only ever require one Azure Virtual Network object. | 1 |
| Subnets | <p>Separate subnets for</p> <ol style="list-style-type: none"> 1. management (Ops Manager, BOSH Director, Jumpbox), 2. PAS, 3. and services. <p>Using separate subnets allows you to configure different firewall rules due to your needs.</p> | 4 |
| Routes | Routes are typically created by Azure dynamically when subnets are created, but you may need to create additional routes to force outbound communication to dedicated SNAT nodes. These objects are required to deploy PCF without public IP addresses. | 3+ |
| Firewall Rules | Azure firewall rules are collected into a Network Security Group (NSG) and bound to a Virtual Network object and can be created to use IP ranges, subnets, or instance tags to match for source and destination fields in a rule. One NSG can be used for all firewall rules. | 12 |
| Load Balancers | Used to handle requests to Gorouters and infrastructure components. Azure uses 1 or more load balancers. The API and Apps load balancer is required. The TCP Router load balancer used for TCP routing feature and the SSH load balancer that allows SSH access to Diego apps are both optional. In addition, you can use a MySQL load balancer to provide high availability to MySQL. This is also optional. | 1-4 |
| | Optional. Provides a way of accessing different network components. For example, you can configure it with your own | |

Jumpbox permissions and then set it up to access to Pivotal Network to download tiles. Using a jumpbox is particularly useful in IaaSes where Ops Manager does not have a public IP address. In these cases, you can SSH into Ops Manager or any other component through the jumpbox.

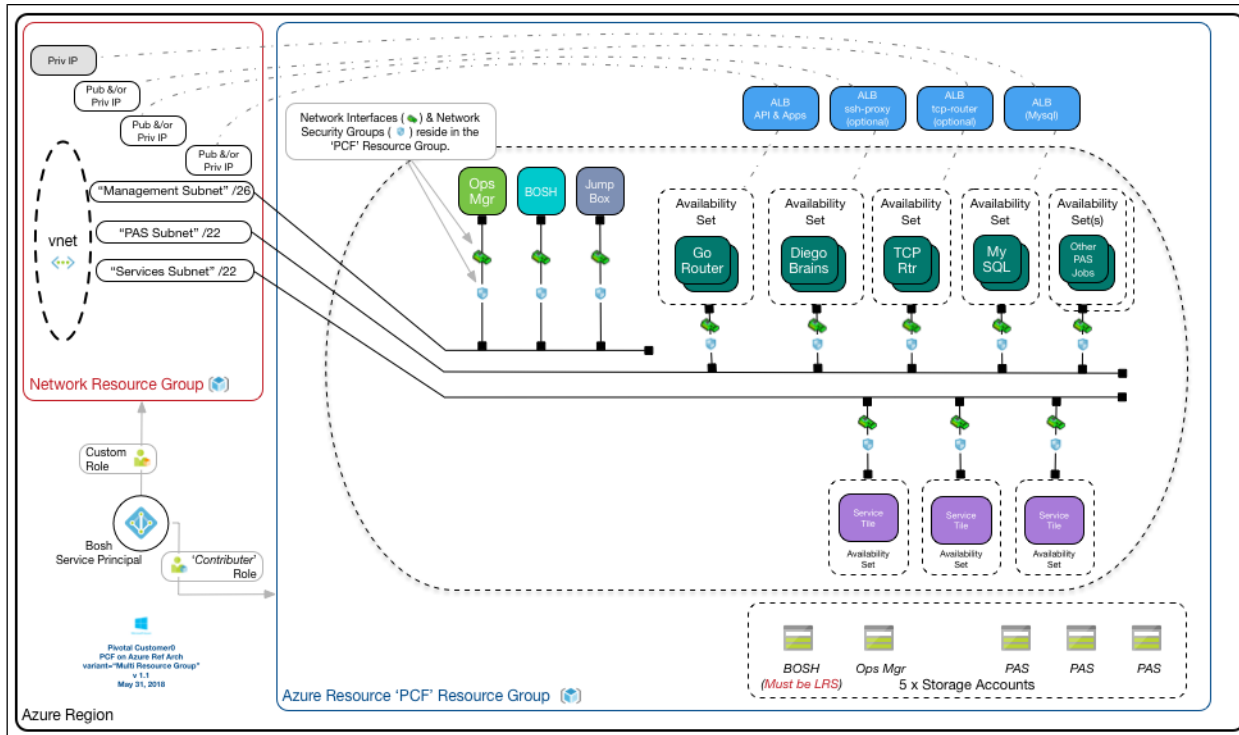
1

Multiple Resource Group Deployment

This diagram illustrates the case where you want to use additional resource groups in your PCF deployment on Azure.

Shared network resources may already exist in an Azure subscription. In this type of deployment, using multiple resource groups allows you to reuse existing resources instead of provisioning new ones.

To use multiple resource groups, you need to provide the BOSH Service Principal with access to the existing network resources.



[View a larger version of this diagram](#).

Multiple Resource Groups Deployment Notes

To deploy PCF on Azure with multiple resource groups, you can define custom roles to grant resource group access to your BOSH Service Principal. For example, you might develop the following:

- Dedicated **Network** Resource Group, limits BOSH Service Principal so that it does not have admin access to network objects.
- Custom Role for BOSH Service Principal, applied to **Network** Resource Group, limits the BOSH Service Principal to minimum read-only access.

```
az role definition create --role-definition
{ \
  "Name": "PCF Network Read Only", \
  "IsCustom": true, \
  "Description": "MVP PCF Read Network Resgroup", \
  "Actions": [ \
    "Microsoft.Network/virtualNetworks/read", \
    "Microsoft.Network/virtualNetworks/subnets/read", \
    "Microsoft.Network/virtualNetworks/subnets/join/action", \
    "Microsoft.Network/networkSecurityGroups/read", \
    "Microsoft.Network/networkSecurityGroups/join/action", \
    "Microsoft.Network/loadBalancers/read", \
    "Microsoft.Network/publicIPAddresses/read", \
    "Microsoft.Network/publicIPAddresses/join/action" \
  ], \
  "NotActions": [], \
  "AssignableScopes": ["/subscriptions/[YOUR_SUBSCRIPTION_ID]" \
  ]
}
```

The actions prefixed with `Microsoft.Network/publicIPAddresses` are only required if using IP addresses.

- Custom Role for BOSH Service Principal, applied to Subscription, allowing the Operator to deploy PCF components

```
az role definition create --role-definition
{ \
  "Name": "PCF Deploy Min Perms", \
  "IsCustom": true, \
  "Description": "MVP PCF Terraform Perms", \
  "Actions": [ \
    "Microsoft.Compute/register/action" \
  ], \
  "NotActions": [], \
  "AssignableScopes": ["/subscriptions/[YOUR_SUBSCRIPTION_ID]" \
  ]
}
```

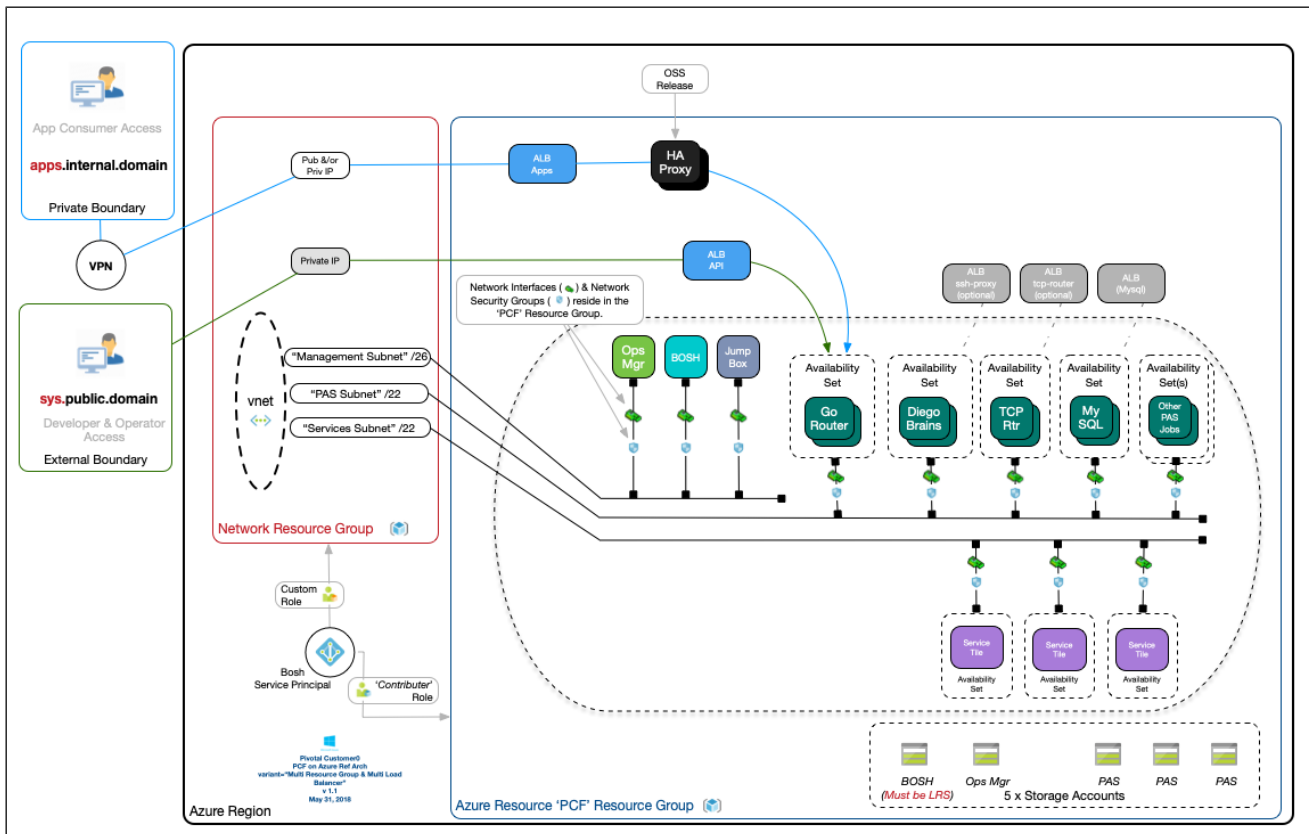
- Custom roles can be assigned to service principals with `az role assignment create --role [ROLE] --assignee [SERVICE_PRINCIPAL_ID]`.

Multiple Resource Group and Multiple Load Balancer Deployment

This diagram illustrates the case where you want to deploy multiple load balancers with your multiple resource group deployment.

The key design points of this deployment are the following:

- Two Azure load balancer (ALBs) to the Gorouter exist. The first ALB is for API access, which utilizes a private IP address. The system domain should resolve to this ALB. The second ALB is for application access, which can either use a public or private IP address. The apps domain should resolve to this ALB.
- Azure does not allow the Gorouters to be members of more than one ALB member pool for the same ports, for example `80` and `443`. This restriction requires an additional reverse proxy to front the Gorouters to allow them to expose traffic on these ports for the system domain.



[View a larger version of this diagram](#)

Log Analytics Integration

[Azure Log Analytics](#) is a service that helps you collect and analyze data generated by resources in your cloud and on-premises environments. The [Microsoft Azure Log Analytics Nozzle for PCF](#) receives logs and metrics from the Loggregator Firehose, filters and resolves the events, and then sends them to Log Analytics, where they appear on unified dashboards and can be correlated with and alerted on other Azure resources.

DNS Delegation

Azure DNS supports DNS delegation, allowing for sub-level domains to be hosted within Azure. This functionality is fully supported within PCF.

Pivotal recommends that you use a sub-zone for your PCF deployment. For example, if your company's domain is `example.com`, your PCF zone in Azure DNS would be `pcf.example.com`.

As Azure DNS does not support recursion, in order to properly configure Azure DNS, create an `NS` record with your registrar which points to the four name servers supplied by your Azure DNS Zone configuration. Once your `NS` records have been created, you can then create the required wildcard `A` records for the PCF application and system domains, as well as any other records desired for your PCF deployments.

You do not need to make any configuration changes in PCF to support Azure DNS.


Azure Blob Storage

Due to limitations in PCF, it is not possible to support a high-availability deployment of the backing NFS store needed for droplets, buildpacks, and other resources. Azure Blob Storage provides fully-redundant hot, cold, or archival storage in either local, regional, or global offerings. It is recommended to use Azure Blob Storage as the external File Storage to provide unlimited scaling and redundancy for high-availability deployments of PCF.

To enable Azure Blob Storage, do the following:

1. Create a Storage Account with the level of redundancy you require. The storage account does not need to be in the same Resource Group as PCF.
2. Create Containers for the buildpacks, droplets, packages, and resources required by PCF.

3. Open Ops Manager.
4. Select **Pivotal Application Services**.
5. Click the **Settings Tab**.
6. Select **File Storage**.
7. Click **External Azure Account**.
8. Enter the Storage Account details.
9. In the Ops Manager main page, apply the changes when you are ready to reconfigure.

 **Note:** There is no direct path to migrate previous objects to Azure Blob Storage. Contact Pivotal Support if you need assistance with this migration.

Load Balancer Migrations

The Azure Load Balancer has two SKUs: Standard and Basic. The Standard SKU Load Balancer is a new load balancer for all TCP and UDP applications with an expanded and more granular feature set over the Basic Load Balancer. Azure's Standard SKU Load Balancer lets you scale your applications and create high availability in environments ranging from small scale deployments to large and complex multi-zone architectures. While the Basic SKU Load Balancer works within the scope of an availability set, a Standard Load Balancer covers an entire virtual network. Pivotal recommends using the Standard SKU Load Balancer instead of the Basic SKU Load Balancer. If you currently use the Basic SKU Load Balancer and wish to migrate to the the Standard SKU, please see the [Migrate Basic SKU Load Balancer to Standard SKU Load Balancer](#) documentation on GitHub.

GCP Reference Architecture

This topic presents two reference architectures for installing Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP): on a [shared virtual private cloud](#) (VPC) and on a [single-project VPC](#). This topic also outlines multiple networking variants for VPC deployment. The architectures are validated for production-grade PCF deployments using multiple AZs.

See [PCF on GCP Requirements](#) for general requirements for running PCF and specific requirements for running PCF on GCP.

PCF Reference Architectures

A PCF reference architecture describes a proven approach for deploying PCF on a specific IaaS, such as GCP.

A PCF reference architecture must meet the following requirements:

- Be secure
- Be publicly-accessible
- Include common PCF-managed services such as MySQL, RabbitMQ, and Spring Cloud Services
- Be able to host at least 100 app instances

Pivotal provides reference architectures to help you determine the best configuration for your PCF deployment.

Shared vs Single-Project VPCs

A [shared VPC](#) installation is harder to configure than a PCF deployment on a single-project VPC, because the required account privileges and resource allocations are more granular and complex. But the shared VPC architecture allows network assets to be centrally located, which simplifies auditing and security. Pivotal recommends the shared VPC model for:

- Deployments with deep auditing and security requirements
- When networks hosting the foundation need to connect back to an internal network via VPN or interconnect

A [single-project VPC](#) lets the platform architect give PCF full access to the VPC and its resources, which makes configuration easier. Pivotal recommends single-project VPC architecture for:

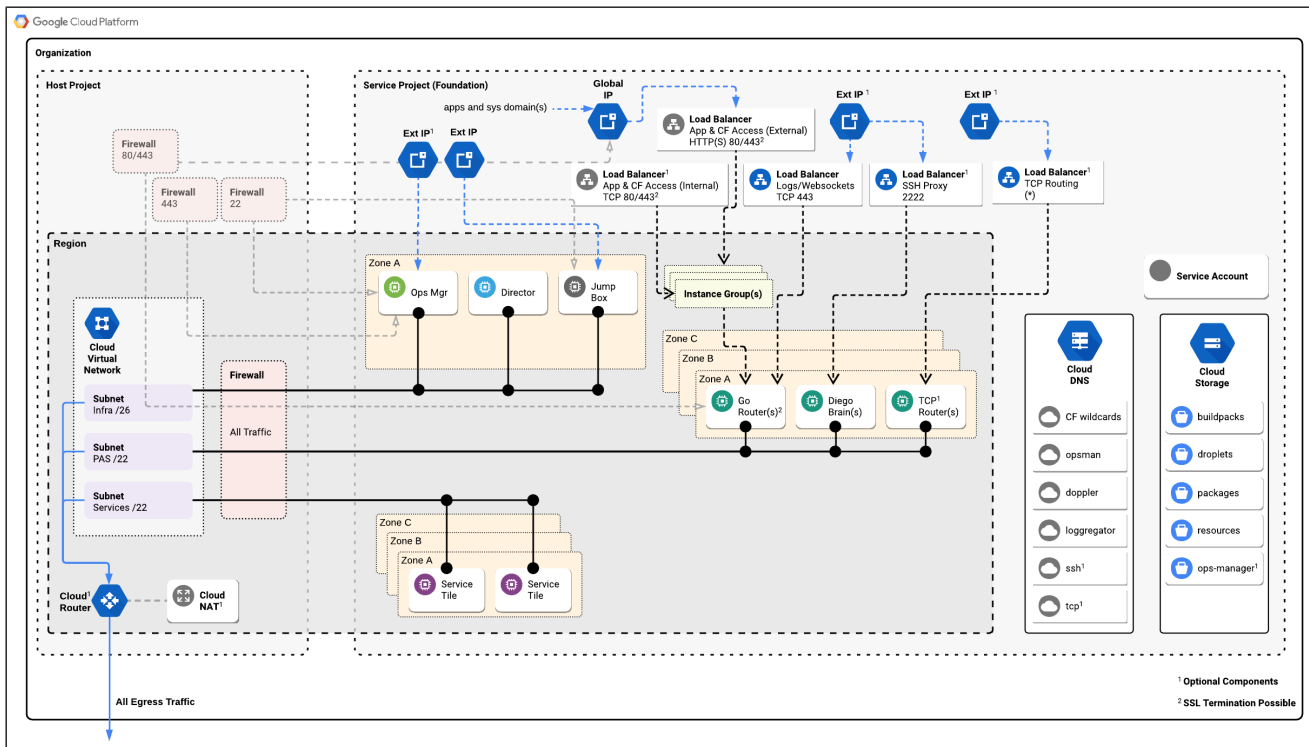
- Standalone deployments that do not connect to an internal network
- Test and experimental deployments, and for projects which do not belong to an organization

Shared VPC GCP Reference Architecture

The following diagram provides an overview of a reference architecture deployment of PCF on a shared VPC on GCP. This architecture requires an organization on the VPC that contains a host project and a service project.

For more information about shared VPCs on GCP, see [Shared VPC Overview](#) in the Google Cloud documentation.

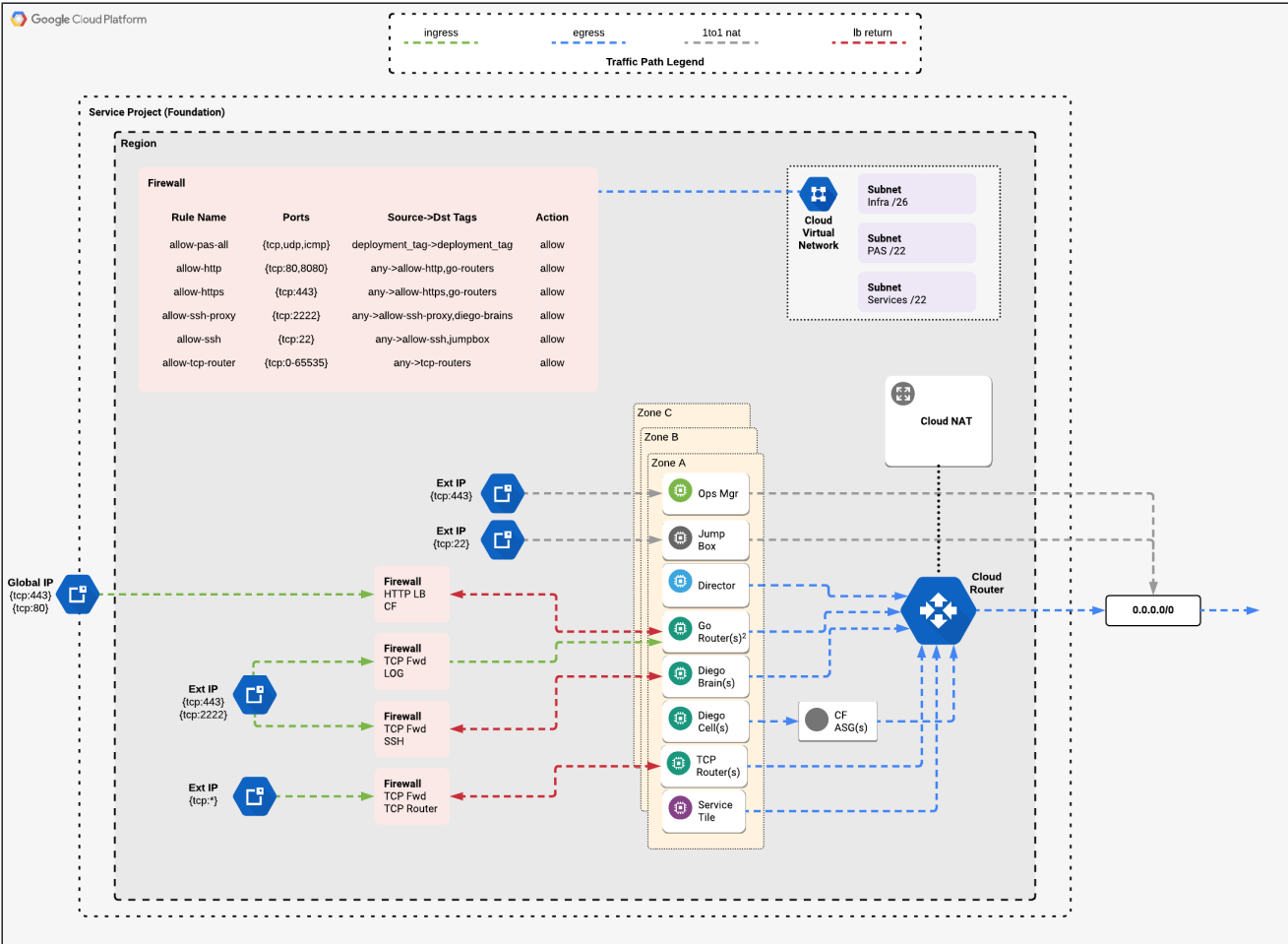
For more information about how this architecture divides resources between projects, see [Host / Service Architecture](#).



[View a larger version of this diagram.](#)

NAT Network Topology

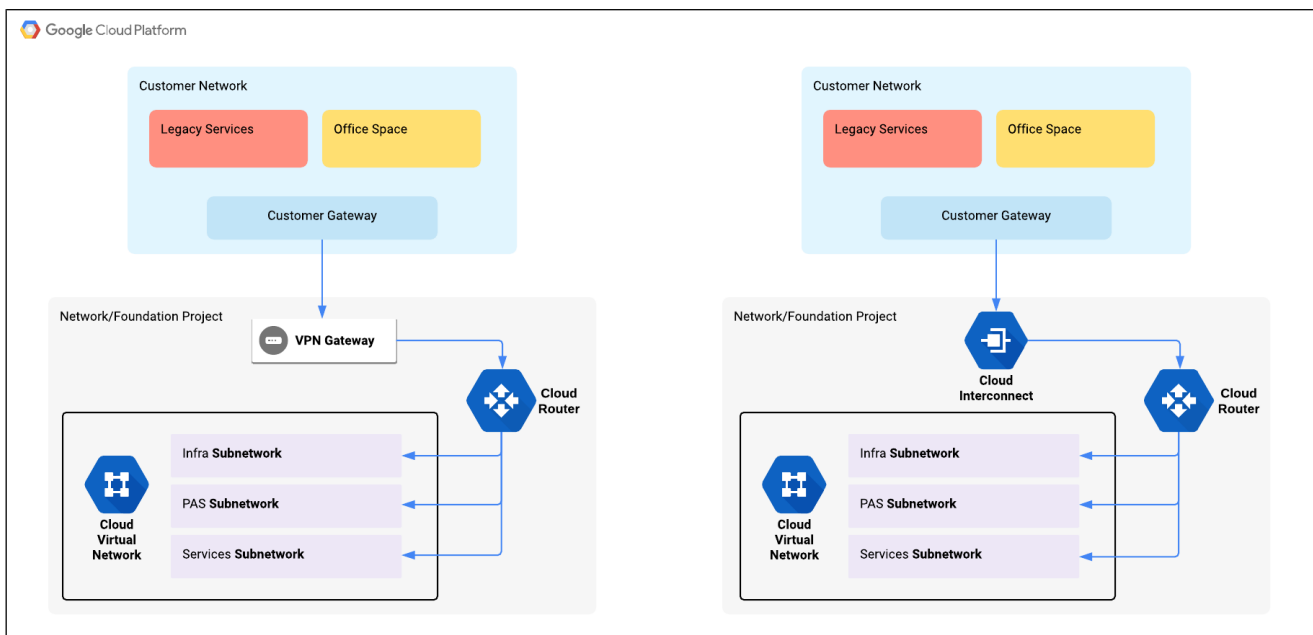
To expose a minimal number of public IP addresses, set up your NAT as shown in this diagram.



[View a larger version of this diagram.](#)

Cloud Interconnect

To speed communication between data centers, use Google Cloud Interconnect as shown in this diagram.



[View a larger version of this diagram.](#)

Host / Service Architecture

GCP allocates resources using a hierarchy that centers around projects. To create a VPC, architects define a *host project* that allocates network resources for the VPC, such as address space and firewall rules. Then they can define one or more *service projects* to run within the VPC, which share the network resources allocated by the host project and include their own non-network resources, such as VMs and storage buckets.

To install PCF in a shared VPC on GCP, you create a host project for the VPC and a service project dedicated to running PCF.

Host Project Resources

The host project centrally manages the following shared VPC network resources for PCF:

- Infra subnet (Ops Manager and BOSH Director)
- PAS subnet
- Services subnet
- Isolation Segments
- Firewall rules
- NAT instances and gateway
- VPN/interconnect
- Routes, e.g. egress internet through NAT or egress on-premises through VPN

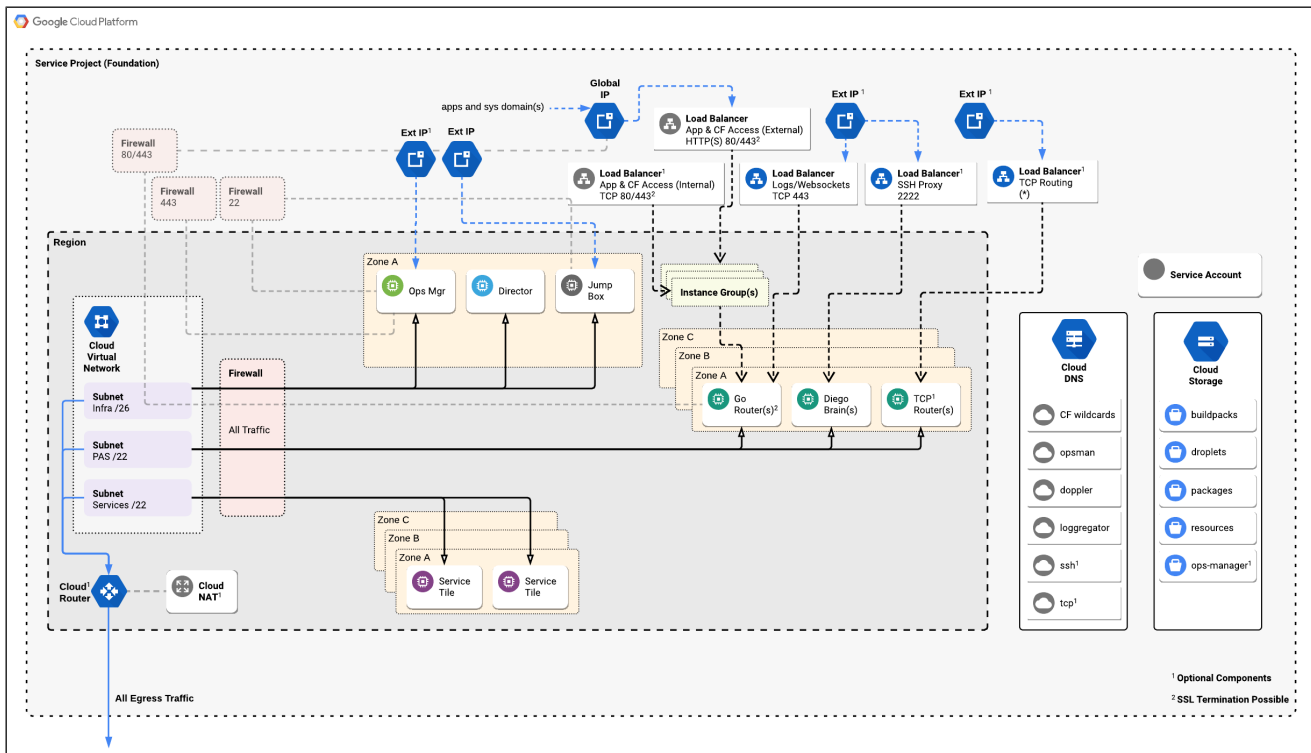
Service Project Resources

The PCF service project manages the following resources:

- Google Cloud Compute instances (VMs)
 - BOSH
 - Ops Manager
 - VMs deployed by BOSH, such as PCF and service components
- Google Cloud Storage buckets, for blobstore
 - BOSH Director
 - Resources
 - Buildpacks
 - Droplets
 - Packages
- Service account and a service account key for PCF to access the storage buckets
- A service account for PCF
- Load Balancers
- Google Cloud SQL instances, if using external databases

Single-Project VPC Base GCP Reference Architecture

The following diagram provides an overview of a reference architecture deployment of PCF on a single-project [VPC](#) on GCP.



[View a larger version of this diagram.](#)

Base Reference Architecture Components

The following table lists the components that are part of a reference architecture deployment with three availability zones.

| Component | Reference Architecture Notes |
|-----------------------------|---|
| Domains & DNS | CF Domain Zones and routes in use by the reference architecture include: domains for *.apps and *.system (required), a route for Ops Manager (required), a route for doppler (required), a route for Loggregator (required), a route for ssh access to app containers (optional) and a route for TCP routing to apps (optional). Reference architecture uses GCP Cloud DNS as the DNS provider. |
| Ops Manager | Deployed on the infrastructure subnet and accessible by FQDN or through an optional jumpbox. |
| BOSH Director | Deployed on the infrastructure subnet. |
| Gorouters | Accessed through the HTTP and TCP WebSockets load balancers. Deployed on the Pivotal Application Service (PAS) subnet, one job per availability zone. |
| Diego Brains | Required. However, the SSH container access functionality is optional and enabled through the SSH Proxy load balancer. Deployed on the PAS subnet, one job per availability zone. |
| TCP Routers | Optional feature for TCP routing. Deployed on the PAS subnet, one job per availability zone. |
| CF Database | Reference architecture uses GCP Cloud SQL rather than internal databases. Configure your database with a strong password and limit access only to components that require database access. |
| CF Blob Storage and Buckets | For buildpacks, droplets, packages and resources. Reference architecture uses Google Cloud Storage rather than internal file storage. |
| Services | Deployed on the PCF managed services subnet. Each service is deployed to each availability zone. |

Alternative GCP Network Layouts for PCF

This section describes the possible network layouts for PCF deployments as covered by the reference architecture of PCF on GCP.

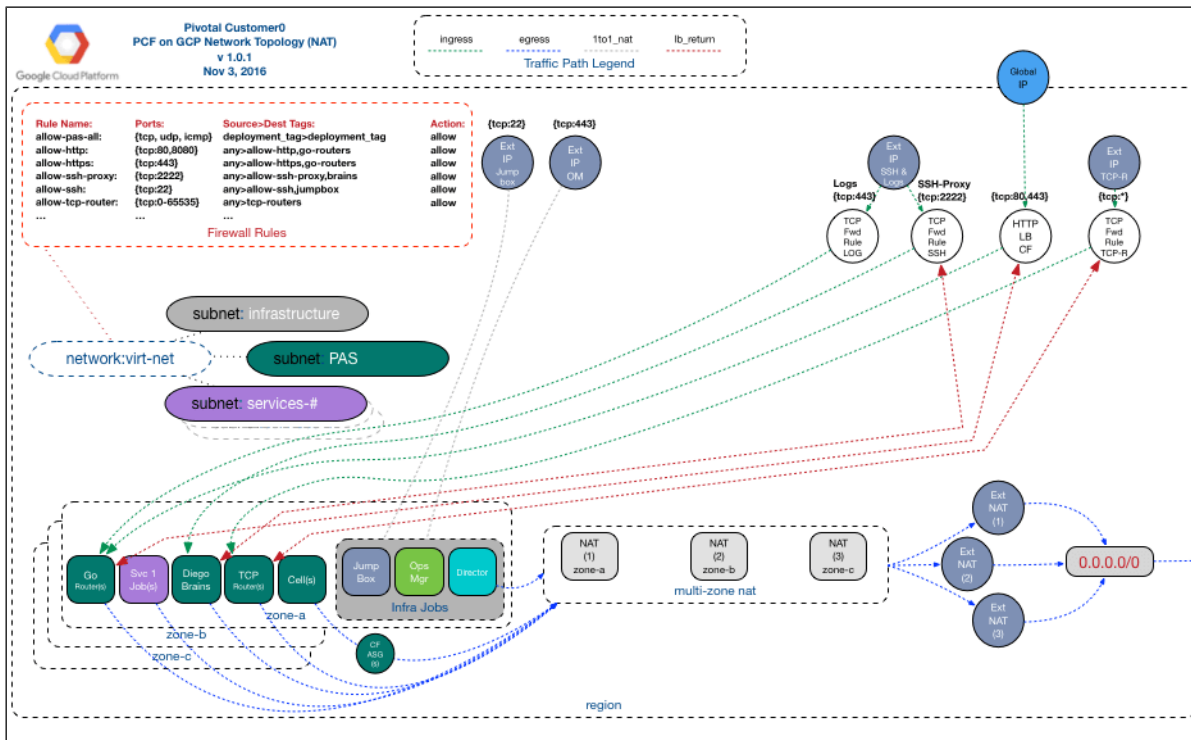
At a high level, there are currently two possible ways of granting public Internet access to PCF as described by the reference architecture:

- NAT provides connectivity from PCF internals to the public Internet.
 - The instructions for [Installing PCF on GCP Manually](#) use this method.
- Every PCF VM receives its own public IP address (no NAT).
 - The instructions for [Installing PCF on GCP using Terraform](#) use this method.

However, if you require NAT, you may refer to the following section.

NAT-based Solution

This diagram illustrates the case where you want to expose only a minimal number of public IP addresses.



[View a larger version of this diagram](#)

Public IP addresses Solution

If you prefer not to use a NAT solution, you can configure PCF on GCP to assign public IP addresses for all components. This type of deployment may be more performant since most of the network traffic between Cloud Foundry components are routed through the front end load balancer and the Gorouter.

Network Objects

The following table lists the network objects expected for each type of reference architecture deployment with three availability zones (assumes you are using NAT).

| Network Object | Notes | Minimum Number: NAT-based | Minimum Number: Public IP Addresses |
|----------------|---|---------------------------|-------------------------------------|
| External IPs | For a NAT solution, use global IP address for apps and system access, and Ops Manager or optional jumpbox | 2 | 30+ |
| NAT | One NAT per availability zone. | 3 | 0 |
| Network | One per deployment. GCP Network objects allow multiple subnets with multiple CIDRs, so a typical deployment of PCF will likely only ever require one GCP Network object | 1 | 1 |
| | Separate subnets for infrastructure (Ops Manager, BOSH Director, Jumpbox), PAS, and services. Using separate | | |

| | | | |
|------------------------------|---|----------------------------------|--|
| Subnets | subnets allows you to configure different firewall rules due to your needs. | Minimum Number: NAT-based | Minimum Number: Public IP Addresses |
| Network Object Routes | Routes are typically created by GCP dynamically when subnets are created, but you may need to create additional routes to force outbound communication to dedicated SNAT nodes. These objects are required to deploy PCF without public IP addresses. | | |
| Firewall Rules | GCP firewall rules are bound to a Network object and can be created to use IP ranges, subnets, or instance tags to match for source & destination fields in a rule. The preferred method use in the reference architecture deployment is instance tags. | 6+ | 6+ |
| Load balancers | Used to handle requests to Gorouters and infrastructure components. GCP uses two or more load balancers. The HTTP load balancer and TCP WebSockets load balancer are both required. The TCP Router load balancer used for TCP routing feature and the SSH load balancer that allows SSH access to Diego apps are both optional. The HTTP load balancer provides SSL termination. | 2+ | 2+ |
| Jumpbox | Optional. Provides a way of accessing different network components. For example, you can configure it with your own permissions and then set it up to access to Pivotal Network to download tiles. Using a jumpbox is particularly useful in IaaS where Ops Manager does not have a public IP address. In these cases, you can SSH into Ops Manager or any other component through the jumpbox. | (1) | (1) |

Network Communication in GCP Deployments

This section provides more background on the reasons behind certain network configuration decisions, specifically for the Gorouter.

Load Balancer to Gorouter Communications and TLS Termination

In a PCF on GCP deployment, the Gorouter receives two types of traffic:

1. Unencrypted HTTP traffic on port 80 that is decrypted by the HTTP(S) load balancer.
2. Encrypted secure web socket traffic on port 443 that is passed through the TCP WebSockets load balancer.

In a PCF on GCP deployment, the Gorouter receives two types of traffic:

1. Unencrypted HTTP traffic on port 80 that is decrypted by the HTTP(S) load balancer.
2. Encrypted secure web socket traffic on port 443 that is passed through the TCP WebSockets load balancer.

TLS is terminated for HTTPS on the HTTP load balancer and is terminated for WebSockets (WSS) traffic on the Gorouter.

PCF deployments on GCP use two load balancers to handle Gorouter traffic because HTTP load balancers currently do not support WebSockets.

ICMP

GCP routers do not respond to ICMP; therefore, Pivotal recommends disabling ICMP checks in [BOSH Director network configuration](#).

OpenStack Reference Architecture

This guide presents a reference architecture for Pivotal Cloud Foundry (PCF) on OpenStack. This architecture is valid for most production-grade PCF deployments in a single project using three availability zones (AZs).

See [OpenStack on PCF Requirements](#) for general requirements for running PCF and specific requirements for running PCF on OpenStack.

PCF Reference Architectures

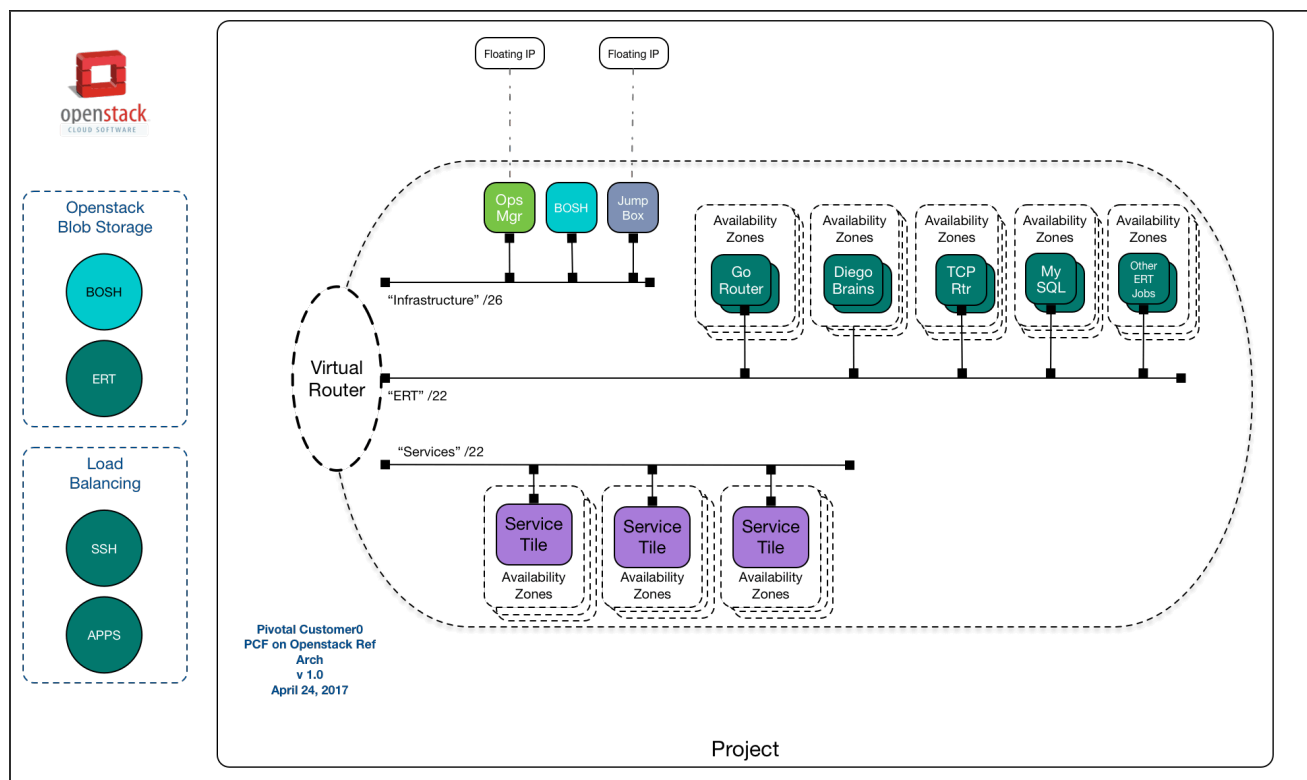
A PCF reference architecture describes a proven approach for deploying Pivotal Cloud Foundry on a specific IaaS, such as OpenStack, that meets the following requirements:

- Secure
- Publicly-accessible
- Includes common PCF-managed services such as MySQL, RabbitMQ, and Spring Cloud Services
- Can host at least 100 app instances, or far more

Pivotal provides reference architectures to help you determine the best configuration for your PCF deployment.

Base OpenStack Reference Architecture

The following diagram provides an overview of a reference architecture deployment of PCF on OpenStack using three AZs.



[View a larger version of this diagram.](#)

Base Reference Architecture Components


The following table lists the components that are part of a base reference architecture deployment on OpenStack with three AZs.


| Component | Reference Architecture Notes |
|-----------|--|
| | CF Domain zones and routes in use by the reference architecture include: |

| | |
|----------------------------------|--|
| Domains & DNS | <ul style="list-style-type: none"> • zones for *.apps and *.sys (required) • a route for Ops Manager (required) • a route for Doppler (required) • a route for Loggregator (required) • a route for ssh access to app containers (optional) • a route for tcp access to tcp routers (optional) |
| Ops Manager | Deployed on the infrastructure network and accessible by FQDN or through an optional jumpbox. |
| BOSH Director | Deployed on the infrastructure network. |
| Application Load Balancer | Required. Load balancer that handles incoming HTTP, HTTPS, TCP, and SSL traffic and forwards them to the Gorouters. Load balancers are outside the scope of this document. |
| SSH Load Balancer | Optional. Load balancer that provides SSH access to application containers for developers. Load balancers are outside the scope of this document. |
| Gorouters | Accessed through the Application Load Balancer. Deployed on the Pivotal Application Service (PAS) network, one per AZ. |
| Diego Brains | This component is required. However, the SSH container access functionality is optional and enabled through the SSH Load Balancers. Deployed on the PAS network, one per AZ. |
| TCP Routers | Optional feature for TCP routing. Deployed on the PAS network, one per AZ. |
| CF Database | Reference architecture uses internal MySQL. |
| Storage Buckets | Reference architecture uses customer provided blobstore. Buckets are needed for BOSH and PAS. |
| Service Tiles | Deployed on the services network. |
| Service Accounts | <p>Two service accounts are recommended: one for OpenStack “paving,” and the other for Ops Manager and BOSH. Consult the following list:</p> <ul style="list-style-type: none"> • Admin Account: Concourse will use this account to provision required OpenStack resources as well as a Keystone service account. • Keystone Service Account: This service account will be automatically provisioned with restricted access only to resources needed by PCF. |
| OpenStack Quota | The default compute quota on a new OpenStack subscription is typically not enough to host a multi-AZ deployment. The recommended quota for instances is 100. Your OpenStack network quotas may also need to be increased. |

OpenStack Objects

The following table lists the network objects in this reference architecture.

| Network Object | Notes | Estimated Number |
|------------------------------|--|------------------|
| Floating IP addresses | Two per deployment. One assigned to Ops Manager, the other to your jumpbox. | 2 |
| Project | One per deployment. A PCF deployment exists within a single project and a single OpenStack region, but should distribute PCF jobs and instances across three OpenStack AZs to ensure a high degree of availability. | 1 |
| Networks | <p>The reference architecture requires the following Tenant Networks:</p> <ul style="list-style-type: none"> • 1 x (/24) Infrastructure (Ops Manager, BOSH Director, Jumpbox). • 1 x (/20) PAS (Gorouters, Diego Cells, Cloud Controllers, etc.). • 1 x (/20) Services (RabbitMQ, MySQL, Spring Cloud Services, etc.) • 1 x (/24) On-demand services (Various.) <p>An Internet-facing network is also required:</p> <ul style="list-style-type: none"> • 1 x Public network. <p> Note: In many cases, the public network is an “under the cloud” network that is shared across projects.</p> | 5 |
| | This reference architecture requires one router attached to all networks: | |

| Routers | <ul style="list-style-type: none">VirtualRouter: This router table enables the ingress/egress routes from/to Internet to the project networks and provides sNAT services. | 1 | | | | | | | | | | | | | | | | | | | | |
|-----------------|--|----------------|---------------|--|----------|-------------|----------|-------------|-----------|------|------------------------------|----------|-------------|-----------|-------|--|-------|------------------|----------|-----|--|---|
| Security Groups | <p>The reference architecture requires one Security Groups. The following table describes the Security Group ingress rules:</p> <table><tr><th>Security Group</th><th>Port</th><th>From CIDR</th><th>Protocol</th><th>Description</th></tr><tr><td>OpsMgrSG</td><td>22</td><td>0.0.0.0/0</td><td>TCP</td><td>Ops Manager SSH access</td></tr><tr><td>OpsMgrSG</td><td>443</td><td>0.0.0.0/0</td><td>TCP</td><td>Ops Manager HTTP access</td></tr><tr><td>VmsSG</td><td>ALL</td><td>VPC_CIDR</td><td>ALL</td><td>Open up connections among BOSH-deployed VMs</td></tr></table> <p>Additional security groups may be needed which are specific to your chosen load balancing solution.</p> | Security Group | Port | From CIDR | Protocol | Description | OpsMgrSG | 22 | 0.0.0.0/0 | TCP | Ops Manager SSH access | OpsMgrSG | 443 | 0.0.0.0/0 | TCP | Ops Manager HTTP access | VmsSG | ALL | VPC_CIDR | ALL | Open up connections among BOSH-deployed VMs | 5 |
| Security Group | Port | From CIDR | Protocol | Description | | | | | | | | | | | | | | | | | | |
| OpsMgrSG | 22 | 0.0.0.0/0 | TCP | Ops Manager SSH access | | | | | | | | | | | | | | | | | | |
| OpsMgrSG | 443 | 0.0.0.0/0 | TCP | Ops Manager HTTP access | | | | | | | | | | | | | | | | | | |
| VmsSG | ALL | VPC_CIDR | ALL | Open up connections among BOSH-deployed VMs | | | | | | | | | | | | | | | | | | |
| Load Balancers | <p>PCF on OpenStack requires a load balancer, which can be configured with multiple listeners to forward HTTP/HTTPS/TCP traffic. Two load balancers are recommended: one to forward the traffic to the Gorouters, <code>AppsLB</code> , the other to forward the traffic to the Diego Brain SSH proxy, <code>SSHLB</code> .</p> <p>The following table describes the required listeners for each load balancer:</p> <table><tr><th>Name</th><th>Instance/Port</th><th>LB Port</th><th>Protocol</th><th>Description</th></tr><tr><td>AppsLB</td><td>gorouter/80</td><td>80</td><td>HTTP</td><td>Forward traffic to Gorouters</td></tr><tr><td>AppsLB</td><td>gorouter/80</td><td>443</td><td>HTTPS</td><td>SSL termination and forward traffic to Gorouters</td></tr><tr><td>SSHLB</td><td>diego-brain/2222</td><td>2222</td><td>TCP</td><td>Forward traffic to Diego Brain for container SSH connections</td></tr></table> <p>Each load balancer needs a check to validate the health of the back-end instances:</p> <ul style="list-style-type: none"><code>AppsLB</code> checks the health on Gorouter port 80 with TCP<code>SSHLB</code> checks the health on Diego Brain port 2222 with TCP <div> Note: In many cases, the load balancers are provided as an “under the cloud” service that is shared across projects.</div> | Name | Instance/Port | LB Port | Protocol | Description | AppsLB | gorouter/80 | 80 | HTTP | Forward traffic to Gorouters | AppsLB | gorouter/80 | 443 | HTTPS | SSL termination and forward traffic to Gorouters | SSHLB | diego-brain/2222 | 2222 | TCP | Forward traffic to Diego Brain for container SSH connections | 2 |
| Name | Instance/Port | LB Port | Protocol | Description | | | | | | | | | | | | | | | | | | |
| AppsLB | gorouter/80 | 80 | HTTP | Forward traffic to Gorouters | | | | | | | | | | | | | | | | | | |
| AppsLB | gorouter/80 | 443 | HTTPS | SSL termination and forward traffic to Gorouters | | | | | | | | | | | | | | | | | | |
| SSHLB | diego-brain/2222 | 2222 | TCP | Forward traffic to Diego Brain for container SSH connections | | | | | | | | | | | | | | | | | | |
| Jumpbox | Optional. Provides a way of accessing different network components. For example, you can configure it with your own permissions and then set it up to access to Pivotal Network to download tiles. Using a jumpbox is particularly useful in IaaS where Ops Manager does not have a public IP address. In these cases, you can SSH into Ops Manager or any other component through the jumpbox. | 1 | | | | | | | | | | | | | | | | | | | | |

vSphere Reference Architecture

This guide provides reference architectures for Pivotal Cloud Foundry (PCF), including Pivotal Application Service (PAS) and Pivotal Container Service (PKS), on vSphere.

Overview

Pivotal validates the reference architectures described in this topic against multiple production-grade usage scenarios.

This document does not replace the installation instructions provided in the [PCF on vSphere Requirements](#) topic. Instead, it gives examples of how to apply those instructions to real-world production environments.

| PCF Products Validated | Version |
|--|----------------|
| vSphere | 6.5 |
| VMware NSX-T | 2.2 |
| Pivotal Cloud Foundry Operations Manager | 2.2 or later |
| PAS | 2.2 or later |
| PKS | 1.1.5 or later |

Base vSphere Reference Architecture

This reference architecture includes VMware vSphere and NSX-T, a software-defined network virtualization platform that runs on VMware ESXi virtual hosts.

The reference architecture supports capacity growth at the vSphere and PCF levels as well as installation security through the NSX-T firewall. It allocates a minimum of three servers to each cluster and spreads PCF components across three clusters for high availability (HA). For information about HA in PCF, see [High Availability in Cloud Foundry](#).

To use all features listed in this topic for your PAS installation, you must have **Advanced** or above licensing from VMware for NSX-T. For PKS, the required licensing is included by default.

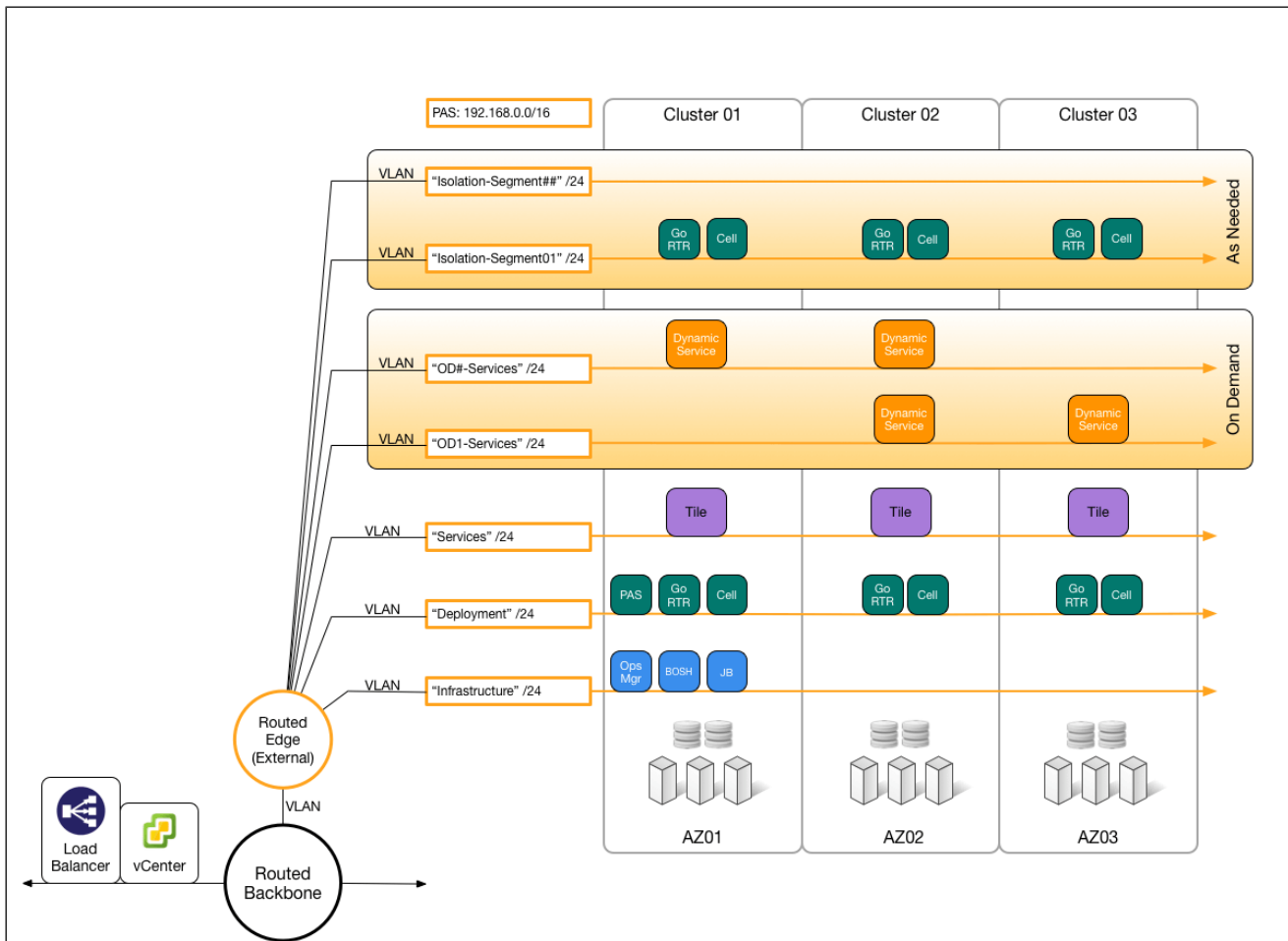
If you want to deploy PCF without NSX-T, see [vSphere Reference Architecture](#), which includes NSX-V design considerations.

Non-SDN Deployments

This section provides information about VLAN and container-to-container networking considerations for PCF deployments that do not use software-defined networking (SDN).

VLAN Considerations

Without an SDN environment, you draw network address space and broadcast domains from the greater data center pool. For this approach, you need to deploy PAS and PKS in a particular alignment.



[View a larger version of this diagram](#)

When designing a non-SDN environment, ensure that VLANs and address space for PAS and PKS do not overlap. In addition, note that non-SDN PCF environments have the following characteristics:

- Load balancing is performed external to the PCF installation.
- Client SSL termination must happen either at the load balancer or Gorouters, or both. Ensure your certificates can accomplish this.
- Firewall layer is accomplished external to the PCF installation.

Container-to-Container Networking and CNI Considerations

Changing your container-to-container networking strategy after deployment is possible. However, with NSX-T, you need both the VMware NSX-T Container Plug-In for PCF tile and NSX-T infrastructure. For information about deploying PAS on vSphere with NSX-T internal networking using the VMware NSX-T Container Plug-In for PCF tile, see [Deploying PAS with NSX-T Networking](#).

Migrating from a non-SDN environment to an SDN-enabled solution is possible but best considered as a greenfield deployment. Inserting an SDN layer under an active PCF installation is disruptive.

PAS Without SDN

You can use PAS without an SDN overlay. For more information, see [PCF on vSphere Requirements](#).

PKS Without SDN

NSX-T SDN is included in PKS by default, along with the associated licensing. Alternatively, you can use a built-in network stack, Flannel, which handles container networking.

If you want to deploy PKS without NSX-T, select **Flannel** as your container networking interface in the **Networking** pane of the PKS tile. For information

about configuring your container networking interface, see the [Networking](#) section in *Installing PKS on vSphere*.


In addition, you must define networks for deploying PKS and PKS-provisioned Kubernetes clusters. For information about defining these networks in Ops Manager, see the [Create Networks Page](#) section in *Configuring Ops Manager on vSphere*.

SDN-Enabled Deployments With NSX-T

This section provides information about network requirements, routing, and load balancing for PAS and PKS deployments that use SDN.

Network Requirements for PAS

PAS requires a number of statically defined networks to host the main components it is composed of. For the Tenant side of an NSX-T deployment, a series of non-routable address banks that the NSX-T routers will manage is defined as follows:

 **Note:** These static networks have a smaller host address space assigned than reference designs for PCF v1.xx.

- Infrastructure: 192.168.1.0/24
- Deployment: 192.168.2.0/24
- Services: 192.168.3.0/24
The Services network can be used with other Ops Manager tiles that you install in addition to PAS. Some of these tiles may require on-demand network capacity. Pivotal recommends that you consider adding a network per tile that needs on-demand resources and pair them up in the tile's configuration. For more information, see *OD-Services#* below.
- OD-Services#: 192.168.4.0 - 192.168.9.0 in /24 segments
For example, the Redis for PCF tile asks for Network and Services Network. The first one is for placing the broker, and the second one is for deploying worker VMs to support the service. In this scenario, you can deploy a new network OD-Services1 and instruct Redis for PCF to use the Services network for the broker and the OD-Services1 network for the workers. The next tile can use the Services network for the broker and a new OD-Services2 network for workers and so on.
- Isolation Segments: 192.168.10.0 - 192.168.63.0 in /24 segments
Isolation segments can be added to an existing PAS installation. This range of address space is used when you add one or more segments. A /24-network in this range should be deployed for each new isolation segment. The capacity of this address bank is sufficient for more than 50 isolation segments, each having more than 250 VMs.
- PAS Dynamic Orgs: 192.168.128.0/17 = 128 orgs/foundation
Dynamically assigned Org networks are attached to automatically generated NSX-T Tier-1 routers. Instead of defining these networks in Ops Manager, the operator provides a non-overlapping block of address space. This is configurable in the NCP pane of the VMware NSX-T Container Plug-In for PCF tile in Ops Manager. Every Org receives a new /24 network.

This reference uses a pattern that follows previous references. However, all networks now break on the /24 boundary, and the network octet is numerically sequential (1-2-3).

Network Requirements for PKS

When deploying PKS through Ops Manager, you must allocate a block of address space for dynamic networks that PKS will deploy per namespace.

Network requirements for PKS are as follows:

- PKS Clusters: 172.24.0.0/14
- PKS Pods: 172.28.0.0/14

Summary

The complete addressing strategy for both PAS and PKS is as follows:

- Infrastructure: 192.168.1.0/24
- Deployment: 192.168.2.0/24
- Services: 192.168.3.0/24
- OD-Services#: 192.168.4.0 - 192.168.9.0 in /24 segments

- Isolation Segments: 192.168.10.0 - 192.168.63.0 in /24 segments
- Undefined: 192.168.64.0 - 192.168.127.0
- PAS Dynamic Orgs: 192.168.128.0/17
- PKS Clusters: 172.24.0.0/14
- PKS Pods: 172.28.0.0/14

Network Requirements for External Routing

Routable external IPs on the provider side, for example, for NATs, PAS orgs, and load balancers, are assigned to the T0 router, which is located in front of the PCF installation. There are two approaches to assigning address space blocks to this job:

- Without PKS or with PKS Ingress: The T0 router needs some routable address space to advertise on the BGP network with its peers. Select a network range with ample address space that can be split into two logical jobs: one job is advertised as a route for traffic, and the other job is for aligning T0 DNATs and SNATs, load balancers, and other jobs. Unlike with NSX-V, SNATs consume much more address space than before.
- With PKS No Ingress: Compared to the approach above, this approach has much higher address space consumption for load balancer VIPs. Therefore, allow for 4x the address space because Kubernetes service types allocate addresses frequently.

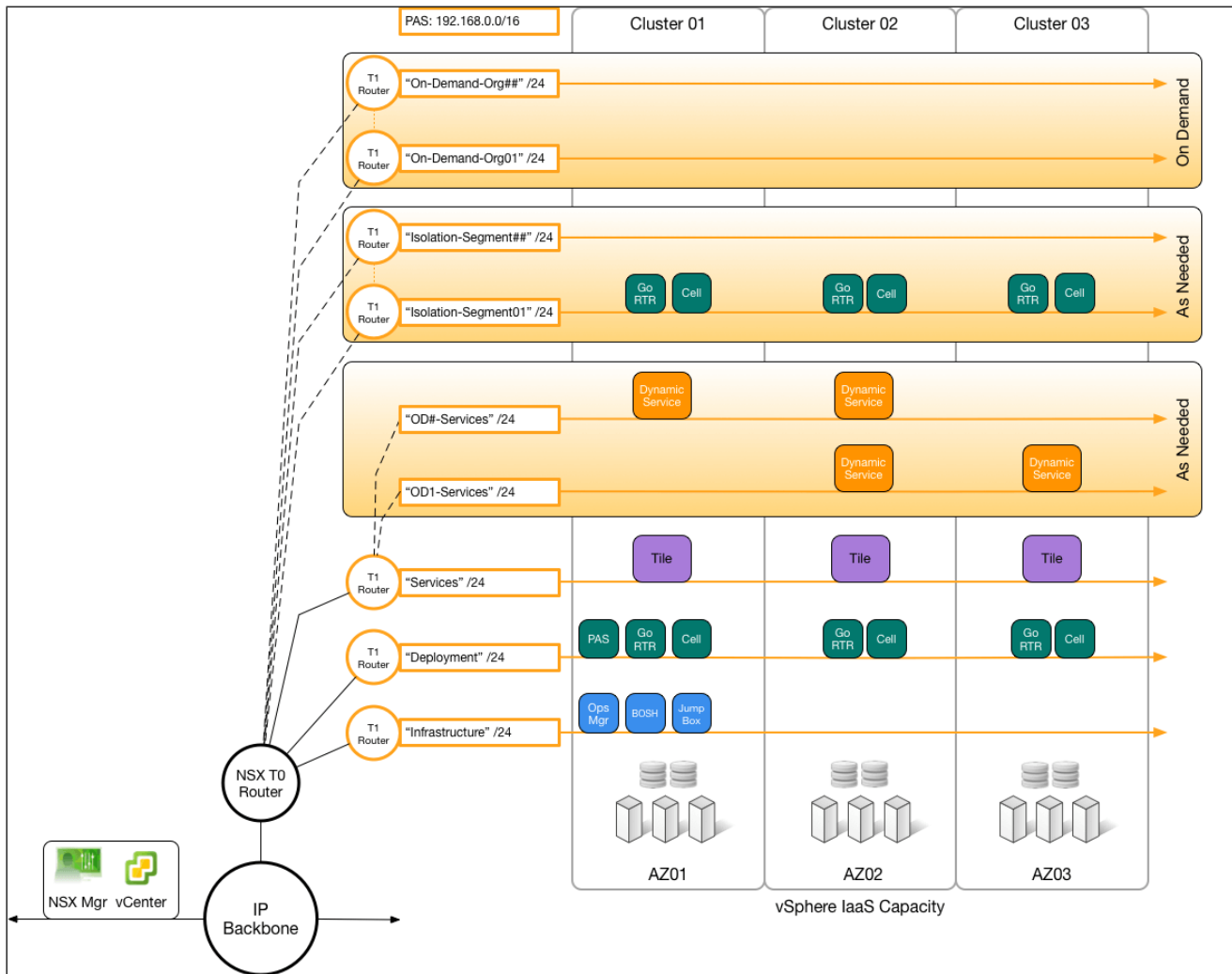
Provider routable address space is /25 or /23 for PKS No Ingress.

NSX-T handles the routing between a T0 router and any T1 routers associated with it.

PAS with NSX-T

Expanding PAS with SDN features is best considered as a greenfield effort. Inserting an SDN layer under a working PAS installation is non-trivial and likely triggers a rebuild. NSX-T constructs that can be used by PAS include the following:

- Logical networks, encapsulated broadcast domains
- VLAN exhaustion avoidance through the use of logical networks
- Routing services and NAT/SNAT to network fence the PCF installation
- Load balancing services to pool systems such as Gorouters
- SSL termination at the load balancer
- Distributed routing and firewall services at the hypervisor



[View a larger version of this diagram](#)

The VMware NSX-T Container Plug-In for PCF tile, which provides a container networking stack instead of the built-in Silk solution, interlocks with NSX-T already deployed on the IaaS. This tile cannot be used unless NSX-T has already been established on the IaaS. These technologies cannot be retrofitted into an established PKS or PAS installation.

To deploy PAS with NSX-T, you need to provide the following in the VMware NSX-T Container Plug-In for PCF tile:

- NSX Manager host
- Username and password
- NSX Manager CA certificate
- PAS foundation name that must match the tag added to T0 router, external NAT pool, and IP block
- Subnet prefix, which controls the size of each org and defaults to /24, that is, 254 addresses

In addition, you must select **Enable SNAT for Container Networks** in the tile. For more information about configuring PAS with NSX-T networking, see [Deploying PAS with NSX-T Networking](#).

Each new job, such as an isolation segment, falls to a broadcast domain or logical switch connected to a T1 router acting as the gateway to that network. This approach provides a DNAT and SNAT control point and a firewall boundary.

The Services network is an exception. It shares a T1 router with any associated OD-Services# networks. Because these networks are considered part of the same system, inserting any NATs or firewall rules between them is not needed.

Load Balancing for PAS

Without NSX-T, you need to choose a suitable load balancer to send traffic to the Gorouters and other systems. Installations approaching production level typically use external load balancing from hardware appliance vendors or other network-layer solutions.

With NSX-T, load balancing is available in the SDN layer. These load balancers are a logical entity tied to the resources in the Edge Cluster and align to the network or networks represented by a T1 router. They function as a Layer 4 load balancer. SSL termination is available on the NSX-T load balancer. However, Pivotal recommends passing the SSL through to your Gorouters.

Common deployments of load balancing in PAS are as follows:

- HTTP/HTTPS traffic to and from Gorouters
- TCP traffic to and from TCP routers
- Diego Brain

NSX-T load balancers can support many VIPs. Consider deploying one load balancer per network (T1) and one-to-many VIPs on that load balancer per job. Edge Cluster resources are consumed for load balancing. When designing your deployment, consider how many load balancers are needed and how much capacity is available for them.

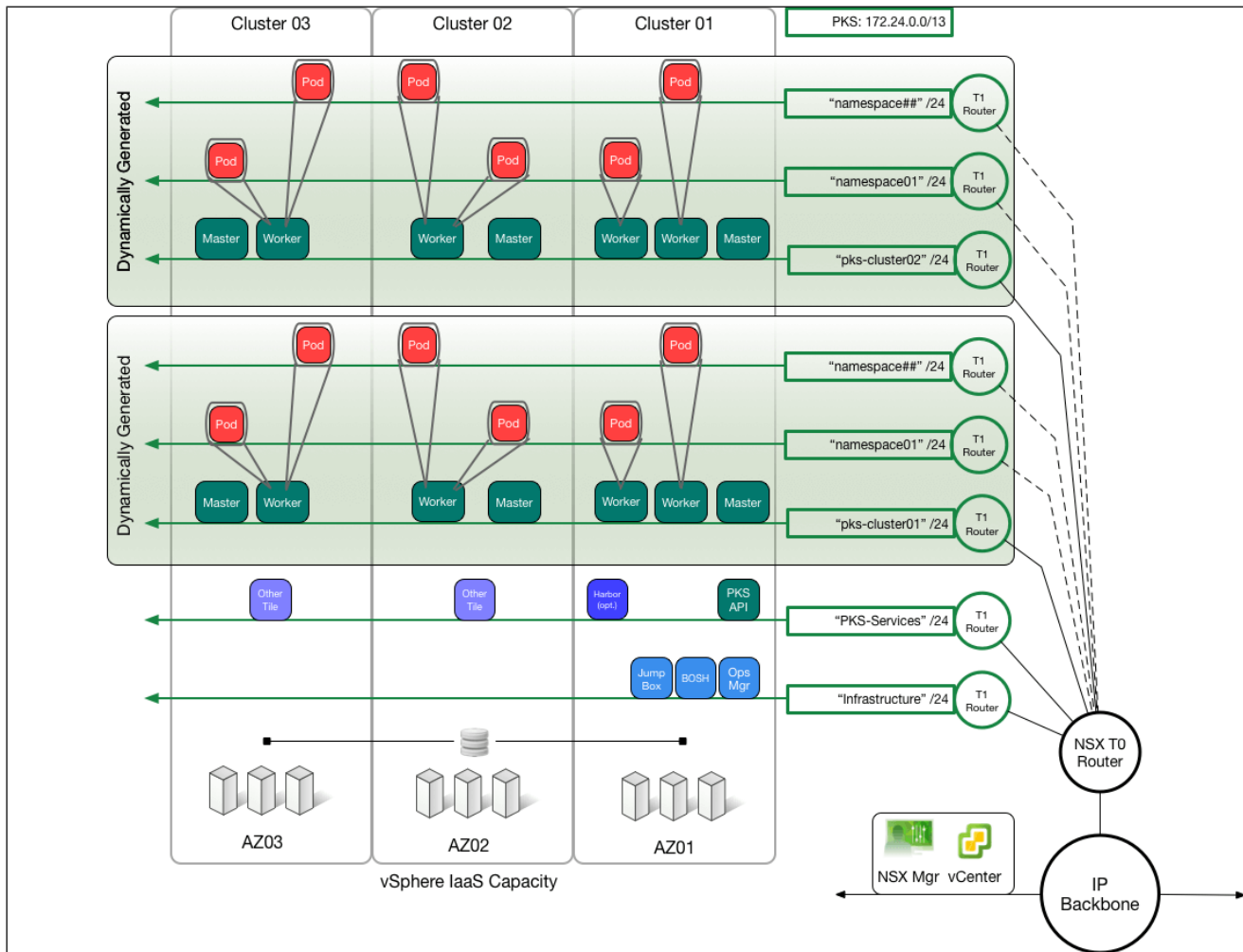
BOSH can manage the members of the server pools for the NSX-T load balancers using NS Groups.

PKS with NSX-T

NSX-T SDN is included in PKS by default, along with the associated licensing. To use NSX-T SDN and its dynamic constructs, you need to provide the following information when configuring PKS:

- NSX Manager host
- Username and password
- NSX Manager CA certificate
- T0 router to connect dynamically created namespace networks to
- NSX IP block from which to pull networks for pods per namespace
- NSX IP block from which to pull networks for each new cluster
- Floating IP pool ID created for externally facing IPs (NATs and VIPs)

For more information about configuring PKS with NSX-T networking, see [Installing and Configuring PKS with NSX-T Integration](#).



[View a larger version of this diagram](#)

New T1 routers are deployed on-demand as new namespaces are added to PKS. Because these can grow rapidly, allocate a large Pod IP block such as /14 in NSX-T, and then NSX-T provisions /24 address blocks for new namespaces. Reference the Pod IP block from your PKS tile configuration.

PKS v1.1.5 and later supports multiple master nodes. The number of master nodes is defined per plan in the PKS tile. You must use an odd number of master nodes to allow etcd to form a quorum. Pivotal recommends using at least 1 master node per AZ for HA and disaster recovery.

With NSX-T SDN, networks for both PKS clusters and pods are created dynamically. Pivotal recommends using multiple clusters instead of a single cluster with multiple namespaces. Multiple clusters provide security, customization per cluster, privileged containers, failure domains, and version choice.

Ingress Routing and Load Balancing for PKS

This section provides information about ingress routing (Layer 7) and load balancing (Layer 4) for your PKS deployment.

Ingress Routing

NSX-T provides a native ingress router. Third-party options include Istio or Nginx that are running as containers in the cluster.

Wildcard DNS entries are needed for pointing at the ingress service in the style of Gorouters in PAS. Domain information for ingress is defined in the manifest of your Kubernetes deployment. See the example below.

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: music-ingress
  namespace: music1
spec:
  rules:
  - host: music1.pks.domain.com
    http:
      paths:
      - path: /*
        backend:
          serviceName: music-service
          servicePort: 8080
```

Load Balancing

When pushing a Kubernetes deployment with `type` set to `LoadBalancer`, NSX-T automatically creates a new VIP for the deployment on the existing load balancer for that namespace.

You need to specify a listening and translation port in the service, along with a name for tagging. You also specify a protocol to use. See the example below.

```
apiVersion: v1
kind: Service
metadata:
  ...
spec:
  type: LoadBalancer
  ports:
  - port: 80
    targetPort: 8080
    protocol: TCP
    name: web
```

Storage Design

Shared storage is a requirement for PCF. You can allocate networked storage to the host clusters following one of two common approaches: horizontal or vertical. The approach you follow should reflect how your data center arranges its storage and host blocks in its physical layout.

The following describes the vertical and horizontal approaches to configuring shared storage:

- **Vertical:** You grant each cluster its own dedicated datastores, creating a cluster-aligned storage strategy. vSphere VSAN is an example of this architecture. The vertical alignment is the preferred choice for PCF as it matches the AZ model of the PaaS. Loss of storage in a cluster constitutes loss on an AZ, which is a recoverable failure when at least two more AZs are operational.
For example, with six datastores `ds01` through `ds06`, you assign datastores `ds01` and `ds02` to your first cluster, `ds03` and `ds04` to your second cluster, and `ds05` and `ds06` to your third cluster. You then instruct your first PCF installation to use `ds01`, `ds03`, and `ds05` and your second PCF installation to use `ds02`, `ds04`, and `ds06`. In this arrangement, all VMs in the same installation and cluster share a dedicated datastore.
- **Horizontal:** You grant all hosts access to all datastores and assign a subset to each installation.
For example, with six datastores `ds01` through `ds06`, you grant all nine hosts access to all six datastores. You then instruct your first PCF installation to use stores `ds01` through `ds03` and your second PCF installation to use `ds04` through `ds06`.

Warning: If you use the horizontal storage design approach, any storage loss could affect datastores in all AZs. This could result in downtime and unrecoverable loss of data. To avoid downtime and data loss, Pivotal recommends implementing the vertical storage design approach or implementing strong redundancy design at the storage array.

Highly redundant storage systems, such as hyperconverged systems, are the optimal choice for a fully HA PaaS. In addition, hyperconverged systems scale with capacity growth and are aligned to the AZ strategy of PCF.

To improve the resiliency of your deployment, you can use separate storage for the management plane of PCF, Ops Manager and BOSH, as well as separate storage for the blobstore.

Note: If a datastore is part of a vSphere storage cluster using sDRS (Storage DRS), you must disable the s-vMotion feature on any datastores used by PCF. Otherwise, s-vMotion activity can rename independent disks and cause BOSH to malfunction. For more information, see [How to Migrate PCF to a New Datastore in vSphere](#).

Storage Capacity

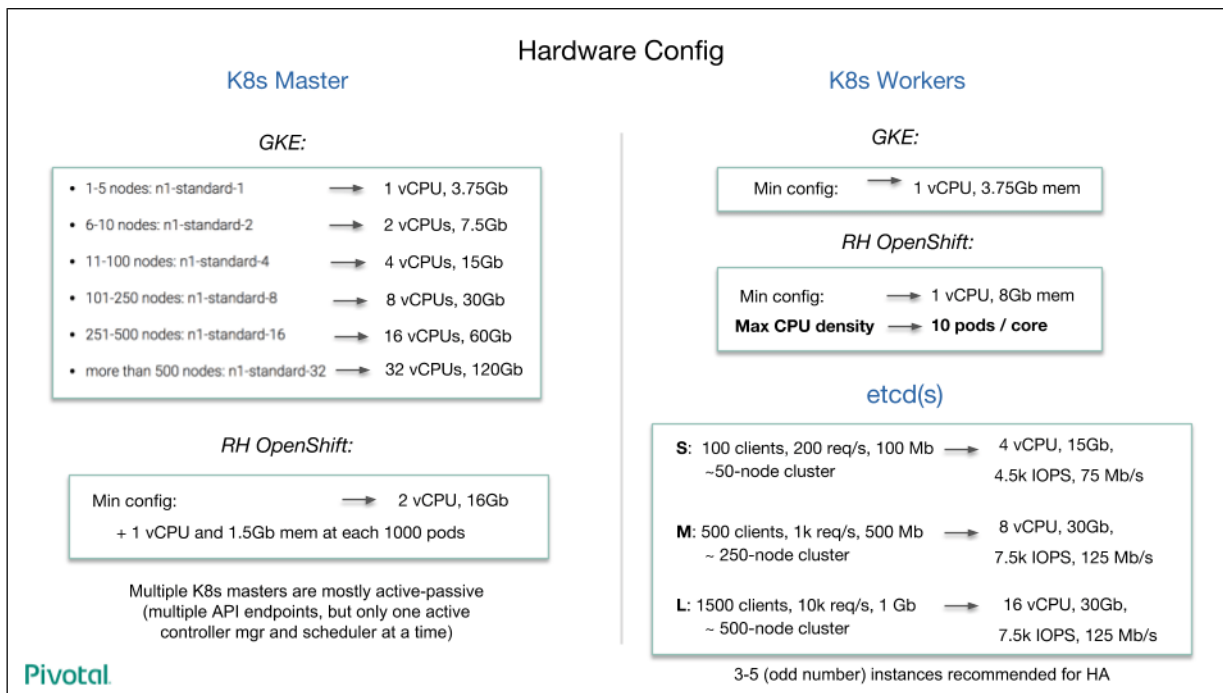
Pivotal recommends the following capacity allocation for PAS installations:

- For production use, at least 8 TB of data storage, either as one 8-TB store or a number of smaller volumes adding up to 8 TB. Frequent development may require significantly more storage to accommodate new code and buildpacks.
- For small installations, 4-6 TB of data storage is recommended.

The primary consumer of storage is NFS or WebDAV.

Note: PCF does not currently support using vSphere storage clusters with the versions of PCF validated for this reference architecture. Datastores should be listed in the vSphere tile by their native name, not the cluster name created by vCenter for the storage cluster.

When planning storage allocation for PKS installations based on Pod and Node needs, consider the following chart.



Compute and HA Considerations

In PAS, a consolidation ratio for containers should follow a conservative 4:1 ratio of vCPUs to pCPUs. You can use a more conservative ratio, which is 2:1.

A standard Diego cell is 4x16 (XL) by default. At a 4:1 ratio, you have a 16-vCPU budget, or about 12 containers.

If you want to run more containers in a cell, scale the vCPUs accordingly. However, high core count VMs become increasingly hard to schedule on the pCPU without high physical core counts in the socket.

HA considerations include the following:

- For non-production environments, the number of AZs that PAS requires for HA depends on the location of its system databases.
 - With external databases, PAS requires at least two AZs for HA.
 - With internal system databases, PAS requires at least three AZs for HA.

PCF achieves redundancy through the AZ construct and the loss of an AZ is not considered catastrophic. BOSH Resurrector can replace lost VMs as needed to repair a foundation. Foundation backup and restoration is accomplished externally by BOSH Backup and Restore (BBR). For information about BBR, see [Backing Up and Restoring Pivotal Cloud Foundry](#).

- PKS has no inherent HA capabilities to design for. To support PKS, design HA at the IaaS, storage, power, and access layers.

PCF achieves redundancy through the AZ construct, and the loss of an AZ is not considered catastrophic. BOSH Resurrector replaces lost VMs as needed to repair a foundation.

Foundation backup and restoration is accomplished externally by BOSH Backup and Restore (BBR). For information about BBR, see [Backing Up and](#)

[Restoring Pivotal Cloud Foundry](#) [↗](#).

Scaling and Capacity Management

This section provides information about scaling and capacity management for PCF.

Small PCF Installations

A small-sized PCF foundation looks as follows:

- 1 vSphere cluster/1 AZ
- 2 resource pools: 1 for NSX components and 1 for PAS or PKS
- 3 hosts minimum for vSphere HA (4 hosts for vSphere VSAN)
- Shared storage/VSAN
- 1 NSX Manager
- 3 NSX controllers
- 2 large edge VMs in a cluster
- PCF: Ops Manager, the BOSH Director, and Small Footprint Runtime

This approach is intended for designing a proof of concept or development-only system. Small Footprint Runtime has no upgrade path to the standard PAS tile.

Medium PCF Installations

A medium-sized PCF foundation looks as follows:

- 2 vSphere clusters/2 AZs
- 3 resource pools: 1 for NSX components and 2 for PAS/1 for PKS
- 3 hosts minimum for vSphere HA (4 hosts for vSphere VSAN) per cluster
- Shared storage/VSAN
- 1 NSX Manager
- 3 NSX controllers
- 2 large edge VMs in a cluster
- PCF: Ops Manager, the BOSH Director, and PAS/PKS

For this design, Pivotal recommends replacing Small Footprint Runtime with PAS. The second AZ doubles compute capacity and expands the NSX-T footprint.

Production-Ready PCF Installations

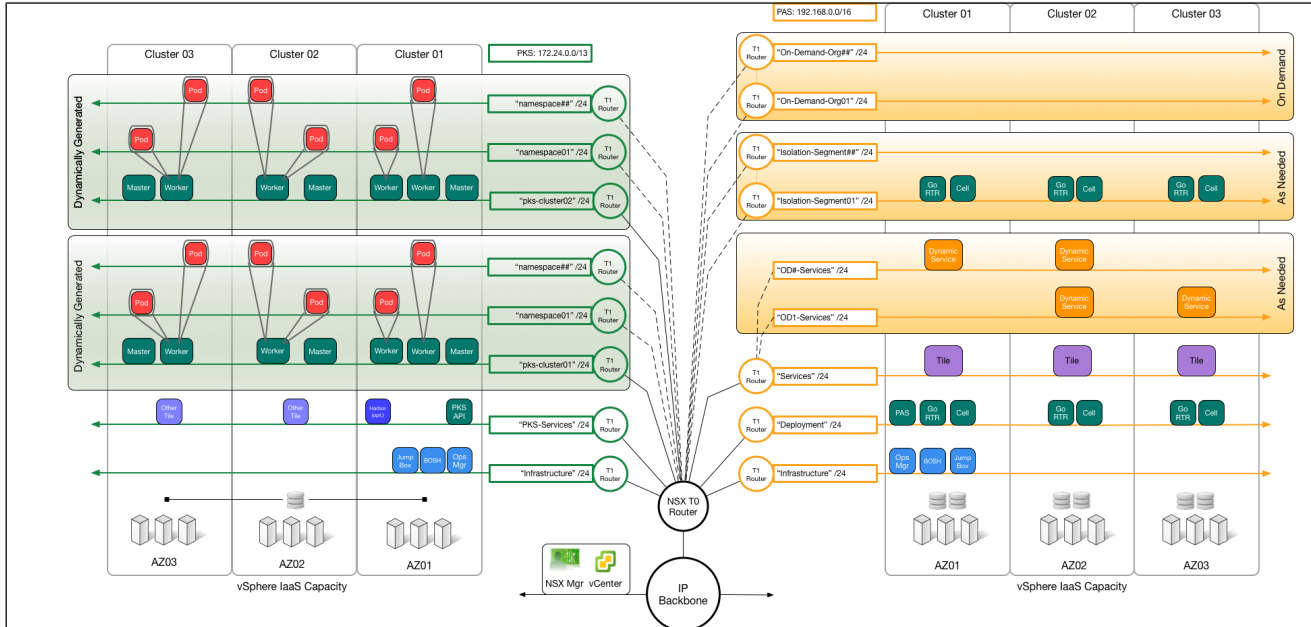
A production-ready PCF foundation looks as follows:

- 3 vSphere clusters/3 AZs
- 4 resource pools: 1 for NSX components and 3 for PAS/1 for PKS
- 3 hosts minimum for vSphere HA (4 hosts for vSphere VSAN)
- Shared Storage/VSAN
- 1 NSX Manager
- 3 NSX Controllers
- 3 large edge VMs in a cluster
- PCF: Ops Manager, the BOSH Director, and PAS/PKS

PAS and PKS with NSX-T

A fully meshed installation of PCF v2.2 or later designed using the recommendations provided in this topic looks as follows:

Note: You should not share an Ops Manager and BOSH Director installation between PKS and PAS in a production environment.



[View a larger version of this diagram](#)

Common components are the NSX T0 router and the associated T1 routers. This approach ensures that any cross-traffic between PKS and PAS apps stays within the bounds of the T0. This also provides a one-stop access point to the whole installation, which simplifies deployment automation for multiple, identical installations.

Note that each design, green PKS and orange PAS, has its own Ops Manager and BOSH Director installation. You should not share an Ops Manager and BOSH Director installation between PKS and PAS.

AZs are aligned to vSphere clusters, with resource pools as an optional organizational tool to place multiple foundations into the same capacity. You can align PKS to any AZ or cluster. Keeping PKS and PAS in completely separate AZs is not required.

You can use resource pools in vSphere clusters as AZ constructs to stack different installations of PCF. As server capacity continues to increase, the efficiency of deploying independent server clusters only for one installation is low. For example, customers are commonly deploying servers with 768-GB RAM and greater.

To allow for max capacity growth, consider using an NSX-T installation per foundation.

If you want to split the PAS and PKS installations into separate network trees, behind separate T0 routers, ensure that approach meets your needs by reviewing VMware's recommendations for T0 to T0 routing. For more information, see [Reference Design Guide for PAS and PKS with VMware NSX-T Data Center](#) in the VMware documentation.

Using Edge Services Gateway on VMware NSX

This cookbook provides guidance on how to configure the NSX firewall, load balancing, and NAT/SNAT services for Pivotal Cloud Foundry (PCF) on vSphere installations. These NSX-provided services take the place of an external device or the bundled HAProxy VM in PCF.

This document presents the reader with fundamental configuration options of an Edge Services Gateway (ESG) with PCF and vSphere NSX. Its purpose is not to dictate the settings required on every deployment, but instead to empower the NSX Administrator with the ability to establish a known good “base” configuration and apply specific security configurations as required.





If you are using NSX, the specific configurations described here supersede any general recommendations in the [Preparing Your Firewall](#) topic.

Assumptions

This document assumes that the reader has the level of skill required to install and configure the following products:

- VMware vSphere v5.5 or greater
- NSX v6.1.x or greater
- PCF v1.6 or greater

For detailed installation and configuration information about these products, see the following:

- [vSphere Documentation](#) 
- [NSX Installation and Upgrade Guide](#) 
- [Reference Design: VMware NSX for vSphere \(NSX\) Network Virtualization Design Guide](#) 
- [Pivotal Cloud Foundry Documentation](#) 

General Overview

This cookbook follows a three-step recipe to deploy PCF behind an ESG:

1. Configure Firewall
2. Configure Load Balancer
3. Configure NAT/SNAT

The ESG can scale to accommodate very large PCF deployments as needed.

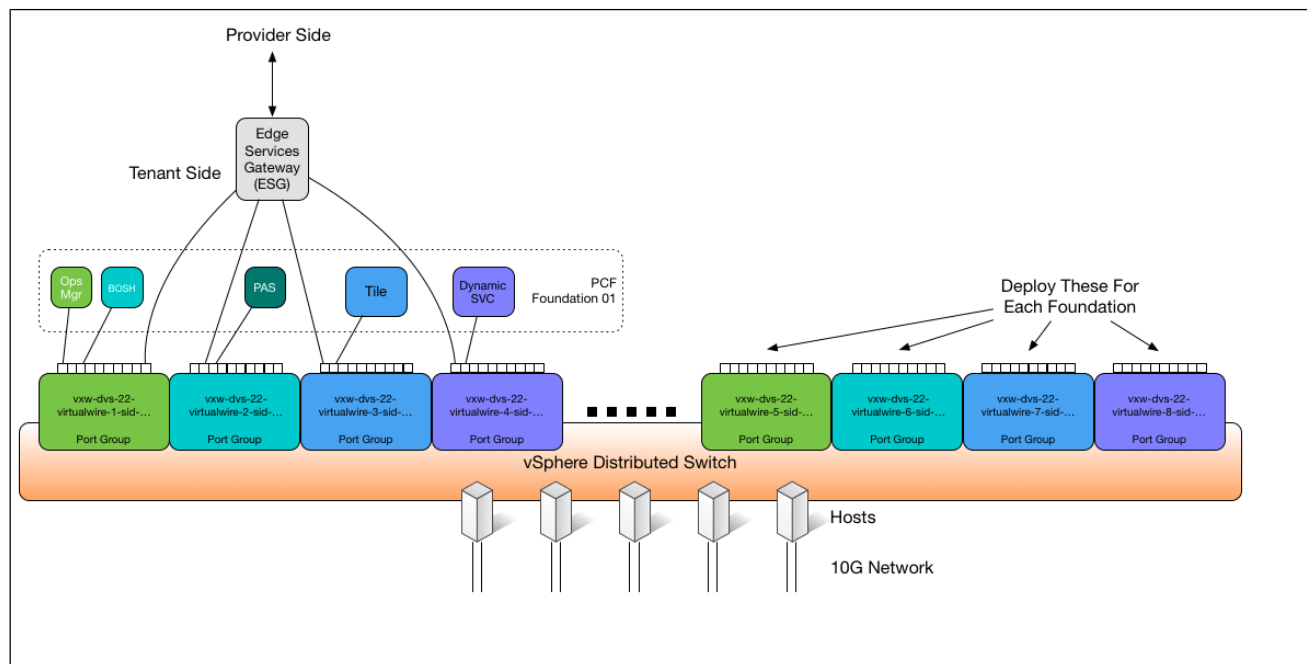
This cookbook focuses on a single-site deployment and makes the following design assumptions:

- There are five non-routable networks on the tenant (inside) side of the ESG.
 - The **Infra** network is used to deploy Ops Manager and BOSH Director.
 - The **Deployment** network is used exclusively by Pivotal Application Service (PAS) to deploy Cells that host apps and related elements.
 - The **CF Tiles** network is used for all other deployed tiles in a PCF installation.
 - The **Services** network is used by BOSH Director for service tiles.
 - The **Container-to-Container** network is used for container to container communication in the Cells.
- There is a single service provider (outside) interface on the ESG that provides Firewall, Load Balancing and NAT/SNAT services.
- The service provider (outside) interface is connected appropriately to the network backbone of the environment, as either routed or non-routed depending on the design. This cookbook does not cover provisioning of the uplink interface.
- Routable IP addresses should be applied to the service provider (outside) interface of the ESG. Pivotal recommends that you apply 10 consecutive routable IP addresses to each ESG.
 - One reserved for NSX use (Controller to Edge I/F)
 - One for NSX Load Balancer to Gorouters
 - One for NSX Load Balancer to Diego Brains for SSH to apps
 - One routable IP address, used to access the Ops Manager frontend
 - One routable IP address, used with SNAT egress
 - Five for future use

Pivotal recommends that operators deploy the ESGs as high availability (HA) pairs in vSphere. Also, Pivotal recommends that they be sized “large” or greater for any pre-production or production use. The deployed size of the ESG impacts its overall performance, including how many SSL tunnels it can terminate.

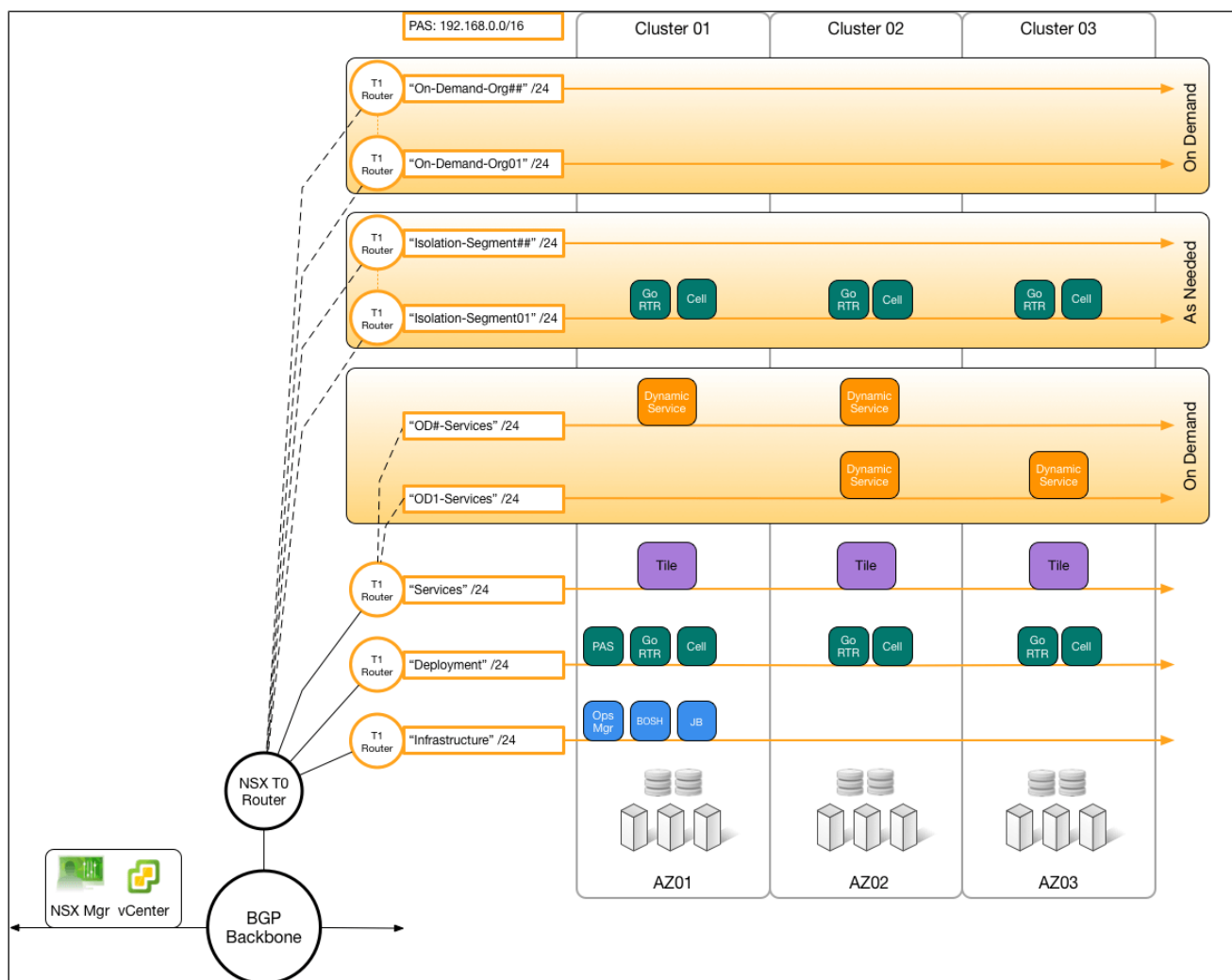
The ESGs have an interface in each port group used by PCF as well as a port group on the service provider (outside), often called the “transit network.” Each PCF installation has a set of port groups in a vSphere DVS to support connectivity, so that the ESG arrangement is repeated for every PCF install. It is not necessary to build a DVS for each ESG/PCF install. You do not re-use an ESG amongst PCF deployments. NSX Logical Switches (VXLAN vWires) are ideal candidates for use with this architecture.

The following diagram provides an example of port groups used with an ESG:



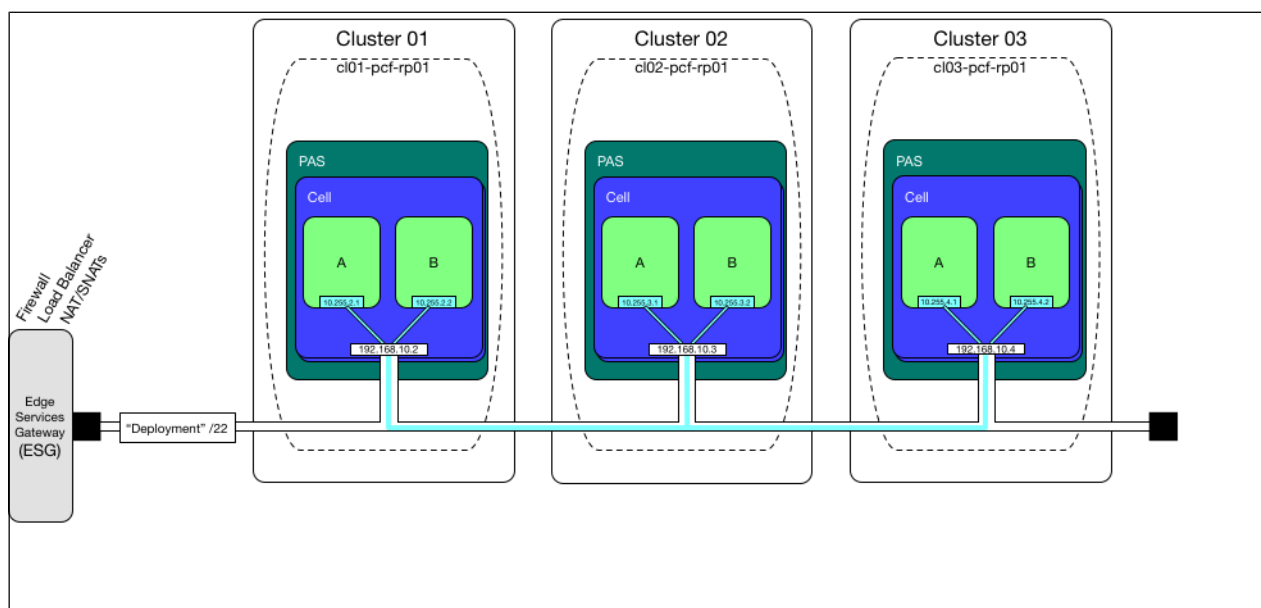
[View a larger version of this diagram.](#)

The following is an example of a network architecture deployment.



[View a larger version of this diagram.](#)

The following diagram illustrates container-to-container networking. The overlay addresses are wrapped and transported using the underlay deployment subnet.



[View a larger version of this diagram.](#)

Prep Step: Configure DNS and Network Prerequisites

As a prerequisite, create wildcard DNS entries for system and apps domains in PCF. Map these domains to the selected IP address on the uplink (outside) interface of the ESG in your DNS server.

The wildcard DNS [A](#) record must resolve to an IP address associated with the outside interface of the ESG for it to function as a load balancer. You can either use a single IP address to resolve both the system and apps domain, or one IP address for each.

In addition, assign the following IP addresses and address ranges within your network:

1. Assign IP Addresses to the “Uplink” (outside) interface
 - Typically you have one SNAT and three DNATs per ESG.
 - IP associated for SNAT use: All PCF internal IP addresses appear to be coming from this IP address at the ESG.
 - IP associated with Ops Manager DNAT: This IP address is the publicly routable interface for Ops Manager UI and SSH access.
2. Assign “Internal” Interface IP Address Space to the Edge Gateway.
 - 192.168.10.0/26 = PCF Deployment Network (Logical Switch or Port Group)
 - 192.168.20.0/22 = Deployment Network for PAS tile
 - 192.168.24.0/22 = CF Tiles Network for all Tiles besides PAS
 - 192.168.28.0/22 = Dynamic Services network for BOSH Director-managed service tiles.
 - 10.255.0.0/16 = Container-to-Container network for intercontainer communication.

You must update the security group and load balancer information for your PCF deployments using NSX-V on vSphere through the Ops Manager API. See [Updating NSX Security Group and Load Balancer Information](#) for more information.

Step 1: Configure Firewall

This procedure populates the ESG internal firewall with rules to protect a PCF installation.

These rules provide granular control on what can be accessed within a PCF installation. For example, rules can be used to allow or deny another PCF installation behind a different ESG access to apps published within the installation you are protecting.

This step is not required for the installation to function properly when the firewall feature is disabled or set to “Allow All.”

To configure the ESG firewall, navigate to **Edge, Manage, Firewall** and set the following:

| Name | Source | Destination | Service | Action |
|-------------------------------|---|---|---------------------|--------|
| Allow Ingress -> Ops Manager | any | IP_of_OpsMgr | SSH, HTTP, HTTPS | Accept |
| Allow Ingress -> PAS | any | IP_of_NSX-LB | HTTP, HTTPS | Accept |
| Allow Ingress -> SSH for Apps | any | tcp:IP_of_DiegoBrain:2222 | any | Accept |
| Allow Ingress -> TCProuter | any | tcp:IP_of_NSX-TCP-LB:5000 | any | Accept |
| Allow Inside <-> Inside | 192.168.10.0/26 192.168.20.0/22 192.168.24.0/22 192.168.28.0/22 | 192.168.10.0/26 192.168.20.0/22 192.168.24.0/22 192.168.28.0/22 | any | Accept |
| Allow Egress -> IaaS | 192.168.10.0/26 | IP_of_vCenter IPs_of_ESXi-Svrs | HTTP, HTTPS | Accept |
| Allow Egress -> DNS | 192.168.0.0/16 | IPs_of_DNS | DNS, DNS-UDP | Accept |
| Allow Egress -> NTP | 192.168.0.0/16 | IPs_of_NTP | NTP | Accept |
| Allow Egress -> SYSLOG | 192.168.0.0/16 | IPs_of_Syslog:514 | SYSLOG | Accept |
| Allow ICMP | 192.168.10.0/26 | * | ICMP | Accept |
| Allow Egress -> LDAP | 192.168.10.0/26 192.168.20.0/22 | IPs_of_LDAP:389 | LDAP, LDAP-over-ssl | Accept |
| Allow Egress -> All Outbound | 192.168.0.0/16 | any | any | Accept |
| Default Rule | any | any | any | Deny |

Step 2: Configure Load Balancer

The ESG provides software load balancing functionality, equivalent to the bundled HAProxy that is included with PCF, or hardware appliances such as an F5 or A10 load balancer.

This step is required for the installation to function properly.

There are seven high level steps to this procedure:

1. Import SSL certificates to the Edge for SSL termination.
2. Enable the load balancer.
3. Create Application Profiles in the Load Balancing tab of NSX.
4. Create Application Rules in the load balancer.
5. Create Service Monitors for each pool type.
6. Create Application Pools for the multiple groups needing load balancing.
7. Create a virtual server (also known as a VIP) to pool balanced IP addresses.

What you will need:


- PEM files of SSL certificates provided by the certificate supplier for only this installation of PCF, or the self-signed SSL certificates generated during PCF installation.

In this procedure you marry the ESG's IP address used for load balancing with a series of internal IP addresses provisioned for Gorouters in PCF. It is important to know the IP addresses used for the Gorouters beforehand.

These IP addresses can be pre-selected or reserved prior to deployment (recommended) or discovered after deployment by looking them up in BOSH Director, which lists them in the release information of the PAS installation.

Step 2.1: Import SSL Certificate

PCF requires SSL termination at the load balancer.

 **Note:** If you intend to pass SSL termination through the load balancer directly to the Gorouters, you can skip the step below and select **Enable SSL Passthru** on the **HTTPS Application Profile**.

To enable SSL termination at the load balancer in ESG, access the ESG UI and do the following:

1. Select **Edge, Manage, Settings**, and then **Certificates**.
2. Click Green Plus button to Add Certificate.
3. Insert PEM file contents from the Networking configuration screen of PAS.
4. Save the results.

Step 2.2: Enable the Load Balancer

To enable the load balancer, access the ESG UI and do the following:

1. Select **Edge, Manage, Load Balancer**, and then **Global Configuration**.
2. Edit load balancer global configuration.
3. Enable load balancer.
4. Enable acceleration.
5. Set logging to desired level (**Info** or greater).

Step 2.3: Create Application Profiles

The Application Profiles allow advanced **x-forwarded** options as well as linking to the SSL Certificate. You must create three Profiles: **PCF-HTTP**, **PCF-HTTPS** and **PCF-TCP**.

To create the application profiles, access the ESG UI and do the following:

1. Select **Edge, Manage, Load Balancer**, and then **Global Application Profiles**.
2. Create/Edit Profile and make the **PCF-HTTP** rule, turning on **Insert X-Forwarded-For HTTP header**.

Edit Profile

Name:

Type: ▼

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: ▼

Cookie Name:

Mode: ▼

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certifica...

☐ Configure Service Certificate

| | Common Name | Issuer | Validity |
|-----|-------------|----------|-----------------------|
| (+) | *.f..... | *.f..... | Mon Apr 13 2015 - Wed |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Cipher: ▼

Client Authentication: ▼

3. Create/Edit Profile and make the **PCF-HTTPS** rule, same as before, but add the service certificate inserted before. If encrypting TLS traffic to the Gorouters, turn on **Enable Pool Side SSL**. Otherwise, leave it unchecked.

4. Create/Edit Profile and make **PCF-TCP** rule, with the Type set to TCP.

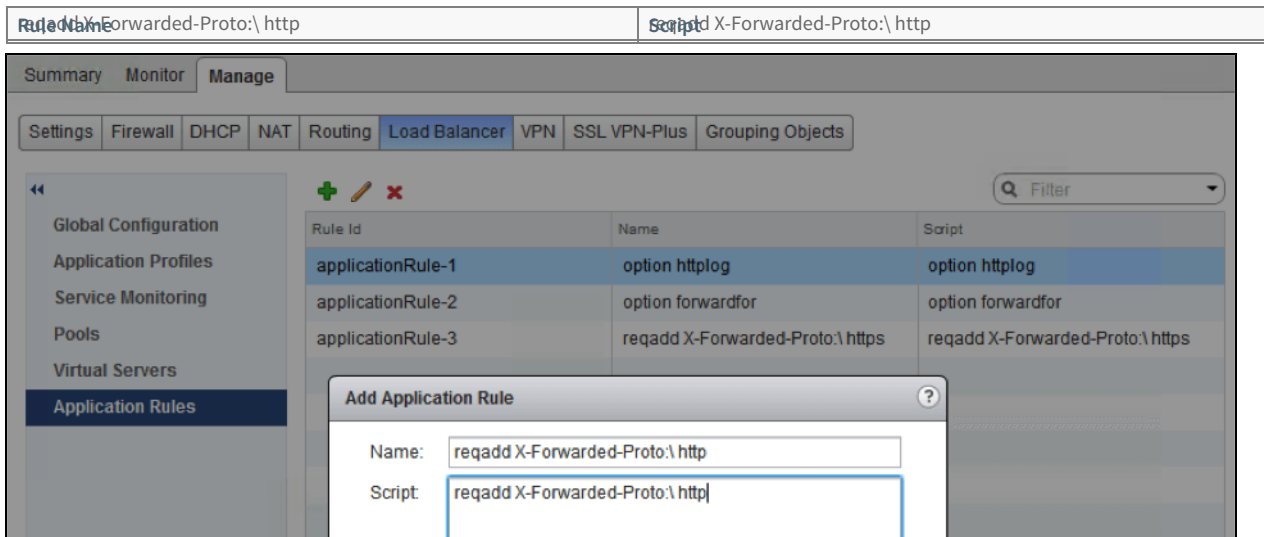
Step 2.4: Create Application Rules

In order for the ESG to perform proper `x-forwarded` requests, you need to add a few HAProxy directives to the ESG Application Rules. NSX supports most directives that HAProxy supports.

To create the application rules, access the ESG UI and do the following:

1. Select **Edge**, **Manage**, **Load Balancer**, and then **Application Rules**.
2. Copy and paste the table entries below into each field, one per rule.

| Rule Name | Script |
|----------------------------------|----------------------------------|
| option httplog | option httplog |
| reqadd X-Forwarded-Proto:\ https | reqadd X-Forwarded-Proto:\ https |



Step 2.5: Create Monitors For Pools

NSX ships with several load balancing monitoring types pre-defined. These types are for HTTP, HTTPS and TCP. For this installation, operators build new monitors matching the needs of each pool to ensure correct 1:1 monitoring for each pool type.

To create monitors for pools, access the ESG UI and do the following:

1. Select **Edge**, **Manage**, **Load Balancer**, and then **Service Monitoring**.
2. Create a new monitor for `http-routers`, and keep the defaults.
3. Set the Type to `HTTP`.
4. Set the Method to `GET`.
5. Set the URL to `/health`.
6. Create a new monitor for `tcp-routers`, and keep the defaults.
7. Set the type to `HTTP`.
8. Set the Method to `GET`.
9. Set the URL to `/health`.
10. Create a new monitor for `diego-brains`, and keep the defaults.
11. Set the type to `TCP`.

These monitors are selected during the next step when pools are created. A pool and a monitor are matched 1:1.

Step 2.6: Create Pools of Multi-Element PCF Targets

The following steps creates the pools of resources that ESG load-balances to: the Gorouter, TCP Router, and Diego Brain jobs deployed by BOSH Director. If the IP addresses specified in the configuration do not exactly match the IP addresses reserved or used for the resources, then the pool will not effectively load balance.

Step 2.6a: Create Pool for `http-routers`

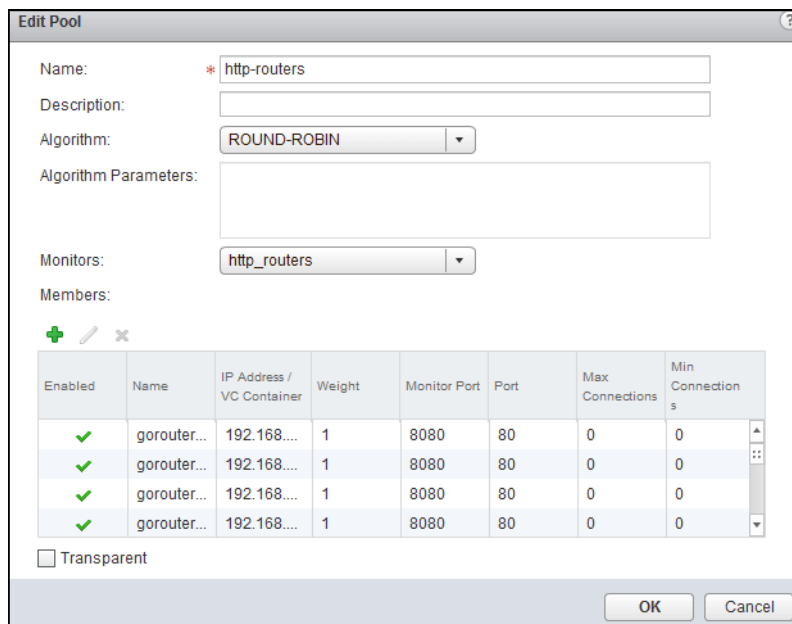
To create pool for `http-routers`, access the ESG UI and do the following:

1. Select **Edge**, **Manage**, **Load Balancer**, and then **Pools**.

2. Enter ALL the IP addresses reserved for the Gorouters into this pool. If you reserved more addresses than you have Gorouters, enter the addresses anyway and the load balancer ignores the missing resources as “down”.

 **Note:** If your deployment matches the [Reference Architecture for PCF on vSphere](#), these IP addresses are in the 192.168.20.0/22 address space.

3. Set the **Port** to 80 and **Monitor Port** to 8080. The assumption is that internal traffic from the ESG load balancer to the Gorouters is trusted because it is on a VXLAN secured within NSX. If using encrypted TLS traffic to the Gorouter inside the VXLAN, set the **Port** to 443.
4. Set the **Algorithm** to `ROUND-ROBIN`.



Edit Pool

Name: * http-routers

Description:

Algorithm: `ROUND-ROBIN`

Algorithm Parameters:

Monitors: http_routers

Members:

| Enabled | Name | IP Address / VC Container | Weight | Monitor Port | Port | Max Connections | Min Connections |
|---------|-------------|---------------------------|--------|--------------|------|-----------------|-----------------|
| ✓ | gorouter... | 192.168.20.1 | 1 | 8080 | 80 | 0 | 0 |
| ✓ | gorouter... | 192.168.20.2 | 1 | 8080 | 80 | 0 | 0 |
| ✓ | gorouter... | 192.168.20.3 | 1 | 8080 | 80 | 0 | 0 |
| ✓ | gorouter... | 192.168.20.4 | 1 | 8080 | 80 | 0 | 0 |

☐ Transparent

OK Cancel

5. Set **Monitors** to `http-routers`.

Step 2.6b: Create Pool for `tcp-routers`

1. Select **Edge**, **Manage**, **Load Balancer**, and then **Pools**.
2. Enter ALL the IP addresses reserved for TCP Routers into this pool. If you reserved more addresses than you have VMs, enter the addresses anyway and the load balancer ignores the missing resources as “down”.

 **Note:** If your deployment matches the [Reference Architecture for PCF on vSphere](#), these IP addresses are in the 192.168.20.0/22 address space.

3. Set the **Port** to empty (these numbers vary) and the **Monitor Port** to 80.
4. Set the **Algorithm** to `ROUND-ROBIN`.
5. Set the **Monitors** to `tcp-routers`.

Step 2.6c: Create Pool for `diego-brains`

1. Select **Edge**, **Manage**, **Load Balancer**, and then **Pools**.
2. Enter ALL the IP addresses reserved for Diego Brains into this pool. If you reserved more addresses than you have VMs, enter the addresses anyway and the load balancer will just ignore the missing resources as “down”.

 **Note:** If your deployment matches the [Reference Architecture for PCF on vSphere](#), these IP addresses are in the 192.168.20.0/22 address space.


3. Set the **Port** to 2222 and the **Monitor Port** to 2222.
4. Set the **Algorithm** to `ROUND-ROBIN`.

5. Set the Monitors to `diego-brains`.


Step 2.7: Create Virtual Servers

This is the Virtual IP (VIP) that the load balancer uses to represent the pool of Gorouters to the outside world. This also links the Application Policy, Application Rules, and backend pools to provide PCF load balancing services. This is the interface that the load balancer balances **from**. You create three Virtual Servers.

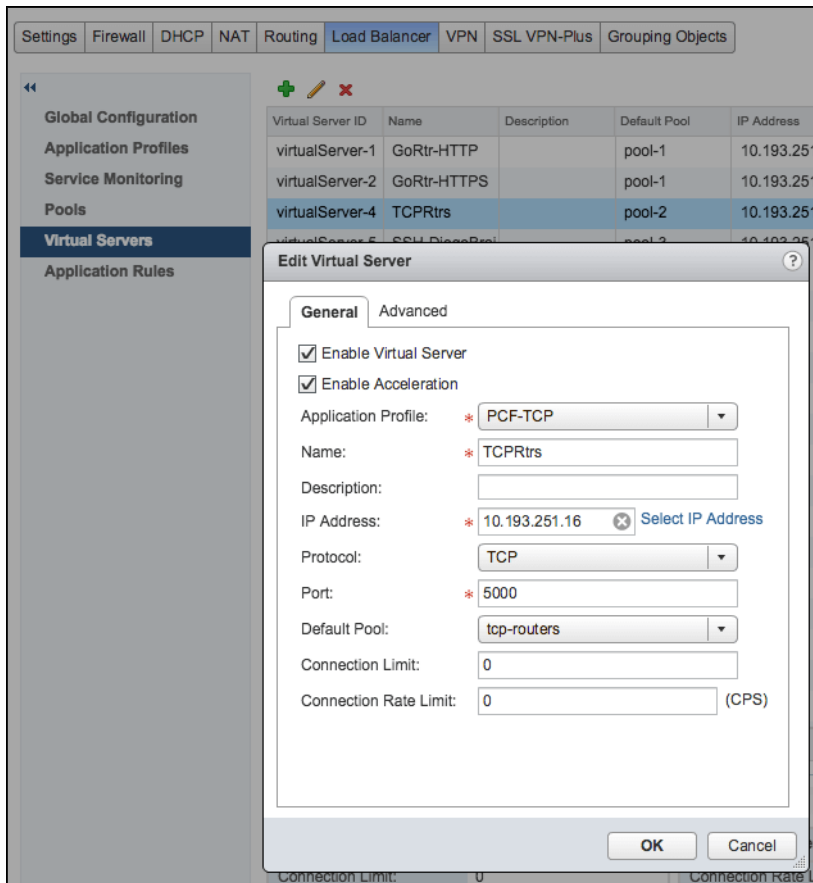
1. Select **Edge**, **Manage**, **Load Balancer**, and then **Virtual Servers**.
2. Select an IP address from the available routable address space allocated to the ESG. For information about reserved IP addresses, see [General Overview](#).
3. Create a new Virtual Server named `GoRtr-HTTP` and select Application Profile `PCF-HTTP`.
 - Use **Select IP Address** to select the IP address to use as a VIP on the uplink interface.
 - Set **Protocol** to match the **Application Profile** protocol (HTTP) and set **Port** to match the protocol (80).
 - Set **Default Pool** to the pool name set in [Step 2.6a: Create Pool for http-routers](#). This connects this VIP to the pool of resources being balanced to.
 - Ignore **Connection Limit** and **Connection Rate Limit** unless these limits are desired.
 - Switch to **Advanced Tab** on this Virtual Server.
 - Use the green plus to add/attach three Application Rules to this Virtual Server:
 - option httplog
 - reqadd X-Forwarded-Proto:\ http

 **Note:** Be careful to match protocol rules to the protocol `VIP-HTTP` to `HTTP` and `HTTPS` to `HTTPS`.

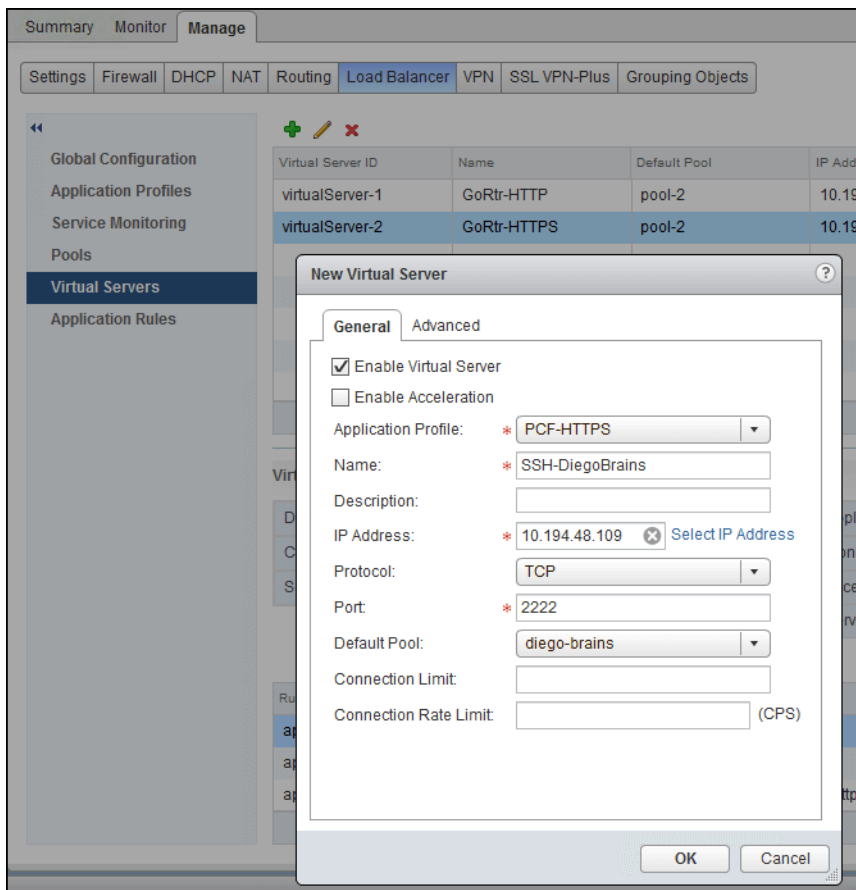
4. Create a new Virtual Server named `GoRtr-HTTPS` and select Application Profile `PCF-HTTPS`.
 - Use **Select IP Address** to select the **same IP address** to use as a VIP on the uplink interface.
 - Set **Protocol** to match the **Application Profile** protocol (`HTTPS`) and set **Port** to match the protocol (443).
 - Set **Default Pool** to the pool name set in [Step 2.6a: Create Pool for http-routers](#) (`http-routers`). This connects this VIP to that pool of resources being balanced to.
 - Ignore **Connection Limit** and **Connection Rate Limit** unless these limits are desired.
 - Switch to **Advanced Tab** on this Virtual Server.
 - Use the green plus to add/attach three Application Rules to this Virtual Server:
 - option httplog
 - reqadd X-Forwarded-Proto:\ https

 **Note:** Be careful to match protocol rules to the protocol `VIP-HTTP` to `HTTP` and `HTTPS` to `HTTPS`.

5. Create a new Virtual Server named `TCPRtr` and select Application Profile `PCF-TCP`.
 - Use **Select IP Address** to select the IP address to use as a VIP on the uplink interface.
 - Set **Protocol** to match the **Application Profile** protocol (TCP) and set **Port** to match the protocol (5000).
 - Set **Default Pool** to the pool name set in [Step 2.6b: Create Pool for tcp-routers](#) (`tcp-routers`). This connects this VIP to the pool of resources being balanced to.
 - Ignore **Connection Limit** and **Connection Rate Limit** unless these limits are desired.



6. Create a new Virtual Server named `SSH-DiegoBrains` and select Application Profile `PCF-HTTPS`.
 - Use **Select IP Address** to select the same IP address to use as a VIP on the uplink interface if you want to use this address for SSH access to apps. If not, select a different IP address to use as the VIP.
 - Set **Protocol** to TCP and set **Port** to 2222.
 - Set **Default Pool** to the pool name set in [Step 2.6c: Create Pool for diego-brains](#) (`diego-brains`). This connects this VIP to that pool of resources being balanced to.
 - Ignore **Connection Limit** and **Connection Rate Limit** unless these limits are desired.



Step 3: Configure NAT/SNAT

The ESG obfuscates the PCF installation through network translation. The PCF installation is placed entirely on non-routable RFC-1918 network address space, so you must translate routable IP addresses to non-routable IP addresses to make connections.

Note: Correct NAT/SNAT configuration is required for the PCF installation to function as expected.

| Action | Applied on Interface | Original IP | Original Port | Translated IP | Translated Port | Protocol | Description |
|--------|----------------------|-------------------|---------------|-------------------|-----------------|----------|------------------------------|
| SNAT | uplink | 192.168.0.0/16 | any | IP_of_PCF | any | any | All Nets Egress |
| DNAT | uplink | IP_of_OpsMgr | any | 192.168.10.OpsMgr | any | tcp | OpsMgr Mask for external use |
| SNAT | infra | 192.168.10.OpsMgr | any | IP_of_OpsMgr | any | tcp | OpsMgr Mask for internal use |
| DNAT | infra | IP_of_OpsMgr | any | 192.168.10.OpsMgr | any | tcp | OpsMgr Mask for internal use |

Note: The NAT/SNAT on the `infra` network in this table is an example of an optional **Hairpin NAT** rule to allow VMs within the **Infrastructure** network to access the Ops Manager API. This is because the Ops Manager hostname and the API HTTPS endpoint are registered to the Ops Manager external IP address. A pair of Hairpin NAT rules are necessary on **each** internal network interface that requires API access to Ops Manager. You should create these rules only if the network must access the Ops Manager API.

NAT/SNAT functionality is not required if routable IP address space is used on the Tenant Side of the ESG. At that point, the ESG simply performs routing between the address segments.

Note: NSX generates a number of DNAT rules based on load balancing configs. You can safely ignore these.

Additional Notes

The ESG also supports scenarios where Private RFC subnets and NAT are not utilized for **Deployment** or **Infrastructure** networks, and the guidance in

this document can be modified to meet those scenarios.

Additionally, the ESG supports up to 10 Interfaces allowing for more Uplink options if necessary.

The use of Private RFC-1918 subnets for PCF Deployment networks was chosen due to its popularity with customers. ESG devices are capable of leveraging ECMP, OSPF, BGP, and IS-IS to handle dynamic routing of customer and/or public L3 IP space. That design is out of scope for this document, but is supported by VMware NSX and Pivotal PCF.

Upgrading vSphere without PCF Downtime

This topic describes how to upgrade the vSphere components that host your Pivotal Cloud Foundry (PCF) installation without service disruption.

Minimum Requirements

At a bare minimum, vSphere contains the following components:

- vCenter Server
- one or more ESXi hosts

You cannot perform an in-place upgrade of vSphere without at least two ESXi hosts in your cluster.


If you do not meet this requirement (in other words, you have insufficient resources to evacuate an entire host), then you may experience PCF downtime during the upgrade.

To upgrade vSphere with only one ESXi host or without sufficient headroom capacity, you must reduce your PCF installation size. In other words, you can either reduce the number of Diego cells in your deployment or pause PCF VMs to make more capacity available. These actions can result in PCF downtime.

Recommended Starting Configuration

If you are running a PCF deployment as recommended by the base reference architecture for PCF on vSphere (recommended), then your vSphere installation should have the following components:

- One vCenter Server
- Three ESXi hosts per cluster
- Three or more clusters
- One (or HA pair) NSX Edge appliances

 **Note:** Pivotal recommends having at least three ESXi hosts in your cluster to maintain PCF high availability during your upgrade.

For more information, see the [Reference Architecture for Pivotal Cloud Foundry on vSphere](#).

Procedure to Upgrade vSphere

To upgrade the vSphere management layer underneath PCF, perform the following steps:

Step 1. Upgrade vCenter

For example, you might be upgrading vCenter 6.0 to vCenter 6.5.


For more information about how to upgrade vCenter, see [Overview of the vCenter Server Upgrade Process](#)  in VMware documentation.

Step 2. Upgrade ESXi Hosts

After a successful vCenter upgrade, upgrade your ESXi hosts one at a time.

Starting with the first ESXi host, perform the following steps:

1. Verify that your ESXi hosts have sufficient resources and headroom to evacuate the VM workload of a single ESXi host to the two remaining hosts.

 **Note:** If you have enabled vSphere HA on your ESXi host, then each ESXi host should have sufficient headroom capacity since HA reserves 66% of available memory.

2. Use vMotion to move all the PCF VMs on the host you want to upgrade to the other ESXi hosts. vMotion places the VMs on the other hosts based on available capacity. For more information, see [Migration with vMotion](#) in VMware documentation.
3. Upgrade the evacuated ESXi host. For example, you may be upgrading from ESXi v6.0 to ESX v6.5. For instructions, see [Upgrading ESXi Hosts](#) in VMware documentation.

After successfully upgrading the first ESXi host, repeat the above steps for each remaining host one at a time. vSphere automatically rebalances all PCF VMs back onto the upgraded hosts via DRS after all the hosts are done.

Step 3. Upgrade ESG on VMware NSX

If your PCF deployment lives on a network behind an Edge Services Gateway (ESG) as recommended by the reference architecture, then upgrade each ESG only after completing the upgrade of vCenter and your ESXi hosts.

When you upgrade an ESG on VMware NSX, you upgrade the NSX Manager software. This upgrade can cause some slight downtime, the amount of which depends on the number of ESGs you are using.

- If your deployment only has one ESG, you can expect a downtime of 5 minutes for network reconvergence.
- If your ESGs are deployed in HA, upgrade the first ESG. Then upgrade the second ESG. This upgrade results only in 15-20 seconds of downtime.

For more information, see the [NSX Upgrade Guide](#) in VMware documentation.

Migrating PCF to a New Datastore in vSphere

Page last updated:

This topic describes how to migrate your Pivotal Cloud Foundry (PCF) installation to a new vSphere datastore.

Prerequisites

Both the new and existing vSphere datastores must reside in the same datacenter.

To avoid service disruption, Pivotal recommends that you configure your overall PCF deployment for [high availability](#). In addition, check for configurations necessary to achieve high availability in each of your installed product tiles.

If your environment has any single points of failure, service may be disrupted as a result of the migration.

Before You Begin

This section describes the steps you should perform prior to the migration.

Step 1: Back Up Your Environment

Ensure that your PCF environment is fully backed up.

For more information about how to backup PCF, see [Backing up Pivotal Cloud Foundry](#).

Step 2: Document Current Environment Settings

Document your current environment settings before proceeding with the datastore migration. Record which VMs are running and in which datastore they reside. If you experience any issues during or after the migration, you must have this information to restore your environment.

To obtain this information, perform the following steps:

1. Run the `bosh instances` command.
 - If you use [BOSH CLI v2+](#), run the following command, replacing `MY-ENV` with the alias you assigned to your BOSH Director:

```
$ bosh -e MY-ENV instances --details > instances.txt
```

- If you use the original version of the BOSH CLI, run the following command:

```
$ bosh-old instances --details > instances.txt
```

2. Save the resulting file `instances.txt` to a safe location.
3. Note the datastore where each VM resides in vSphere.

Step 3: Check System Health

In Pivotal Application Service (PAS), check the **Status** tab and make sure there are no errors or reported issues.

Step 4: Check Installed Products Health

In each tile installed in your PCF deployment, check the **Status** tab and make sure there are no errors or reported issues.

Step 5: Check BOSH Director Status

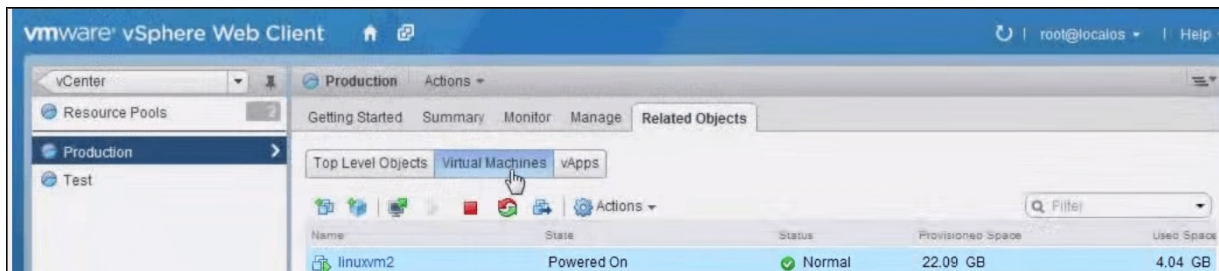
1. Check that there are no pending changes and that the status of all tiles is green.
2. Make sure the last Installation Log does not contain any errors.
3. Before proceeding with the migration, click **Apply Changes** to make sure there are no errors in the Installation Log.

Procedure: Migrate PCF to a New Datastore

1. In BOSH Director, navigate to the **vCenter Config** page.
2. Update the **Ephemeral Datastore Names** and **Persistent Datastore Names** field to reflect the new datastore names, then click **Save**.

Note: If you use the Datastore Clustering feature in vSphere, provide only the individual names of the datastores in the cluster. Do not provide the name of the cluster that contains them.

3. Click **Apply Changes**.
4. Confirm that the BOSH Director VM has persistent disk on the new datastore.
 - a. Navigate to **vCenter Resource Pools** and select the **Resource Pool** that contains your PCF deployment VMs and new datastore.
 - b. Click the **Related Objects** and **Virtual Machines**.
 - c. Locate the Ops Manager VM and verify that the VM has an expected value in the **Provisioned Space** column.



5. In BOSH Director, navigate to the **Director Config** page, and select the **Recreate all VMs** option.
6. Click **Apply Changes**.

After the Migration

When BOSH moves disks, it waits for up to 60 minutes for the operation to complete. If the operation does not complete in time, BOSH can enter a state where it claims that the disks are `out of sync`.

Fix Failed BOSH Deployment with Out-of-Sync Error

If your PCF deployment gets into this state, you can resolve the issue by performing the steps in the KB article [How to recover from a failed bosh deployment when VMs are out of sync on vSphere](#).

Prevent Out-of-Sync Error

You can also prevent the `out of sync` BOSH error by increasing the CPI timeout to a larger value before performing the migration. Follow the instructions in the KB article [How to Increase the Timeout on Bosh CPI Command Calls](#).

Control Plane Reference Architectures

Introduction

Concourse is the main continuous integration and continuous delivery (CI/CD) tool that the Pivotal and open-source Cloud Foundry communities use to develop, test, deploy and manage Cloud Foundry foundations.

This topic describes topologies and best practices for deploying Concourse on [BOSH](#), and using Concourse to manage Pivotal Cloud Foundry (PCF) foundations. For production environments, Pivotal recommends deploying Concourse with BOSH.

The three topologies described in this document govern the network placement and relationship between two systems:

- The **control plane** runs Concourse to gather sources for, integrate, update, and otherwise manage PCF foundations. This layer may also host internal Docker registries, S3 buckets, git repositories, and other tools.
- Each **PCF foundation** runs PCF on an instance of BOSH.

Each topology described below has been developed and validated in multiple PCF customer and Pivotal Labs environments.

Deployment Topologies

Security policies are usually the main factor that determines which CI/CD deployment topology best suits a site's needs. Specifically, the decision depends on what network connections are allowed between the control plane and the PCF foundations that it manages.

The following three topologies answer a range of security needs, ordered by increasing level of security around the PCF foundations:

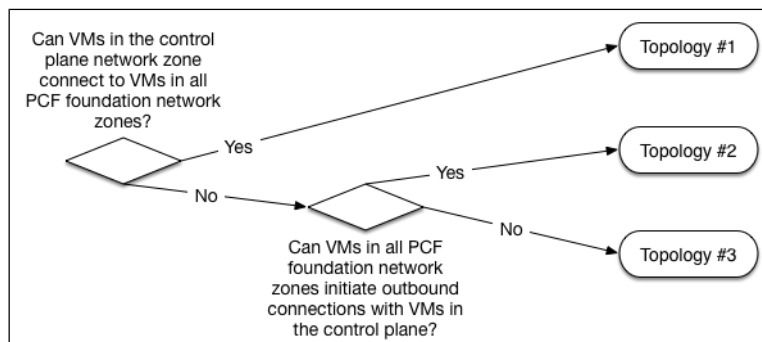
- [Topology 1](#): Concourse server and worker VMs all colocated on control plane
- [Topology 2](#): Concourse server on control plane, and remote workers colocated with PCF foundations
- [Topology 3](#): Multiple Concourse servers and workers colocated with PCF foundations

Across these three topologies, the increasing level of PCF foundation security correlates with:

- Increasing network complexity
- Increasing effort required for initial deployment and ongoing maintenance

Security Decision Factors

The graph below captures the decision factors dictated by network security policy, and recommends Concourse deployment topologies that adhere to those policies.



Additional Decision Factors

In addition to security policy, deciding on a CI/CD deployment topology may also depend on factors such as:

- Network latency across network zones

- Air-gapped vs. Internet-connected environments
- Resource limitations

The [Credentials Management](#) and [Storage Services](#) sections below includes notes and recommendations regarding credentials management, Docker registries, S3 buckets, and git repositories, but does not cover these tools extensively.

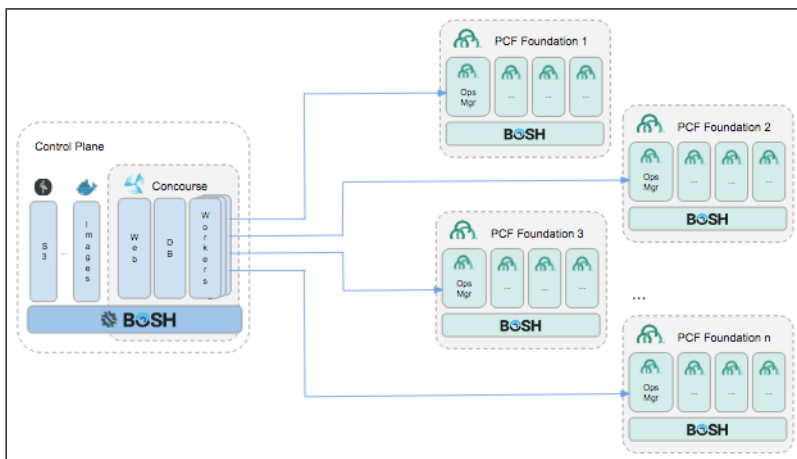
Topology Objects

Complete deployment topologies dictate the internal placement or remote use of the following:

- Concourse server and worker VMs, as discussed [above](#)
- Credentials managers such as CredHub or Vault
- Docker registries, public or private
- S3 or other storage buckets, public or private
- git or other code repositories, public or private

Topology 1: Concourse Server and Worker VMs All Colocated on Control Plane

This simple topology follows network security policies that allow a single control plane to connect to all PCF foundations deployed across multiple network zones or data centers.



In this topology, the Concourse server and worker VMs, along with other tools (e.g. Docker registry, S3 buckets, Vault server), are all deployed to the same subnet.

Connectivity Requirements

Concourse worker VMs must be allowed to connect to:

- The Ops Manager VM or a jumpbox VM in all of the PCF foundations networks
- (on vSphere) The vCenter API for each PCF foundation

Performance Notes

Network data transfers between the control plane and each PCF foundation network zone may carry large files such as PCF tiles, release files, and PCF foundation backup pipelines output.

Pivotal recommends that you test network throughput and latency between those network zones to make sure that data transfer rates do not make pipeline execution times unacceptably long.

Firewall Requirements

All Concourse worker VMs are required to connect to certain VMs on PCF foundation subnets across networks zones or data centers.

See [PCF CI/CD Pipelines](#) section for required VMs, ports, and external websites required for PCF CI/CD pipelines.

Pros

- Simplified deployment and maintenance of centralized control plane, which requires only one BOSH deployment and runs one BOSH Director.
- Simplified setup and maintenance of PCF CI/CD pipelines. All pipelines and Concourse teams use a single, centralized server.

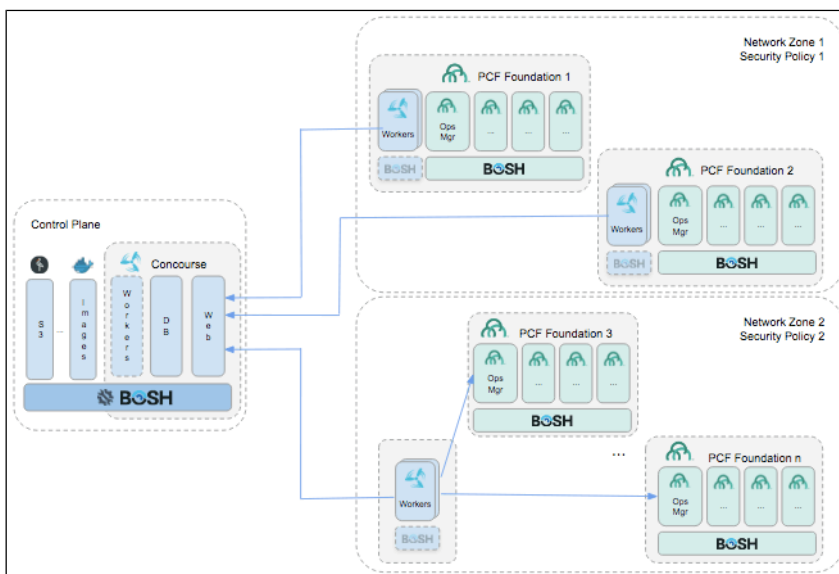
Cons

- You may have to configure firewall rules in each PCF network to allow connectivity from workers in CI/CD zone, as mentioned above.

Topology 2: Concourse Server on Control Plane, and Remote Workers Colocated with PCF Foundations

This topology supports environments where PCF foundation VMs cannot receive incoming traffic from IP addresses outside their network zone or data center, but they can initiate outbound connections to outside zones.

As in [Topology 1](#), the Concourse server, and potentially other VMs for tools such as Docker registries or S3 buckets, are deployed to a dedicated subnet. The difference here is that Concourse worker VM pools are deployed inside each PCF foundation subnet, network zone, or data center.



Connectivity Requirements

Concourse worker VMs in each PCF foundation network zone or data center must:

- Connect to the Ops Manager VM or a jumpbox VM in each PCF foundations network
- (on vSphere) Connect to the vCenter API for each PCF foundation
- Have outbound connection access to the Concourse web/ATC server on port 2222. This lets them handshake with the Concourse server to open a reverse SSH tunnel for ongoing communication between them and the Concourse ATC.

For more details, see [Concourse Architecture](#).

Performance Notes

Remote workers have to download large installation files from either the Internet or from a configured S3 artifacts repository. For PCF backup pipelines, workers may also have to upload large backup files to the S3 repository.

Pivotal recommends that you test network throughput and latency between those network zones to make sure that data transfer rates do not make pipeline execution times unacceptably long.

Firewall Requirements

Remote worker VMs require outbound access to the Concourse web/ATC server on port 2222.

Remote worker VMs inside each PCF foundation network zone or data center are required to connect to VMs in their colocated foundation. They may also require access to external web sites or S3 repositories for downloading installation files.

See the [PCF CI/CD Pipelines](#) section for required VMs and ports required for PCF CI/CD pipelines.

Pros

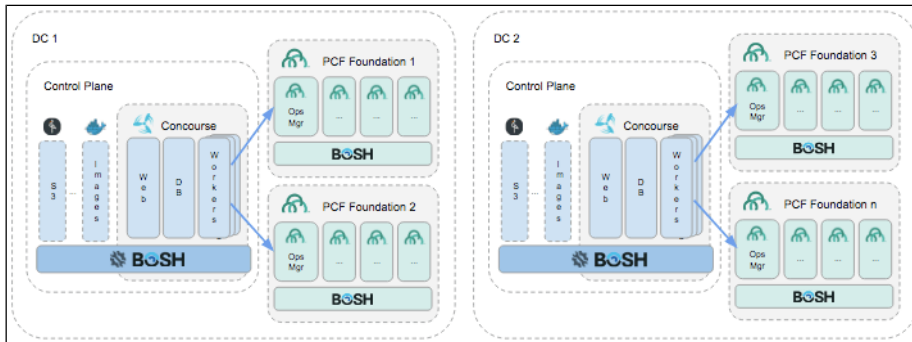
- Relatively simple maintenance of centralized control plane, which contains single Concourse server and other tools.
- Simplified setup and maintenance of PCF CI/CD pipelines. All pipelines and Concourse teams use a single, centralized server.

Cons

- You have to reconfigure firewalls to grant outbound access to remote worker VMs.
- In addition to deploying the control plane, you need an additional BOSH deployment and running BOSH Director for each PCF Foundation network zone or data center.
- You need to manage multiple Concourse worker pools in multiple locations.

Topology 3: Multiple Concourse Servers and Workers Colocated with PCF Foundations

This topology supports environments where PCF foundation VMs can only be accessed from within the same network zone or data center. This scenario requires deploying complete and dedicated control planes within each deployment zone.



Performance Notes

Since workers run in the same network zone or data center as the PCF foundation, data transfer throughput should not limit pipeline performance.

Firewall Requirements

- **Air-gapped environments** require some way to bootstrap S3 repository with Docker images and PCF releases files for pipelines from external sites.
- **Non-air-gapped environments**, in which workers can download required files from external websites, need those websites to be whitelisted in the proxy or firewall setup.

Pros

- Requires little or no firewall rules configuration for control plane VMs. In non-air-gapped environments, worker VMs download PCF releases and Docker images for pipelines from external websites.

Cons

- Requires deploying and maintaining multiple Concourse and other tools.
- Requires deploying and maintaining multiple PCF pipelines for each Concourse server.
- For air-gapped environments, requires setting up an S3 repository for each control plane.

Deploying CI/CD to the Control Plane

There are a few alternatives to deploy BOSH Directors, Concourse servers, and other tool releases to the control plane. Details on those alternatives are outside of the scope of this document, but refer to the links below for the most common options:

Manual deployments

- BOSH Director: [BOSH create-env](#)
- Concourse
 - [Concourse](#)
 - [Concourse with CredHub](#)
 - [Concourse with Vault](#)

- Docker registries
 - [Private Docker Registry](#)
 - [VMware Harbor Registry](#)
- S3 buckets
 - [Minio S3](#)
 - [EMC Cloud Storage](#)

Automated deployments

- [Bosh Bootloader \(BBL\)](#) deploys BOSH Director and Concourse on multiple IaaS.

Control Plane Deployment Best Practices

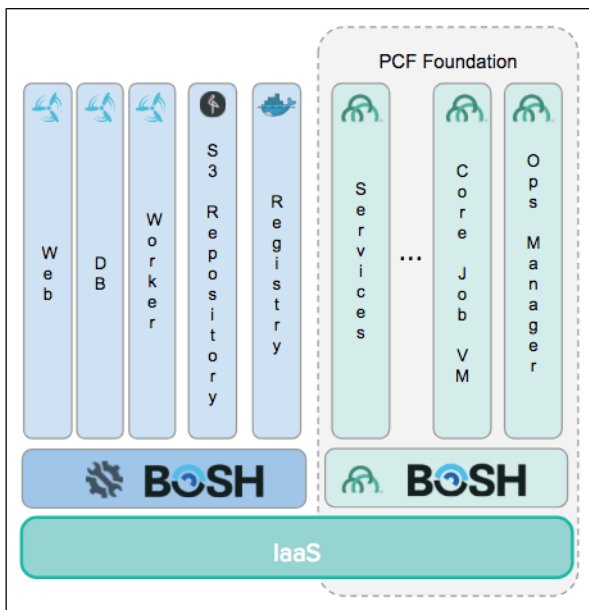
Here are some best practices for control plane components that apply across all deployment topologies:

Dedicated BOSH Director

Pivotal recommends deploying Concourse and other control plane tools on their own, dedicated BOSH layer, with their own BOSH Director that runs separately from the PCF foundations that the control plane manages.

Pivotal does **not** recommend using an existing PCF BOSH Director instance to deploy Concourse and other software (e.g. Minio S3, private Docker registry, CredHub). Sharing the same BOSH Director with PCF deployments increases the risk of accidental or undesired updates or deletion of those deployments.

Dedicating a BOSH Director to Concourse and other control plane tools also provides higher flexibility for PCF foundation upgrades and updates, such as stemcell patches.



Credentials Management

All credentials and other sensitive information that feeds into a Concourse pipeline should be encrypted and stored using credentials management software such as CredHub or Vault. Never store credentials as plain text in parameter files in file repositories.

Credentials Management with CredHub

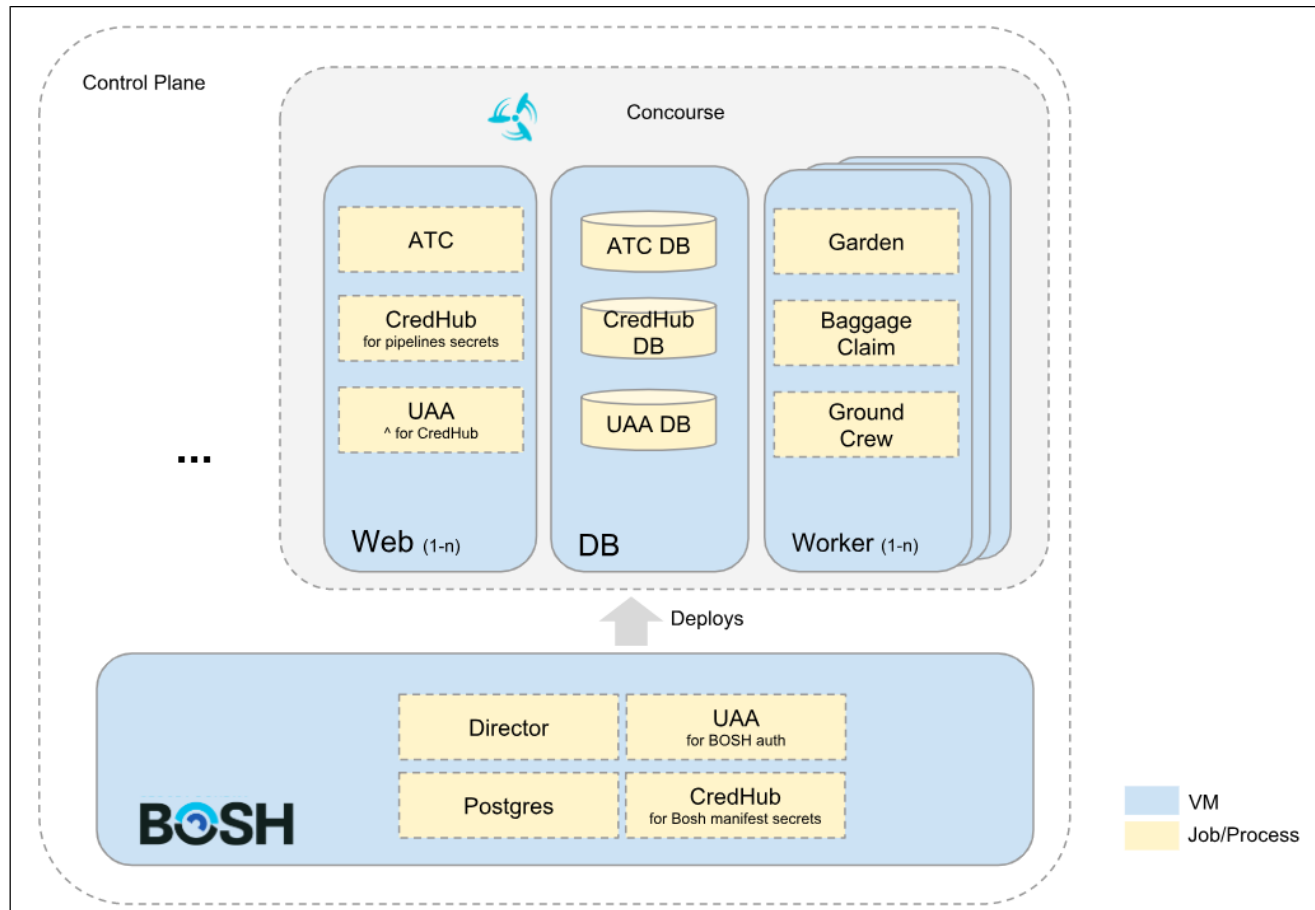
Concourse integrates with CredHub to manage credentials in its pipelines. The pipelines reference encrypted secrets stored in a CredHub server and retrieve them automatically during execution of tasks.

To integrate Concourse with a CredHub server, you configure its ATC job's deployment properties with information about the CredHub server and corresponding UAA authentication credentials.

You can deploy CredHub in multiple ways: as a dedicated VM, or integrated with other VMs, such as colocating the CredHub server with the BOSH Director VM or Concourse's ATC/web VM.

Colocating a CredHub server with Concourse's ATC VM dedicates it to the Concourse pipelines and lets Concourse administrators manage the credentials server. This configuration also means that during Concourse upgrades, the CredHub server only goes down when the Concourse ATC job is also down, which minimizes potential credential server outages for running pipelines.

The diagram below illustrates the jobs of Concourse VMs, along with the ones for the BOSH Director VM, when a dedicated CredHub server is deployed with Concourse.



The [Concourse Pipelines Integration with CredHub](#) documentation in the PCF Pipelines repository describes how to deploy a CredHub server integrated with Concourse.

Credentials Management with Vault

For how to configure Vault to manage credentials for Concourse pipelines, see [Secure credential automation with Vault and Concourse](#) in the PCF Pipelines repository.

Storage Services

Git Server

BOSH and Concourse implement the concepts of infrastructure-as-code and pipelines-as-code. As such, it is important to store all source code for deployments and pipelines in a version-controlled repository.

PCF CI/CD pipelines assume that their source code is kept in git-compatible repositories. [GitHub](#) is the most popular git-compatible repository for Internet-connected environments.

GitLab, BitBucket and [GOGS](#) are examples of git servers that can be used for both connected and air-gapped environments.

A git server that contains configuration and pipeline code for a PCF foundation needs to be accessible by the corresponding worker VMs that run CI/CD pipelines for that foundation.

S3 Repository

In all environments Concourse requires an S3 repository to store PCF backups and possibly other files. If your deployment requires a private, internal S3 repository but your IaaS lacks built-in options, you can use BOSH to deploy your own S3 releases, such as [Minio S3](#) and [EMC Cloud Storage](#) to your control plane.

For air-gapped environments, an S3 repository is also the preferred method to store release files for PCF tiles, stemcells and buildpacks. Docker images can also be stored to an S3 repository as an alternative to a private Docker registry. See [Offline Pipelines for Airgapped Environments](#) for details.

Private Docker Registry

For air-gapped environments, Docker Images for Concourse pipelines need to be stored either on a private Docker registry or in an S3 repository. For BOSH-deployed private registry alternatives, check [Docker Registry](#) or [VMWare Harbor](#).


High Availability

For details on how to set up a load balancer to handle traffic across multiple instances of the ATC/web VM, and how to deploy multiple worker instances, see the [Concourse Architecture](#) topic.

PCF CI/CD Pipelines

PCF Pipelines

PCF Platform Automation with Concourse (PCF Pipelines) is a collection of Concourse pipelines for installing and upgrading Pivotal Cloud Foundry. See the [source on Github](#) or download from [Pivotal Network](#) (sign-in required).

 **warning:** At time of publication, the PCF Pipelines repository is undergoing planned deprecation.


To run PCF Pipelines, you need:

- Ops Manager web UI, API and VM installed
- (vSphere environments) vCenter API installed
- For proxy- or Internet-connected environments, whitelist the following sites:
 - [Docker Hub](#): hub.docker.io
 - [Pivotal Network](#): network.pivotal.io
 - bosh.io

BOSH Backup and Restore (BBR) PCF Pipelines

BBR PCF Pipelines automate PCF foundation backups. See and download the [source on Github](#).


To run BBR PCF Pipelines, you need an S3 repository for storing backup artifacts.

 **Note:** BBR PCF Pipelines is a PCF community project not officially supported by Pivotal.

Pipelines Orchestration Frameworks

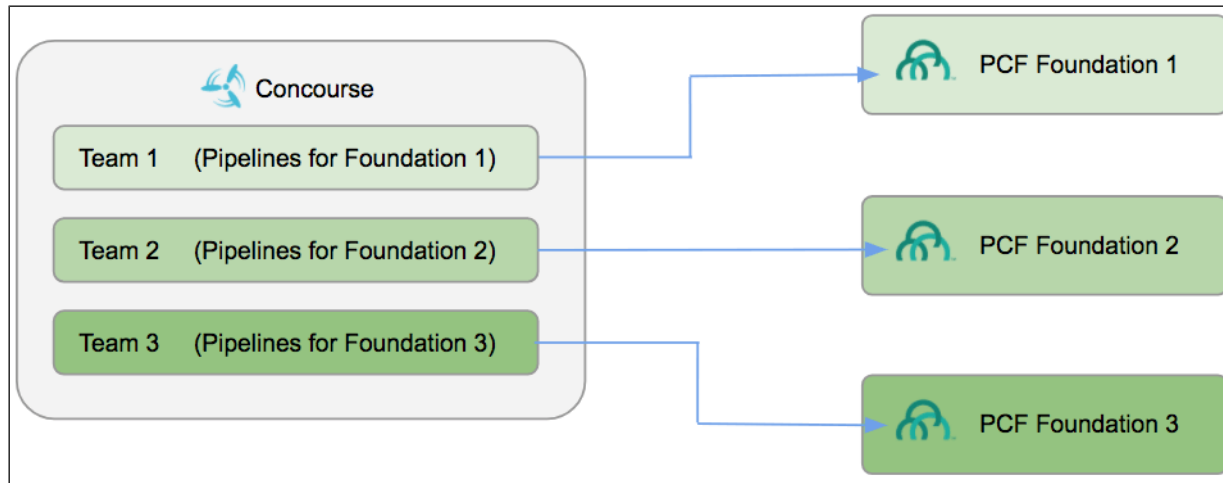
[PCF Pipelines Maestro](#) uses a Maestro framework to:

- Automate pipeline creation and management for multiple PCF foundations
- Promote and audit configuration changes and version upgrades across all foundations

 **Note:** PCF Pipelines Maestro is a PCF community project not officially supported by Pivotal.

Concourse Team Management Best Practices

When a single Concourse server hosts CI/CD pipelines for more than one PCF foundation, Pivotal recommends creating one Concourse team (not `main`) specific to each foundation, and associating that team with all pipelines for that foundation, e.g. install, upgrade, backup, and metering.



Dedicating a Concourse team to each PCF foundation has the following benefits:

- **It avoids the clutter of pipelines in a single team.** The list of pipelines for each foundation may be long, depending how many tiles are deployed to it.
- **It avoids the risk of operators running a pipeline for the wrong foundation.** When a single team hosts maintenance pipelines for multiple foundations, the clutter of dozens of pipelines may lead operators to accidentally run a pipeline (e.g. upgrade or delete tile) targeted at the wrong PCF foundation.
- **It allows for more granular access control settings per team.** PCF pipelines for higher environments (e.g. Production) may require a more restricted access control than ones from lower environments (e.g. Sandbox). Authentication settings for Concourse teams enable that level of control.
- **It allows workers to be assigned to pipelines of a specific foundation.** Concourse deployment configuration allows for the assignment of workers to a single team. If that team contains pipelines of only one foundation, then the corresponding group of workers run pipelines only for that foundation. This is useful when security policy requires tooling and automation for a foundation (e.g. Production) to run on specific VMs.

Concourse Teams for App Development Orgs and Spaces

When a Concourse server hosts pipelines for an app development team, Pivotal recommends creating a Concourse team associated with that development team, and associating Concourse team membership with org and space membership defined in the Pivotal Application Service (PAS) user authentication and authorization (UAA) server.

Associating Concourse teams with PAS org and space member lists synchronizes access between PAS and Concourse, letting developers see and operate the build pipelines for the apps they develop.

Implementing a Multi-Foundation PKS Deployment

Page last updated:

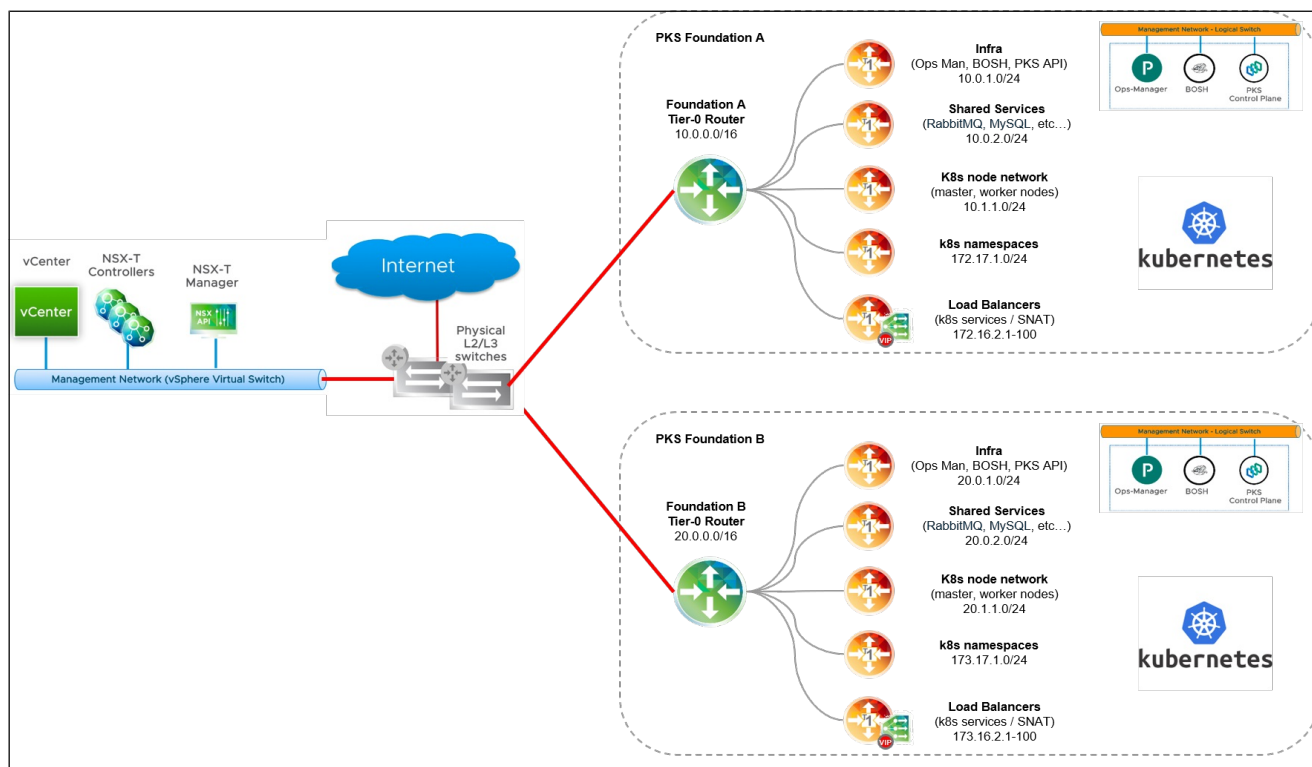
This topic describes how to deploy multiple instances of PKS on vSphere with NSX-T infrastructure.

About Multi-Foundation PKS

A multi-foundation deployment of PKS lets you install and run multiple instances of PKS. The purpose of a multi-foundation deployment of PKS is to share a common vSphere and NSX-T infrastructure across multiple foundations, while providing complete networking isolation across foundations.

As shown in the diagram, with a multi-foundation PKS topology, each PKS instance is deployed to a dedicated NSX-T Tier-0 router. Foundation A T0 router with Management CIDR 10.0.0.0/16 connects to the vSphere and NSX-T infrastructure. Similarly, Foundation B T0 router with Management CIDR 20.0.0.0/16 connects to the same vSphere and NSX-T components.

As with a single instance deployment, PKS management components are deployed to a dedicated network, for example, 10.0.0.0/24 for PKS Foundation A; 20.0.0.0/24 for PKS Foundation B. When PKS is deployed, networks are defined for nodes, pods, and load balancers. Because of the dedicated Tier-0 router, there is complete networking isolation between each PKS instance.



Requirements

To implement a multi-foundation PKS topology, adhere to the following requirements:

- One Tier-0 router for each PKS instance. For more information, see [Configuring Multiple Tier-0 Routers for Tenant Isolation](#).
- The Floating IP pool must not overlap. The CIDR range for each Floating IP Pool must be unique and not overlapping across foundations. For more information, see [Create Floating IP Pool](#).
- PKS instances can be deployed in NAT and no-NAT mode. If more than one PKS instance is deployed in no-NAT mode, the Nodes IP Block networks cannot overlap.
- For any Pods IP Block used to deploy Kubernetes clusters in no-NAT (routable) mode, the Pods IP Block cannot overlap across foundations.

The image below shows three PKS installations across three Tier-0 foundations. Key considerations to keep in mind with a multi-foundation PKS topology include the following:

- Each foundation must rely on a dedicated Tier-0 router



- You can mix-and-match NAT and no-NAT mode across foundations for Node and Pod networks
- If you are using non-routable Pods IP Block networks, the Pods IP Block addresses can overlap across foundations
- Because Kubernetes nodes are behind a dedicated Tier-0 router, if clusters are deployed in NAT mode the Nodes IP Block addresses can also overlap across foundations
- For each foundation you must define a unique Floating ID Pool with non-overlapping IPs

| PKS Foundation A | | PKS Foundation B | PKS Foundation C |
|--|----------------------------|--------------------------------------|---------------------------------------|
| <input checked="" type="checkbox"/> NAT mode | Can mix modes | <input type="checkbox"/> NAT mode | <input type="checkbox"/> NAT mode |
| Pods IP Block ID * | Must be unique if routable | Pods IP Block ID * | Pods IP Block ID * |
| 927a2eff-fa86-4df8-bb21-c45b5314f547 | | 927a2eff-fa86-4df8-bb21-c45b5314f547 | 1b81b967-a269-4a62-9ff5-e2a39a5feaae |
| Nodes IP Block ID * | Can overlap | Nodes IP Block ID * | Nodes IP Block ID * |
| 3d577e5c-acaf-4921-9458-a12b0e1318e6 | | 3d577e5c-acaf-4921-9458-a12b0e1318e6 | 3d577e5c-acaf-4921-9458-a12b0e1318e6 |
| T0 Router ID * | Must be unique | T0 Router ID * | T0 Router ID * |
| 40445803-8c3c-417e-bb24-a84cf9d330b5 | | 5c579e37-5318-4255-9658-1a2e99e1d1e9 | 791f220b-155b-4fe9-bf3b-58199e4ea911d |
| Floating IP Pool ID * | Must be unique | Floating IP Pool ID * | Floating IP Pool ID * |
| 86213c33-9b7a-4a91-b470-7145941bccc3 | | 31e0fd4e-19e7-4122-b300-438d465e486f | 8b3c7a55-16c9-4baf-a404-e9b0bf8e07ce |
| Nodes DNS * | Should be the same | Nodes DNS * | Nodes DNS * |
| 10.40.53.1 | | 10.40.53.1 | 10.40.53.1 |
| vSphere Cluster Names * | Should be unique | vSphere Cluster Names * | vSphere Cluster Names * |
| Cluster-A | | Cluster-B | Cluster-C |

Please send any feedback you have to pbs-feedback@pivotal.io.

Global DNS Load Balancers for Multi-Foundation Environments

This topic describes global DNS load balancers (GLBs) for multi-foundation environments. This topic also describes concepts such as foundation affinity and healthchecks.

 **Note:** If you want to configure a load balancer dedicated to one PCF foundation and you are using an F5 LTM, see [Configuring an F5 Load Balancer for PAS](#) .

About Multi-Foundation Environments

Multi-foundation environments are multiple instances of BOSH and Ops Manager that can communicate with each other. Each foundation can use different infrastructures to fit your preferences.


Multi-foundation environments are commonly deployed in an active-active or active-passive pattern. See below for descriptions of each term:

| Term | Description |
|------------------------|--|
| Active-active pattern | Instances of apps run on two foundations and they are both in use. |
| Active-passive pattern | Instances of apps run on two foundations, but the instances may only be active on one foundation. The other foundation becomes active only in the event of a failover. |

Configure Your GLB

The typical setup for foundation failover requires the GLB be authoritative for a wildcard app domain. The wildcard app domain is not the same domain as the foundation-default app domain.

To configure your GLB, do the following:

- Find and record your wildcard app domain. For Pivotal Application Service (PAS), your wildcard app domain is typically the **Apps Domain** you configure in the **Domains** pane of the PAS tile.
- Add the domain you recorded to both PCF foundations using a shared domain. You can create a shared domain using the Cloud Foundry Command Line Interface (cf CLI). For more information about the cf CLI command to create shared domains, see [create-shared-domain](#)  in the cf CLI reference guide.
- To support failover, set the time-to-live (TTL) in the wildcard DNS record. Set the TTL to about 30 to 180 seconds. When determining your TTL, consider the tradeoff between the app performance impact and the resulting time for failover to occur.

About Foundation Affinity

Foundation affinity occurs when the GLB favors one foundation over another during a route request. For example, users experience less latency if they are routed to a foundation that is geographically closer, so the GLB may favor that foundation.

Different GLBs have their own mechanisms to achieve this. See the following table for common concepts:

| Foundation Affinity Concepts | |
|--|--|
| Term | Description |
| Topology/geographically-based affinity | The GLB attempts to direct traffic to the graphically nearest foundation based on IP geolocation or provided topology for private networks of the LDNS server performing the lookup. |
| Static-persist/member-hashing affinity | The GLB attempts to direct traffic to the graphically nearest foundation based on IP geolocation or provided topology for private networks of the LDNS server performing the lookup. |
| Active/passive foundations | If one foundation is usually idle, you can always pick the active foundation IP as long as it remains available. |
| Microservice-to-microservice affinity | For microservice apps, you typically use a Services Registry to manage traffic between microservices. There are two ways to do this: <ul style="list-style-type: none"> If the microservices are using the domain which maps to the GLB, then their traffic is routed through the GLB. If the microservices are communicating using IP address or internal domains, such as when using Envoy, then the |

traffic does not pass through the GLB.

About Healthchecks

Healthchecks determine whether a foundation for an app is healthy or not.

See the following table for the levels at which you can check the health of your foundation:

| Level | Description |
|------------|--|
| Foundation | GLB relies on a local load balancer in front of the PCF Gorouters to determine the overall health of the foundation. GLB can perform healthchecks on TCP port 443 or 80 or on the local load balancer. The local load balancer healthchecks the backend pool of Gorouters on port 8080. |
| App | Healthchecks are set only for apps which have instances on both foundations. Each app instance has canary DNS records. The canary DNS records are the same for the app instances on each foundation. You would also need to add more VIPs dedicated to these canary apps that would be used to check their health. |

⚠ warning Pivotal does not recommend setting healthchecks at the app level. Configuring healthchecks in this way can cause more frequent failover and delays while pushing apps. Complete failover of a foundation affects all apps on the platform. Healthchecks on a per-app basis can require additional overhead beyond the control of an app developer.


Architecture and Installation Overview

For PCF Architects and Operators

This guide shows you how to design a Pivotal Cloud Foundry (PCF) platform and install it on an IaaS. If you are doing this, you have one or both of the following roles:

- **Architects** design a PCF platform. They know the IaaS that they will deploy it to, and what other relevant resources they have. In their design, they consider needs for the platform's capacity, availability, security, geography, budget, and other factors. If they do not install PCF themselves, they provide the architectural specifications to whoever does.
- **Operators** run a PCF platform, keep it up-to-date, monitor its health and performance, and fix any problems. They may also install the platform, or perform "Day 2" configurations that expand its functionality and integrate it with external systems.

This guide helps people in both roles create a PCF platform that does what they want it to. The contents of this guide follow the phases of a typical PCF planning and installation effort.

 **Note:** Elastic Runtime has been renamed Pivotal Application Service.

Planning and Installation Overview



PCF is a suite of products that runs on multiple IaaS. Planning and installing PCF means building layers from the bottom up, starting with the details of your IaaS and ending with "Day 2" configurations that you perform on a installed and running PCF deployment.

Here's the typical PCF planning and installation process:

1. Plan

- Review the Requirements for your IaaS ([AWS](#), [Azure](#), [GCP](#), [OpenStack](#), [vSphere](#)).
- Refer to the Reference Architecture for your IaaS.
- Assess your platform needs, including capacity, availability, container support, host OS, resource isolation, and geographical distribution. Discuss with your Pivotal contact.



2. Deploy BOSH and Ops Manager

- [BOSH](#)  is an open-source tool that lets you run software systems in the cloud.
 - BOSH and its IaaS-specific Cloud Provider Interfaces (CPIs) are what enable PCF to run on multiple IaaS.
 - See [Deploying with BOSH](#)  for a brief description of the BOSH deployment process.
- [Ops Manager](#) is a GUI application deployed by BOSH that streamlines deploying subsequent software to the cloud via BOSH.
 - Ops Manager represents PCF products as *tiles* with multiple configuration panes that let you input or select configuration values needed for the product.
 - Ops Manager generates BOSH manifests containing the user-supplied configuration values, and sends them to the Director.
 - After you install Ops Manager and BOSH, you use Ops Manager to deploy almost all PCF products.
- Deploying Ops Manager deploys both BOSH and Ops Manager with a single procedure.
 - On AWS, you can deploy Ops Manager manually, or automatically with a CloudFormation template.
 - On Azure, you can deploy Ops Manager manually, or automatically with an Azure Resource Manager (ARM) template. On Azure Government Cloud and Azure Germany you can only deploy Ops Manager manually.

3. Deploy BOSH Add-ons (Optional)

- BOSH add-ons include the [IPsec](#) , [ClamAV](#) , and [File Integrity Monitoring](#) , which enhance PCF platform security and security logging.
- You deploy these add-ons via BOSH rather than installing them with Ops Manager tiles.

4. Install Runtimes

- [PAS](#)  (Pivotal Application Service) lets developers develop and manage cloud-native apps and software services.
 - PAS is based on the Cloud Foundry Foundation's open-source Application Runtime (formerly Elastic Runtime) project.
- [PKS](#)  (Pivotal Container Service) uses BOSH to run and manage Kubernetes container clusters.

- PKS is based on the Cloud Foundry Foundation’s open-source Container Runtime (formerly Kubo) project.
- [PCF Isolation Segment](#) lets a single PAS deployment run apps from separate, isolated pools of computing, routing, and logging resources.
 - Operators replicate and configure an Isolation Segment tile for each new resource pool they want to create.
 - You must install PAS before you can install Isolation Segment.
- [PAS for Windows 2012R2](#) enables PAS to manage Windows Server 2012 cells hosting .NET apps, and can also be replicated to create multiple isolated resource pools.
 - As with Isolation Segment, Operators replicate and configure a PAS for Windows 2012R2 tile for each new resource pool they want to create.
 - You must install PAS before you can install PAS for Windows 2012R2.
- [Small Footprint PAS](#) is an alternative to PAS that uses far fewer VMs than PAS but has limitations.

5. Install Services

- Install software services for PCF developers to use in their apps.
 - Services include the databases, caches, and message brokers that stateless cloud apps rely on to save information.
 - Installing and managing software services on PCF is an ongoing process, and is covered in the [PCF Operator Guide](#).

6. Day 2 Configurations

- Day 2 configurations set up internal operations and external integrations on a running PCF platform.
 - Examples include front-end configuration, user accounts, logging and monitoring, internal security, and container and stemcell images.

Guide Contents

This guide has two parts. The first part explains the PCF planning and installation process, and the second describes the main tools that operators use when installing PCF.

Planning and Installation

PCF is a suite of products that runs on multiple IaaS. Planning and installing PCF means building layers from the bottom up, starting with the details of your IaaS and ending with “Day 2” configurations that you perform on a installed and running PCF deployment.

This guide follows this bottom-up progression:

- [Planning PCF](#) - Design a PCF platform that runs on your IaaS and fits your needs.
- [Deploying BOSH and Ops Manager](#) - Build the foundation of PCF.
- [Deploying BOSH Add-Ons](#) - Use BOSH to extend foundation-level PCF capabilities.
- [Using Ops Manager](#) - Ops Manager provides a dashboard for installing and configuring PCF products and services.
- [Using the Cloud Foundry Command Line Interface \(cf CLI\)](#) - The cf CLI runs PCF operations in the cloud from a shell on your local workstation.
- [Installing Runtimes](#) - Install the application and container runtime environments that PCF exists for.
- [Installing Platform Extension Tiles](#) - Use Ops Manager to extend PCF platform capabilities.
- [Day 2 Configurations](#) - Set up internal operations and external integrations for PCF.
- [Troubleshooting and Diagnostics](#)

After installing PCF, Operators install the software services that PCF developers use in their apps. These PCF services include the databases, caches, and message brokers that stateless cloud apps rely on to save information.

Installing and managing software services on PCF is an ongoing process, and is covered in the [PCF Operator Guide](#).

Related Documentation

The [PCF Operator Guide](#) explains how to maintain a running PCF platform, including monitoring, tuning, troubleshooting, and upgrading.

The [PCF Security Guide](#) explains how PCF security systems work and how to keep your PCF platform secure.

[Getting Started with PCF](#) gives a high-level overview of how PCF works and explains how you can try a simple deployment on your own local machine.

See [Pivotal Cloud Foundry Documentation](#) for all PCF documentation.

Preparing Your Firewall

Page last updated:

This topic describes how to configure your firewall for [Pivotal Cloud Foundry](#) (PCF) and how to verify that PCF resolves DNS entries behind your firewall.

Configure Your Firewall for PCF

Ops Manager and Pivotal Application Service (PAS) require the following open TCP ports:

- **25555**: Routes from Ops Manager to the BOSH Director.
- **443**: Routes to HAProxy or, if configured, your own load balancer.
- **80**: Routes to HAProxy or, if configured, your own load balancer.
- **8844**: Routes from Ops Manager to BOSH CredHub.
- **8443**: Routes from Ops Manager to BOSH Director UAA.
- **6868**: Routes to the BOSH Agent.
- **2222**: Necessary for using Application SSH. For details, see the [Diego Architecture Diagram](#).
- **25595**: Routes from the Traffic Controller to the BOSH Director, to enable sending BOSH health metrics to the Firehose.

UDP port **123** must be open if you want to use an external NTP server.

For more information about required ports for additional installed products, see [Network Communication Paths](#).

Example: Configure Firewall with iptables

The following example procedure uses `iptables` commands to configure a firewall.

Note: `GATEWAY_EXTERNAL_IP` is a placeholder. Replace this value with your `PUBLIC_IP`.

1. Open `/etc/sysctl.conf`, a file that contains configurations for Linux kernel settings, with the command below:

```
$ sudo vi /etc/sysctl.conf
```

2. Add the line `net.ipv4.ip_forward=1` to `/etc/sysctl.conf` and save the file.
3. If you want to remove all existing filtering or Network Address Translation (NAT) rules, run the following commands:

```
$ iptables --flush
$ iptables --flush -t nat
```

4. Add environment variables to use when creating the IP rules:

```
$ export INTERNAL_NETWORK_RANGE=10.0.0.0/8
$ export GATEWAY_INTERNAL_IP=10.0.0.1
$ export GATEWAY_EXTERNAL_IP=203.0.113.242
$ export PIVOTALCF_IP=10.0.0.2
$ export HA_PROXY_IP=10.0.0.254
```

5. Run the following commands to configure IP rules for the specified chains:

- **FORWARD:**

```
$ iptables -A FORWARD -i eth1 -j ACCEPT
$ iptables -A FORWARD -o eth1 -j ACCEPT
```

- **POSTROUTING:**

```
$ iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
$ iptables -t nat -A POSTROUTING -d $SHA_PROXY_IP -s $INTERNAL_NETWORK_RANGE \
  -p tcp --dport 80 -j SNAT --to $GATEWAY_INTERNAL_IP
$ iptables -t nat -A POSTROUTING -d $SHA_PROXY_IP -s $INTERNAL_NETWORK_RANGE \
  -p tcp --dport 443 -j SNAT --to $GATEWAY_INTERNAL_IP
```

◦ PREROUTING:

```
$ iptables -t nat -A PREROUTING -d $GATEWAY_EXTERNAL_IP -p tcp --dport \
  25555 -j DNAT --to $PIVOTALCF_IP
$ iptables -t nat -A PREROUTING -d $GATEWAY_EXTERNAL_IP -p tcp --dport \
  443 -j DNAT --to $SHA_PROXY_IP
$ iptables -t nat -A PREROUTING -d $GATEWAY_EXTERNAL_IP -p tcp --dport \
  80 -j DNAT --to $SHA_PROXY_IP
$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 8443 -j DNAT \
  --to $PIVOTALCF_IP:443
$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \
  --to $SHA_PROXY_IP:80
$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 8022 -j DNAT \
  --to $PIVOTALCF_IP:22
$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 8080 -j DNAT \
  --to $PIVOTALCF_IP:80
```

6. Run the following command to save the iptables:

```
$ service iptables save
```

For more information about administering IP tables with `iptables`, refer to the [iptables documentation](#).

Verify PCF Resolves DNS Entries Behind a Firewall

When you install PCF in an environment that uses a strong firewall, the firewall might block DNS resolution. For example, if you use [xip.io](#) to test your DNS configuration, the tests will fail without warning if the firewall prevents PAS from accessing `*.xip.io`.

To verify that PAS can correctly resolve DNS entries:

1. SSH into the Pivotal Ops Manager VM. For more information, refer to the [SSH into Ops Manager](#) section of the Advanced Troubleshooting with the BOSH CLI topic.
2. Run any of the following network administration commands with the IP address of the VM:
 - `nslookup`
 - `dig`
 - `host`
 - The appropriate `traceroute` command for your OS
3. Review the output of the command and fix any blocked routes. If the output displays an error message, review the firewall logs to determine which blocked route or routes you need to clear.
4. Repeat steps 1-3 with the BOSH Director VM and the HAProxy VM.

IaaS Permissions Guidelines

This topic describes practices recommended by Pivotal for creating secure IaaS user roles.

Pivotal Cloud Foundry (PCF) is an automated platform that connects to IaaS providers such as AWS and OpenStack. This connectivity typically requires accounts with appropriate permissions to act on behalf of the operator to access IaaS functionality such as creating virtual machines (VMs), managing networks and storage, and other related services.

Ops Manager and Pivotal Application Service (PAS) can be configured with IaaS users in different ways depending on your IaaS. Other product tiles and services might also use their own IaaS credentials. Refer to the documentation for those product tiles or services to configure them securely.

Least Privileged Users (LPUs)

Pivotal recommends following the principle of least privilege by scoping privileges to the most restrictive permissions possible for a given role. In the event that someone gains access to credentials by mistake or through malicious intent, LPUs limit the scope of the breach. Pivotal recommends following best practices for the particular IaaS you are deploying.

AWS Guidelines

See the recommendations detailed in the [AWS Permissions Guidelines](#) topic.

Azure Guidelines

See the permissions recommendations in [Preparing to Deploy Ops Manager on Azure Manually](#), and use the minimum permissions necessary when creating your service principal.

GCP Guidelines

For GCP, Pivotal recommends using two different accounts with the least privilege.

Use one account with the minimum permissions required to create desired GCP resources in your GCP project, then create a separate service account with the minimum permissions required to deploy PCF components such as Pivotal Ops Manager and PAS. For more information about creating the service account, see *Step 1: Set up IAM Service Accounts* in [Preparing to Deploy Ops Manager on GCP Manually](#).

OpenStack Guidelines

Pivotal recommends following the principle of least privilege by scoping privileges to the most restrictive permissions possible for a given role.

vSphere Guidelines

See the vCenter permissions recommendations in the [Installing Pivotal Cloud Foundry on vSphere](#) topic.

Installing PCF in Airgapped Environments

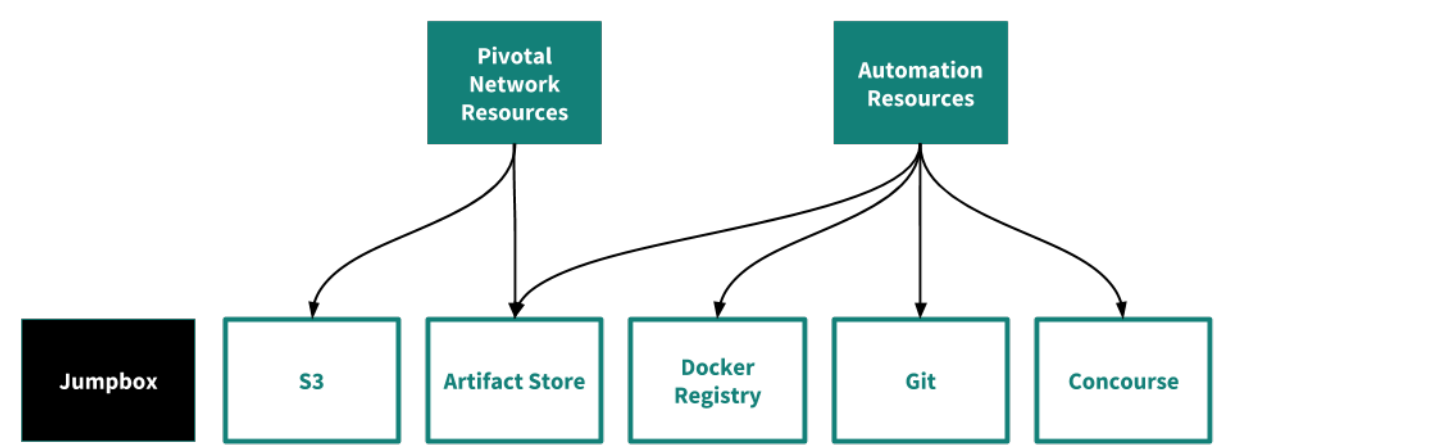
Page last updated:

This topic provides an overview of the components and resources needed to install PCF in airgapped environments, including the typical corresponding automation resources. It also describes one example solution that has been used in the past.

Offline Components

To run PCF offline, you must obtain resources from the internet and move them into offline components that store and use them. The method you use to move a resource from Pivotal Network or GitHub into an offline environment can vary from setting up a designated proxy to burning a DVD.

The following image displays types of resources and the components you must move them to in your offline environment. It also includes a jumpbox. The jumpbox is a Linux host for running commands such as `bosh`, `uaac`, and `fly`. You could use the Ops Manager VM for this purpose.



The following table provides more detail about resources and the component you must move them to:

| Resource | Component |
|---|--|
| Pivotal Network products such as tiles, stemcells, BOSH releases, and Ops Manager | S3 and artifact store |
| Pipelines and scripts | Git |
| Configuration | Git |
| Container images | Docker Registry, S3, or artifact store |
| Third Party Resources such as NSX-T and OSS BOSH releases | Artifact store |
| Backup artifacts | S3 |

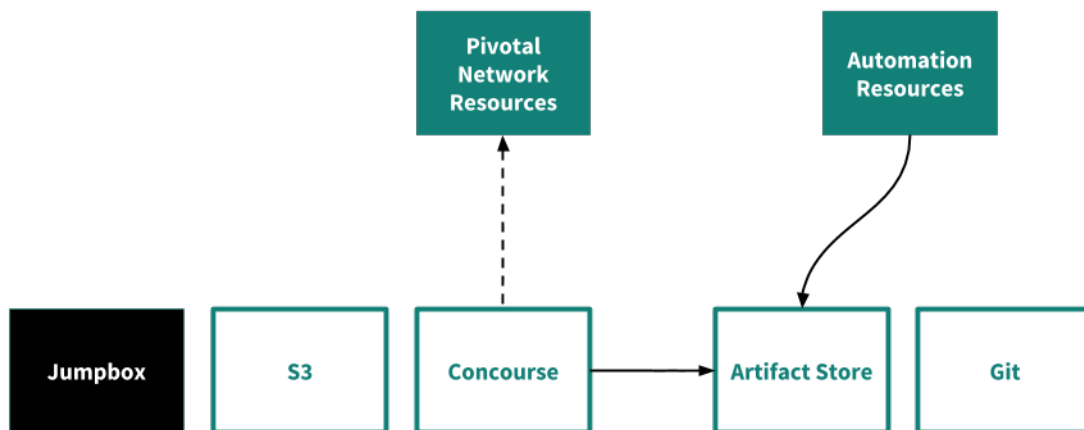
Architectural Patterns

The following sections describe three architectural patterns for running PCF in airgapped environments. The pattern you use depends on how your environment is set up.

Pattern One: Artifact Store with Internet Access

It is common for organizations to deploy an artifact store such as Artifactory or Nexus as a gateway to the Internet. In this configuration, the artifact store is typically configured as a Docker mirror.

This pattern includes an S3 component that is used only for backups of the PCF installation.

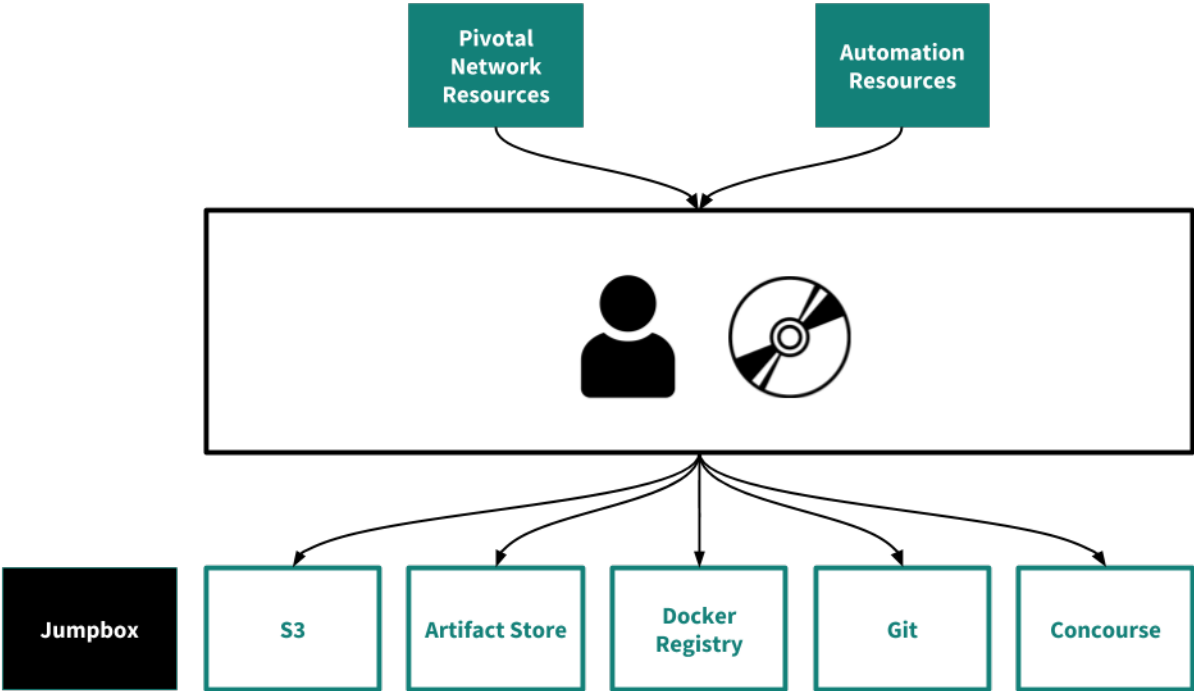


The following table provides an example of how you might handle resources in this scenario:

| Resource | Component |
|---|---|
| Pivotal Network products such as tiles, stemcells, BOSH releases, and Ops Manager | This architectural pattern presents the challenge of getting Pivotal Network resources from the Internet into the artifact store. For example, Artifactory and Nexus cannot interact directly with Pivotal Network. You could place Pivotal Network resources in an artifact store either through a remote Concourse worker with access to the Internet, by downloading them from the Internet and placing them in the artifact store manually, or some other method. |
| Pipelines and scripts | Store in Git. Use manual clone and push. Modify pipelines to use <code>registry_mirror</code> . |
| Configuration | Store in Git. Use manual clone and push. |
| Container images | Store in the artifact store that you configured as a mirror. |
| Third Party Resources such as NSX-T and OSS BOSH releases | Store in a generic artifact store repository. |
| Backup artifacts | Store in a S3 blobstore. |

Pattern Two: Completely Offline

In completely offline environments, you must bring in all resources manually and store them in the available local components.

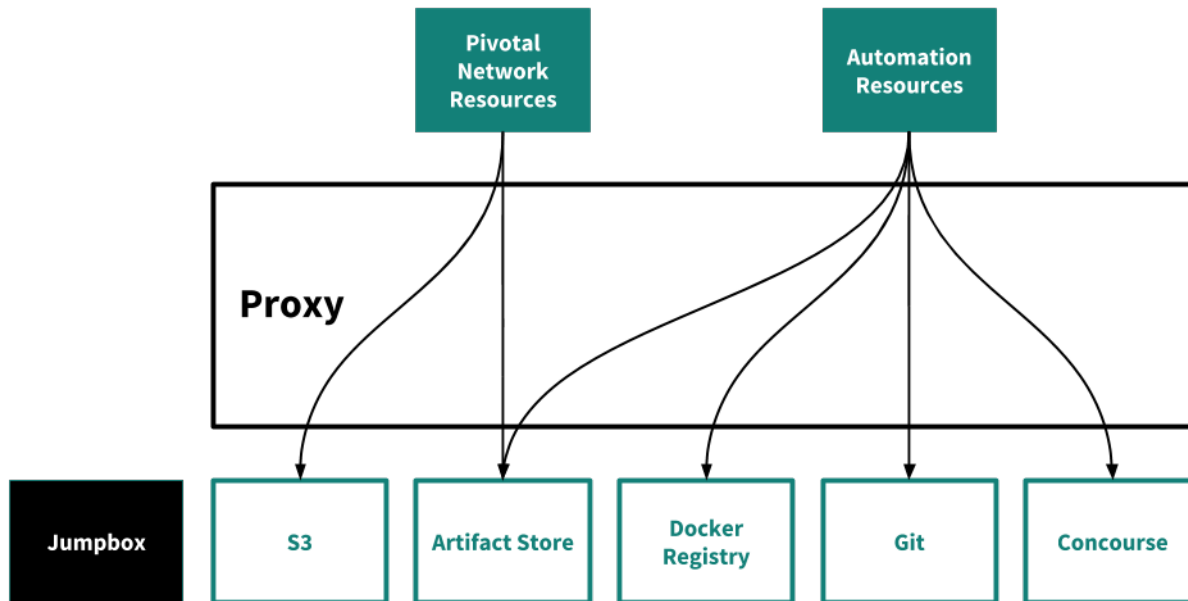


In this architectural pattern, you must configure pipelines to watch components for changes and apply updates when available. The following table provides an example of how you might handle resources in this scenario:

| Resource | Component |
|---|---|
| Pivotal Network products such as tiles, stemcells, BOSH releases, and Ops Manager | Manually upload to Nexus. |
| Pipelines and scripts | Modify pipelines to use a local Harbor Docker registry. Manually clone an online environment, bring it to the offline environment on DVD, and push it to offline Git. |
| Configuration | Store in your offline Git. |
| Container Images | Get from the Internet, transfer to USB, and push to offline Harbor. |
| Third Party Resources such as NSX-T and OSS BOSH releases | Store in a generic artifact store repository. |
| Backup artifacts | Store in a S3 blobstore. |

Pattern Three: TLS Intercepting Proxy

This pattern allows Internet access, but only through a proxy that decrypts and rewrites TLS certificates. In general, this resembles an online install, however it requires that you add your corporate certificate to all BOSH-deployed VMs.



Some of the challenges in this pattern include the following:

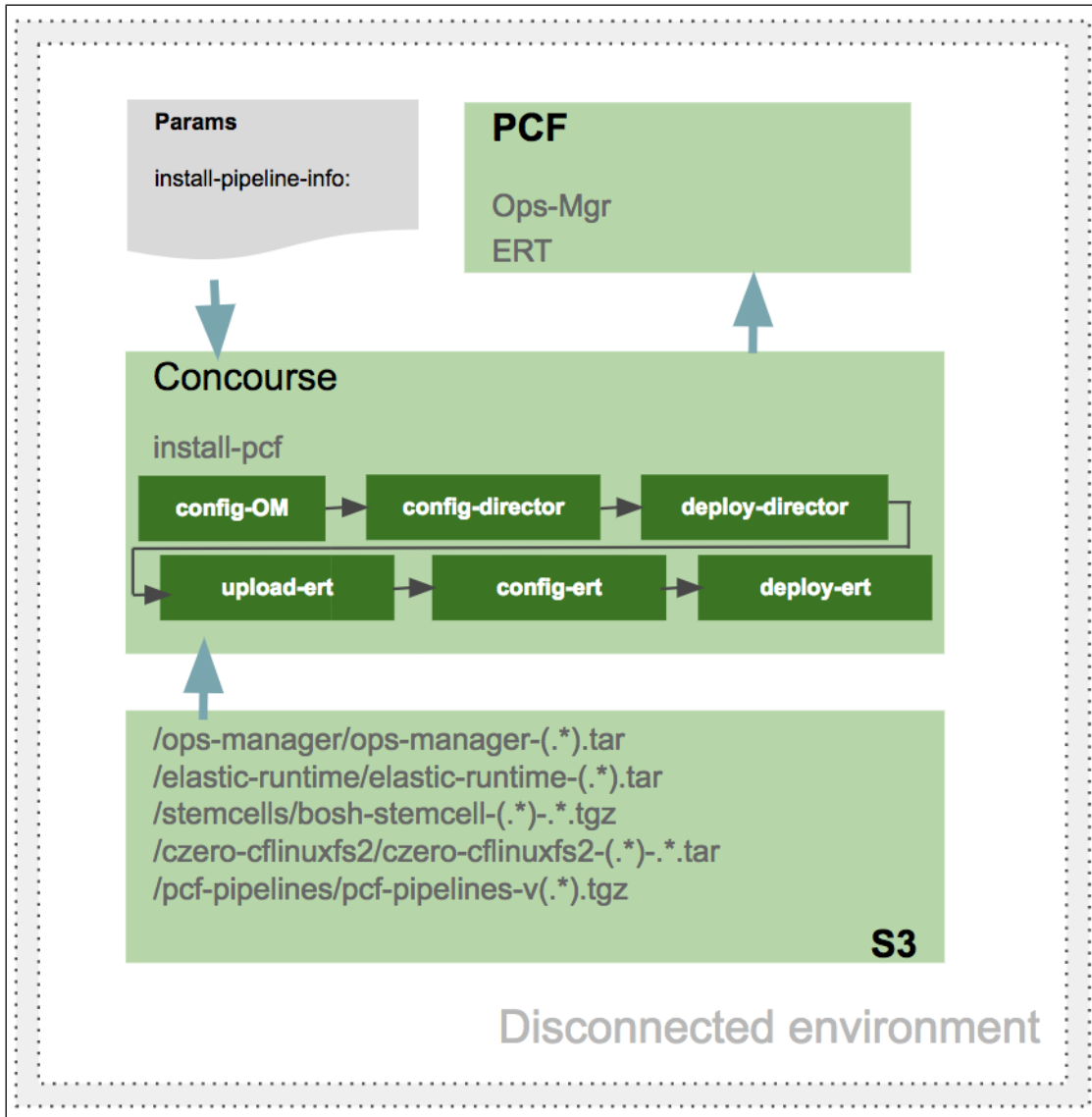
- Any automation that calls to the Internet will fail if it does not have the corporate certificate in its trust store.
- Concourse tasks that do not use resources do not receive updated BOSH root certificates. This means you must configure tasks to ignore TLS errors or update the root certificates as part of the tasks.

Example Installation in Airgapped Environment

In this example solution, an operator uses [Concourse](#) as the [control plane architecture](#) and specialized [PCF Pipelines](#) to deploy PCF to computer networks physically isolated from the Internet.

⚠ warning: At time of publication, the PCF Pipelines repository is undergoing planned deprecation. Use this document only as a model and reference when implementing your own solution.

The following diagram presents a high-level overview of this solution:



This implementation runs in two environments, one airgapped and one Internet-connected. Each environment has its own Concourse server and pipeline. The airgapped environment bootstraps from an internal S3 repository populated by contents moved over as `tar` files from the Internet-connected environment.

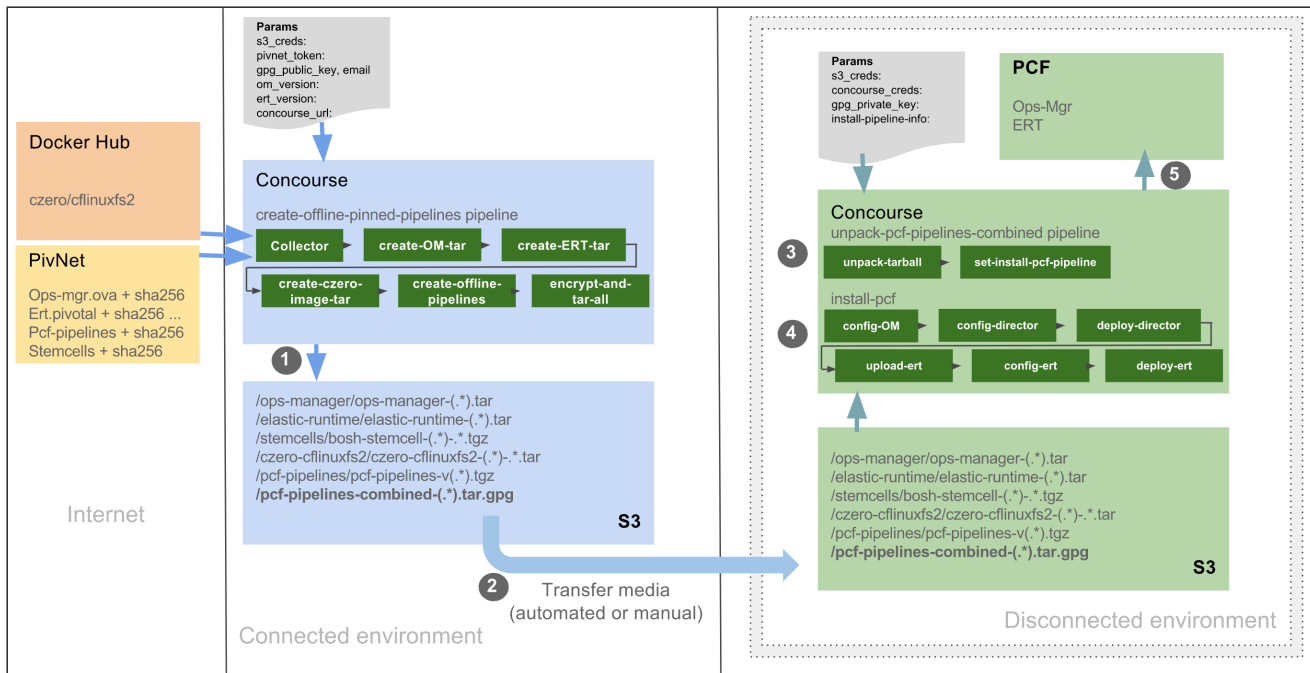
Requirements

This solution requires the following:

- Internet-connected environment with access to DockerHub and PivNet.
- Concourse v3.3.3 or later, installed in both the Internet-connected and airgapped environments.
- A path from the Internet-connected environment to the airgapped environment. All artifacts, such as release files, Docker images and scripts, must be downloaded and packaged within an Internet-connected network, then transferred to the airgapped environment.
- An offline S3-compatible blobstore. The airgapped Concourse pipeline retrieves artifacts from a Concourse [S3 Resource](#). There are many S3-compatible blobstores that you can use within airgapped environments, such as [Minio](#) and [Dell EMC Elastic Cloud Storage](#).

Bootstrap the Pipelines

As illustrated in the diagram below, two pipelines help bootstrap the offline environment, `create-offline-pinned-pipelines` and `unpack-pcf-pipelines-combined`. These pipelines are meant to facilitate physical transfer of artifacts to the airgapped environment.



Pipelines Execution Flow

1. Download artifacts from external sources, sign, package and upload them to S3 repository.
2. Move packaged artifacts to disconnected environment's S3 repository (either manual or automated.)
3. Unpack artifacts, check their signature and setup offline `pcf-pipelines` with new artifacts.
4. `pcf-pipelines` are triggered upon existence of new artifacts in S3 repository.
5. PCF is deployed by `pcf-pipelines` in disconnected environment.

Create Offline Pinned Pipelines

The `create-offline-pinned-pipelines` does the following:

- Pulls all required resources (images, products and pipelines) from their locations on the Internet and package them.
- Transforms `pcf-pipelines` to consume the resources from S3-compatible blobstore.
- Creates an encrypted tarball with all resources, and a shasum manifest for each resource.
- Puts the tarball to a location within S3 storage for it to be transferred to the airgapped environment.

To download this pipeline, see [create-offline-pinned-pipelines](#).

The following screenshot shows how this pipeline appears in the Concourse dashboard.



[View a larger version of this diagram.](#)

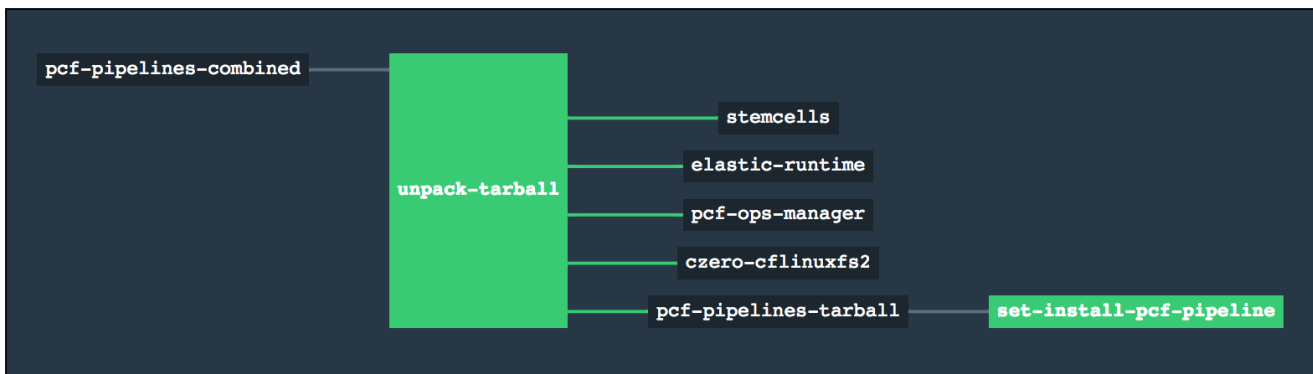
Unpack PCF Pipelines

The `unpack-pcf-pipelines-combined` does the following:

- Downloads, decrypts, and extracts the GPG-encrypted tarball into its components after it has been transferred to the `pcf-pipelines-combined/` path in the S3-compatible store.
- Verifies the `shasum` manifest of the tarball contents.
- Puts the tarball parts into their appropriate locations within the airgapped S3 storage for use by the pipelines.

To download this pipeline, see [unpack-pcf-pipelines-combined](#).

The following screenshot shows how this pipeline appears in the Concourse dashboard.



[View a larger version of this diagram.](#)

From this point, the `pcf-pipelines` folder in the configured S3 bucket in the airgapped environment contains the pcf-pipelines tarball that can then be used to set a pipeline on an airgapped Concourse, in the same fashion as a standard `pcf-pipelines` setup.

Bootstrapping Requirements

For the `unpack-pcf-pipelines-combined` to work, there must be a single manual transfer of the `cszero-cflinuxfs2` tarball to the `cszero-cflinuxfs2` folder within the airgapped environment's S3 storage. Only after that is done can the `unpack-pcf-pipelines-combined` pipeline be set and unpaused.

Install in the China Region

Question: I am a customer headquartered in the US with another location in China, but am experiencing problems downloading Pivotal software directly to my China location. What should I do?

Disclaimer: This question has legal implications, and Pivotal cannot provide legal advice to anyone about their specific obligations under any applicable laws and regulations in China or elsewhere (including, but not limited to, the laws and regulations on import/export and cyber security.) So you should seek legal guidance regarding your own import/export compliance under all the applicable laws or other obligations regarding this issue. The following

information is provided to you for your reference only. Pivotal expressly disclaims all liabilities in respect to actions taken or not taken based on the following information.

Certain customers have used the above solution under the above use case, which may or may not address your issue. A customer headquartered in the United States (U.S.) has another location in China, each with their own environments/systems. Customer downloads our software from Pivotal Network (PivNet) from our PivNet servers in the U.S. Customer employee then copies our software from the customer's environment in the U.S. to customer's environment in China. Customer's China location then uses that locally available version of our software, instead of downloading it directly from PivNet to customer's China location.

Installing Pivotal Cloud Foundry on AWS

Page last updated:

This guide describes how to install [Pivotal Cloud Foundry](#) (PCF) on Amazon Web Services (AWS).

Overview

You can install PCF on AWS with either the Pivotal Application Service (PAS) or Pivotal Container Service (PKS) runtime. There are resource requirements specific to each runtime. Ensure you meet the requirements for your runtime and the requirements specific to AWS before installing PCF on AWS.

Requirements

This section lists the following resource requirements for installing PCF on AWS:

- General PCF resource requirements. See [PCF Resource Requirements](#).
- AWS-specific resource requirements. See [AWS Resource Requirements](#).

PCF Resource Requirements

This section lists PCF resource requirements for installing PCF on AWS. It includes general PCF resource requirements for both the PAS and PKS runtimes.

View one of the following, depending on your PCF runtime:

- PAS-specific PCF resource requirements. See [PAS Resource Requirements](#).
- PKS-specific PCF resource requirements. See [PKS Resource Requirements](#).

PAS Resource Requirements

The following are general resource requirements for deploying and managing a PCF deployment with Ops Manager and PAS:

- PAS requires sufficient IP allocation. The following lists the minimum required IP allocations:
 - One static IP address for either HAProxy or one of your Gorouters
 - One static IP address for each job in the Ops Manager **Resource Config** pane for each tile for a full list.
 - One static IP address for each job listed below:
 - Consul
 - NATS
 - File Storage
 - MySQL Proxy
 - MySQL Server
 - Backup Restore Node
 - HAProxy
 - Router
 - MySQL Monitor
 - Diego Brain
 - TCP Router
 - One IP for each VM instance created by the service.
 - An additional IP address for each compilation worker. Use the following formula to determine the total IPs required:

$$\text{IPs needed} = \text{static IPs} + \text{VM instances} + \text{compilation workers}$$
 - Pivotal recommends that you allocate at least 36 dynamic IP addresses when deploying Ops Manager and PAS. BOSH requires additional dynamic IP addresses during installation to compile and deploy VMs, install PAS, and connect to services.
- Pivotal recommends using a network without DHCP for deploying PAS VMs.



Note: If you have DHCP, refer to the [Troubleshooting Guide](#) to avoid issues with your installation.

PKS Resource Requirements

For PKS-specific resource requirements, see [AWS Prerequisites and Resource Requirements](#).

AWS Resource Requirements

The following are AWS-specific resource requirements for installing PCF on AWS with an external database and external file storage:

- Installing PCF on AWS requires a minimum of the following VM instance limits in your AWS account. The number of VMs required depends on the number of tiles and availability zones you plan to deploy. The following VM guidelines apply to the PAS, Small Footprint PAS, and PKS runtimes:
 - PAS:** At a minimum, a new AWS deployment requires the following VMs for PAS:

| AWS Requirements | VM Name | VM Type | Default VM Count | Required or Optional VM |
|------------------|-------------------------------|-----------|------------------|-------------------------|
| PAS | Consul | t2.micro | 3 | Required |
| | NATS | t2.micro | 2 | Required |
| | File Storage | m4.large | 1 | Optional |
| | MySQL Proxy | t2.micro | 2 | Optional |
| | MySQL Server | r4.large | 3 | Optional |
| | Backup Restore Node | t2.micro | 1 | Optional |
| | Diego BBS | t2.micro | 3 | Required |
| | UAA | m4.large | 2 | Required |
| | Cloud Controller | m4.large | 2 | Required |
| | HAProxy | t2.micro | 1 | Optional |
| | Router | t2.micro | 3 | Required |
| | Service Discovery Controller | t2.micro | 2 | Optional |
| | MySQL Monitor | t2.micro | 1 | Optional |
| | Clock Global | t2.medium | 2 | Required |
| | Cloud Controller Worker | t2.micro | 2 | Required |
| | Diego Brain | t2.small | 3 | Required |
| | Diego Cell | r4.xlarge | 3 | Required |
| | Loggregator Trafficcontroller | t2.micro | 3 | Required |
| | Syslog Adapter | t2.micro | 3 | Required |
| | Syslog Scheduler | t2.micro | 2 | Required |
| | Doppler Server | m4.large | 3 | Required |
| | TCP Router | t2.micro | 0 | Optional |
| | CredHub | r4.large | 0 | Optional |
| Istio Router | r4.large | 0 | Optional | |
| Istio Control | r4.large | 0 | Optional | |
| Route Syncer | r4.large | 0 | Optional | |
| Ops Manager | BOSH Director | m4.large | 1 | Required |



Note: If you are deploying a test or sandbox PCF that does not require high availability, then you can scale down the number of VM instances in your deployment. For more information, see [Scaling PAS](#).

- Small Footprint PAS:** To run Small Footprint PAS, a new AWS deployment requires:

| AWS Requirements | VM Name | VM Type | Default VM Count | Minimum HA VM Count | Required or Optional VM |
|------------------|----------|-----------|------------------|---------------------|-------------------------|
| | Compute | r4.xlarge | 1 | 3 | Required |
| | Control | r4.xlarge | 1 | 2 | Required |
| | Database | r4.large | 1 | 3 | Required |
| | Router | t2.micro | 1 | 3 | Required |


| | | | | | |
|---------------------|---------------------|----------|---|----------|----------|
| Small Footprint PAS | File Storage | m4.large | 1 | N/A | Optional |
| | Backup Restore Node | t2.micro | 1 | 1 | Optional |
| | MySQL Monitor | t2.micro | 1 | 1 | Optional |
| | HAProxy | t2.micro | 0 | 2 | Optional |
| | TCP Router | t2.micro | 0 | 1 | Optional |
| Istio Router | r4.large | 0 | 1 | Optional | |
| Istio Control | r4.large | 0 | 2 | Optional | |
| Route Syncer | r4.large | 0 | 1 | Optional | |
| Ops Manager | BOSH Director | m4.large | 1 | N/A | Required |

- **PKS:** See [AWS Prerequisites and Resource Requirements](#).
- The following AWS resources are required for installing PCF on AWS with PAS:
 - 3 Elastic Load Balancers (ELBs)
 - 1 Relational Database Service. As a minimum, Pivotal recommends using a db.m3.xlarge instance with at least 100 GB of allocated storage.
 - 5 S3 Buckets

Prerequisites

To install PCF on AWS, you must do the following:

- Increase or remove the VM instance limits in your AWS account. Installing PCF requires more than the default 20 concurrent instances. For more information about VM resource requirements, see [Requirements](#).
- Configure your AWS account with the appropriate AWS region. For more information about selecting the correct region for your deployment, see [Region and Availability Zone Concepts](#) in the AWS documentation.
- Install the AWS CLI. Configure the AWS CLI with the user credentials that have admin access to your AWS account. To download the AWS CLI, see [AWS CLI](#).
- Configure an AWS EC2 key pair to use with your PCF deployment. For more information, see [Creating an EC2 Key Pair](#) in the AWS documentation.
- Register a wildcard domain for your PCF installation. For more information, see [SSL/TLS Certificates for Classic Load Balancers](#) in the AWS documentation.
- Create an SSL certificate for your PCF domain. For more information, see the [AWS documentation about SSL certificates](#).

 **Note:** To deploy PCF to a production environment, you must obtain a certificate from a certificate authority. Pivotal recommends using a self-signed certificate generated by Ops Manager for development and testing purposes only.

- **(PAS-only)** Configure sufficient IP allocation. For more information about IP allocation requirements, see [PAS Resource Requirements](#).
- **(Optional) (PAS-only)** Configure external storage. Pivotal recommends using external storage if possible. For more information about how file storage location affects platform performance and stability during upgrades, see [Configure File Storage](#).
- **(Optional) (PAS and Ops Manager-only)** Configure external databases. Pivotal recommends using external databases in production deployments for BOSH Director and PAS. An external database must be configured to use the UTC timezone.
- **(Optional) (PAS and Ops Manager-only)** Configure external user stores. When you deploy PCF, you can select a SAML user store for Ops Manager or a SAML or LDAP user store for PAS, to integrate existing user accounts.

Install PCF on AWS

You can install PCF on AWS either manually or using Terraform.

To install PCF on AWS, do one of the following:

- Install PCF on AWS manually. See [Installing PCF on AWS Manually](#).
- Install PCF on AWS using Terraform. See [Install PCF on AWS Using Terraform](#).

Additional Resources

The following are additional resources related to installing PCF on AWS:




- For information about AWS identity and access management, see [What is IAM?](#) in the AWS documentation.
- For information about users, groups, and roles in AWS, see [Identities \(Users, Groups, and Roles\)](#) in the AWS documentation.
- For best practices for managing IaaS users and permissions, see [Temporary Security Credentials](#) in the AWS documentation.
- For recommendations on how to create and scope AWS accounts for PCF, see [AWS Permissions Guidelines](#).
- For more information about certificate requirements for installing PCF, see [Certificate Requirements](#).

AWS Permissions Guidelines

Pivotal recommends that you minimize the use of master account credentials by creating an IAM role and instance profile with the minimum required EC2, VPC, and EBS credentials.

In addition, Pivotal recommends that you follow AWS account security best practices such as disabling root keys, using multi-factor authentication on the root account, and using CloudTrail for auditing API actions.

For more Amazon-specific best practices, refer to the following Amazon documentation:

- [IAM Roles Best Practices](#) 
- [AWS Security Best Practices Whitepaper](#) 
- [AWS Well-Architected Framework](#) 

Installing PCF on AWS Manually

Page last updated:

This topic describes how to manually configure the Amazon Web Services (AWS) components that you need to run [Pivotal Cloud Foundry](#) (PCF) on AWS.

To deploy PCF on AWS, you must perform the procedures in this topic to create objects in the AWS Management Console that PCF requires.

To view the list of AWS objects created by the procedures in this topic, see the [Required AWS Objects](#) section.

After completing the procedures in this topic, proceed to [Configuring BOSH Director on AWS](#) to continue deploying PCF.

Step 1: File a Ticket

Log in to the AWS Management Console, and file a ticket with Amazon to ensure that your account can launch more than the default 20 instances. In the ticket, ask for a limit of 50 `t2.micro` instances and 20 `c4.large` instances in the region you are using.

Note: To deploy PCF to AWS GovCloud (US), log in to the [AWS GovCloud \(US\) Console](#) instead of the standard AWS Management Console and select the `us-gov-west-1` region.

Note: To deploy PCF to AWS China, set up an [AWS China](#) account and contact the Platform Architect assigned for your Pivotal account.

You can check the limits on your account by visiting the EC2 Dashboard on the AWS Management Console and clicking **Limits** on the left navigation.

Step 2: Create S3 Buckets

1. Navigate to the S3 Dashboard.

Note: S3 bucket names must be globally unique. When naming buckets, Pivotal recommends that you prefix the generic names below with an unique and helpfully identifiable string (i.e. `ID-STRING-pcf-ops-manager-bucket`, `MY-IDENTIFIER-pcf-buildpacks-bucket`, and so on). Then you should use the same prefix when naming other associated resources, such as IAM policies.

2. Perform the following steps to create five S3 buckets:

- Click **Create Bucket**
- For **Bucket name**, enter `ID-STRING-pcf-ops-manager-bucket`.
- For **Region**, select your region.
- Click **Next** three times.
- Click **Create bucket**.
- Repeat the above steps to create four more S3 buckets: `ID-STRING-pcf-buildpacks-bucket`, `ID-STRING-pcf-packages-bucket`, `ID-STRING-pcf-resources-bucket`, and `ID-STRING-pcf-droplets-bucket`.

Step 3: Create an IAM User for PCF

Perform the following steps to create an Amazon Identity and Access Management (IAM) user with the minimal permissions necessary to run and install PCF:

1. Click **IAM** to access the IAM Dashboard.
2. Click **Users** and then click **Add user**.

Add user

1

2

3

4

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

[Cancel](#) [Next: Permissions](#)


3. Enter a user name, such as `pcf-user`.

4. For AWS access type, select **Programmatic access**.

 **Note:** If you prefer to create your keys locally and import them into AWS, see the [Amazon documentation](#).


5. Click **Next: Permissions**.

6. Click **Next: Review** and review your choices.

 **Note:** On the **Review** page you may see a warning that the user has no permissions. You can disregard this message. You do not need to set user permissions.


7. Click **Create user**.

8. Click **Download .csv** to download the user security credentials.

 **warning:** The `credentials.csv` contains the IDs for your user security access key and secret access key. Keep the `credentials.csv` file for your currently active key pairs in a secure directory. You cannot recover a lost key pair.

9. Click **Close**.

10. On the **Users** page, click the user name to access the user details page.

 **Note:** On the **Users** page you may see a warning that the user has no permissions. You can disregard this message. You do not need to set user permissions.

11. Click **Add inline policy**. You can review your existing inline policies by clicking the down arrow.

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

This policy validation failed and might have errors converting to JSON : The policy must have at least one statement For more information about the IAM policy grammar, see [AWS IAM Policies](#)

Visual editor **JSON** [Import managed policy](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Deny",
6       "Action": [
7         "iam:*"
8       ],
9       "Resource": [
10        "*"
11      ]
12    },
13    {
14      "Sid": "OpsMgrInfrastructureIaasConfiguration",
15      "Effect": "Allow",
16      "Action": [
17        "iam:CreatePolicy",
18        "iam:DeletePolicy",
19        "iam:AttachPolicy",
20        "iam:DetachPolicy"
21      ],
22      "Resource": [
23        "*"
24      ]
25    }
26  ]
27 }
```

[Cancel](#) [Review policy](#)

12. On the **Create policy** page, define a policy:
 - a. Copy the policy document included in the [Pivotal Cloud Foundry for AWS Policy Document](#) topic. You must edit the policy document so the names of the S3 buckets match the ones you created in [Step 2: Create S3 Buckets](#).
 - b. Paste the policy document into the **JSON** tab on the **Create policy** page.
13. Click **Review policy**.
14. In the **Name** field, enter `pcf-iam-policy`.
15. Click **Create policy**. The **Summary** page displays a list of available policies and actions.

Step 4: Create a VPC

1. Navigate to the VPC Dashboard.
2. Click **Start VPC Wizard**.

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Resources

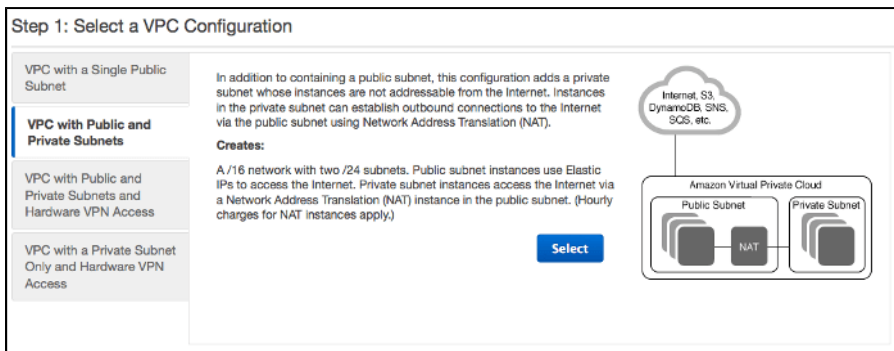
[Start VPC Wizard](#) [Launch EC2 Instances](#)

Note: Your Instances will launch in the US East (N. Virginia) region.

You are using the following Amazon VPC resources in the US East (N. Virginia) region:

| | |
|---------------------------|----------------------------|
| 2 VPCs | 2 Internet Gateways |
| 4 Subnets | 4 Route Tables |
| 2 Network ACLs | 3 Elastic IPs |
| 6 Security Groups | 18 Running Instances |
| 0 VPC Peering Connections | 0 Customer Gateways |
| 0 VPN Connections | 0 Virtual Private Gateways |

3. Select **VPC with Public and Private Subnets** and click **Select**.



4. Specify the following details for your VPC:

- **IPv4 CIDR block:** Enter `10.0.0.0/16`.
- **IPv6 CIDR block:** Select **No IPv6 CIDR Block**.
- **VPC name:** `pcf-vpc`.
- **Public subnet's IPv4 CIDR:** Enter `10.0.0.0/24`.
- Set the **Availability Zone** fields for both subnets to `REGION-#a`. For example, `us-west-2a`.
- **Public subnet name:** Enter `pcf-public-subnet-az0`.
- **Private subnet's IPv4 CIDR:** Enter `10.0.16.0/28`.
- **Private subnet name:** Enter `pcf-management-subnet-az0`.
- Click **Use a NAT instance instead** and do the following:
 - Under **Specify the details of your NAT instance**, set the **Instance type** to `t2.medium`
 - Create a key pair titled `pcf-ops-manager-key`. For more information on creating the key pair, see [Amazon EC2 Key Pairs](#) in the AWS documentation.
 - Select your newly-created `pcf-ops-manager-key` for the **Key Pair name**.
- **Enable DNS hostnames:** Click **Yes**.
- **Hardware tenancy:** Select **Default**.
- Click **Create VPC**.

5. After the VPC is successfully created, click **Subnets** in the left navigation.

6. Click **Create Subnet**.

7. Add the following subnets to the `pcf-vpc` VPC:

Note: You created the first two subnets in the previous step: `pcf-public-subnet-az0` and `pcf-management-subnet-az0`.

| Name | AZ | IPv4 CIDR block |
|--|--|----------------------------|
| <code>pcf-public-subnet-az1</code> | <code>REGION-#b</code> (for example, <code>us-west-2b</code>) | <code>10.0.1.0/24</code> |
| <code>pcf-public-subnet-az2</code> | <code>REGION-#c</code> (for example, <code>us-west-2c</code>) | <code>10.0.2.0/24</code> |
| <code>pcf-management-subnet-az1</code> | <code>REGION-#b</code> (for example, <code>us-west-2b</code>) | <code>10.0.16.16/28</code> |
| <code>pcf-management-subnet-az2</code> | <code>REGION-#c</code> (for example, <code>us-west-2c</code>) | <code>10.0.16.32/28</code> |
| <code>pcf-ert-subnet-az0</code> | <code>REGION-#a</code> (for example, <code>us-west-2a</code>) | <code>10.0.4.0/24</code> |
| <code>pcf-ert-subnet-az1</code> | <code>REGION-#b</code> (for example, <code>us-west-2b</code>) | <code>10.0.5.0/24</code> |
| <code>pcf-ert-subnet-az2</code> | <code>REGION-#c</code> (for example, <code>us-west-2c</code>) | <code>10.0.6.0/24</code> |
| <code>pcf-services-subnet-az0</code> | <code>REGION-#a</code> (for example, <code>us-west-2a</code>) | <code>10.0.8.0/24</code> |
| <code>pcf-services-subnet-az1</code> | <code>REGION-#b</code> (for example, <code>us-west-2b</code>) | <code>10.0.9.0/24</code> |
| <code>pcf-services-subnet-az2</code> | <code>REGION-#c</code> (for example, <code>us-west-2c</code>) | <code>10.0.10.0/24</code> |
| <code>pcf-rds-subnet-az0</code> | <code>REGION-#a</code> (for example, <code>us-west-2a</code>) | <code>10.0.12.0/24</code> |
| <code>pcf-rds-subnet-az1</code> | <code>REGION-#b</code> (for example, <code>us-west-2b</code>) | <code>10.0.13.0/24</code> |
| <code>pcf-rds-subnet-az2</code> | <code>REGION-#c</code> (for example, <code>us-west-2c</code>) | <code>10.0.14.0/24</code> |

Step 5: Configure a Security Group for Ops Manager

1. Return to the EC2 Dashboard.
2. Select **Security Groups>Create Security Group**.
3. For **Security group name**, enter `pcf-ops-manager-security-group`.
4. For **Description**, enter a description to identify this security group.
5. For **VPC**, select the VPC where you want to deploy Ops Manager.
6. Click the **Inbound** tab and add rules according to the table below.



Note: Pivotal recommends limiting access to Ops Manager to IP ranges within your organization, but you may relax the IP restrictions after configuring authentication for Ops Manager.

| Type | Protocol | Port Range | Source |
|---------------|----------|------------|-------------|
| HTTP | TCP | 80 | My IP |
| HTTPS | TCP | 443 | My IP |
| SSH | TCP | 22 | My IP |
| BOSH Agent | TCP | 6868 | 10.0.0.0/16 |
| BOSH Director | TCP | 25555 | 10.0.0.0/16 |

7. Click **Create**.

Step 6: Configure a Security Group for PCF VMs

1. From the **Security Groups** page, click **Create Security Group** to create another security group.
2. For **Security group name**, enter `pcf-vms-security-group`.
3. For **Description**, enter a description to identify this security group.
4. For **VPC**, select the VPC where you want to deploy the PCF VMs.
5. Click the **Inbound** tab and add rules for all traffic from your public and private subnets to your private subnet, as the table and image show. This rule configuration does the following:
 - Enables BOSH to deploy PAS and other services.
 - Enables application VMs to communicate through the router.
 - Allows the load balancer to send traffic to Pivotal Application Service (PAS).

| Type | Protocol | Port Range | Source |
|-------------|----------|------------|-----------------------|
| All traffic | All | 0 - 65535 | Custom IP 10.0.0.0/16 |

6. Click **Create**.

The screenshot shows the AWS Management Console interface for creating a security group. The 'Security group name' is 'pcf/vms', the 'Description' is 'pcf/vms', and the 'VPC' is 'vpc-1e4b1a7b (10.0.0.0/16) pcf-vpc'. Under 'Security group rules', the 'Inbound' tab is active, showing a table with one rule: 'All traffic' from 'Custom IP 10.0.0.0/16' on ports '0 - 65535'.

Step 7: Configure a Security Group for the Web ELB

1. From the **Security Groups** page, click **Create Security Group** to create another security group.

- For **Security group name**, enter `pcf-web-elb-security-group`.
- For **Description**, enter a description to identify this security group.
- For **VPC**, select the VPC where you want to deploy this Elastic Load Balancer (ELB).
- Click the **Inbound** tab and add rules to allow traffic to ports `80`, `443`, and `4443` from `0.0.0.0/0`, as the table and image show.

Note: Allow traffic to port `4443` only if you are in an AWS cloud region that does not support AWS ALBs. For example, the GovCloud region. For more information about AWS regions and availability zones, see [AWS Global Infrastructure](#).

Note: For finer control over what can reach PAS, change `0.0.0.0/0` to be more restrictive. This security group governs external access to PAS from apps such as the cf CLI and app URLs.

| Type | Protocol | Port Range | Source | |
|-----------------|----------|------------|----------|-----------|
| Custom TCP rule | TCP | 4443 | Anywhere | 0.0.0.0/0 |
| HTTP | TCP | 80 | Anywhere | 0.0.0.0/0 |
| HTTPS | TCP | 443 | Anywhere | 0.0.0.0/0 |

- Click **Create**.

Create Security Group

Security group name i

Description i

VPC i

Security group rules:

Inbound

Outbound

| Type <small>i</small> | Protocol <small>i</small> | Port Range <small>i</small> | Source <small>i</small> | Description <small>i</small> |
|-----------------------------|---------------------------|-----------------------------|---|------------------------------|
| Custom TCP <small>i</small> | TCP | 4443 | Anywhere <small>i</small> 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |
| HTTP <small>i</small> | TCP | 80 | Anywhere <small>i</small> 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |
| HTTPS <small>i</small> | TCP | 443 | Anywhere <small>i</small> 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |

Add Rule

Cancel

Create

Step 8: Configure a Security Group for the SSH ELB

- From the **Security Groups** page, click **Create Security Group** to create another security group.
- For **Security group name**, enter `pcf-ssh-elb-security-group`.
- For **Description**, enter a description to identify this security group.
- For **VPC**, select the VPC where you want to deploy this ELB.
- Click the **Inbound** tab and add the following rule:

| Type | Protocol | Port Range | Source | |
|-----------------|----------|------------|----------|-----------|
| Custom TCP rule | TCP | 2222 | Anywhere | 0.0.0.0/0 |

- Click **Create**.

Step 9: Configure a Security Group for the TCP ELB

1. From the **Security Groups** page, click **Create Security Group** to create another security group.
2. For **Security group name**, enter `pcf-tcp-elb-security-group`.
3. For **Description**, enter a description to identify this security group.
4. For **VPC**, select the VPC where you want to deploy this ELB.
5. Click the **Inbound** tab and add the following rule:

| Type | Protocol | Port Range | Source | |
|-----------------|----------|-------------|----------|-----------|
| Custom TCP rule | TCP | 1024 - 1123 | Anywhere | 0.0.0.0/0 |

6. Click **Create**.

Step 10: Configure a Security Group for the Outbound NAT

1. From the **Security Groups** page, click **Create Security Group** to create another security group.
2. For **Security group name**, enter `pcf-nat-security-group`.
3. For **Description**, enter a description to identify this security group.
4. For **VPC**, select the VPC where you want to deploy the Outbound NAT.
5. Click the **Inbound** tab and add a rule to allow all traffic from your VPCs, as the table and image show.

| Type | Protocol | Port Range | Source | |
|-------------|----------|------------|-----------|-------------|
| All traffic | All | All | Custom IP | 10.0.0.0/16 |

6. Click **Create**.

The screenshot shows the AWS Security Groups console. The 'Security group name' is 'OutboundNAT' and the 'Description' is 'OutboundNAT'. The 'VPC' is 'vpc-8ec593eb (10.0.0.0/16) | pcf-vpc'. Under 'Security group rules', the 'Inbound' tab is selected. A rule is added with 'Type' as 'All traffic', 'Protocol' as 'All', 'Port Range' as '0 - 65535', and 'Source' as 'Custom IP' with the value '10.0.0.0/16'.

Step 11: Configure a Security Group for MySQL

Note: If you plan to use an internal database, skip this step. If you are using RDS, you must configure a security group that enables the Ops Manager VM and BOSH Director VM to access the database.

1. From the **Security Groups** page, click **Create Security Group** to create another security group.
2. For **Security group name**, enter `pcf-mysql-security-group`.
3. For **Description**, enter a description to identify this security group.
4. For **VPC**, select the VPC where you want to deploy MySQL.
5. Click the **Inbound** tab. Add a rule of type `MySQL` and specify the subnet of your VPC in **Source**, as the table and image show.

| Type | Protocol | Port Range | Source | |
|-------|----------|------------|-----------|-------------|
| MySQL | TCP | 3306 | Custom IP | 10.0.0.0/16 |

- Click the **Outbound** tab. Add a rule of type **All traffic** and specify the subnet of your VPC in **Destination**, as the table and image show.

| Type | Protocol | Port Range | Destination | |
|-------------|----------|------------|-------------|-------------|
| All traffic | All | All | Custom IP | 10.0.0.0/16 |

- Click **Create**.

Step 12: Launch an Ops Manager AMI

To launch an Amazon Machine Image (AMI) for Ops Manager, do the following:

- Navigate to the **Pivotal Cloud Foundry Operations Manager** section of [Pivotal Network](#).
- Select the version of PCF you want to install from the **Releases** dropdown.
- In the **Release Download Files**, click the file named **Pivotal Cloud Foundry Ops Manager for AWS** to download a PDF.
- Open the PDF and identify the AMI ID for your region.
- Return to the EC2 Dashboard.
- Click **AMIs** from the **Images** menu.
- Select **Public images** from the drop-down filter that says **Owned by me**.
- Paste the AMI ID for your region into the search bar and press enter.

Note: There is a different AMI for each region. If you cannot locate the AMI for your region, verify that you have set your AWS Management Console to your desired region. If you still cannot locate the AMI, log in to the [Pivotal Network](#) and file a support ticket.

- (Optional) If you want to encrypt the VM that runs Ops Manager with AWS Key Management Service (KMS), perform the following additional steps:
 - Right click the row that lists your AMI and click **Copy AMI**.
 - Select your **Destination region**.
 - Enable **Encryption**. For more information about AMI encryption, see [Encryption and AMI Copy](#) from the *Copying an AMI* topic in the AWS documentation.
 - Select your **Master Key**. To create a new custom key, see [Creating Keys](#) in the AWS documentation.
 - Click **Copy AMI**. You can use the new AMI you copied for the following steps.
- Select the row that lists your Ops Manager AMI and click **Launch**.
- Choose **m3.large** for your instance type and click **Next: Configure Instance Details**.

| | Family | Type | vCPUs | Memory (GiB) | Instance Storage (GiB) |
|----------------------------------|-----------------|--------------------------------|-------|--------------|------------------------|
| <input type="checkbox"/> | Micro instances | t1.micro Free tier eligible | 1 | 0.613 | EBS only |
| <input checked="" type="radio"/> | General purpose | t2.micro Free tier eligible | 1 | 1 | EBS only |
| <input checked="" type="radio"/> | General purpose | t2.small | 1 | 2 | EBS only |
| <input checked="" type="radio"/> | General purpose | t2.medium | 2 | 4 | EBS only |
| <input type="checkbox"/> | General purpose | m3.medium | 1 | 3.75 | 1 x 4 (SSD) |
| <input checked="" type="radio"/> | General purpose | m3.large | 2 | 7.5 | 1 x 32 (SSD) |

12. Configure the following for your instance:

- **Network:** Select the VPC that you created.
- **Subnet:** Select `pcf-public-subnet-az0`.
- **Auto-assign for Public IP:** Select **Enable**.
- **IAM role:** Select the IAM role associated with your pcf-user profile. If you have not created one, click **Create new IAM role** and follow the [Guidelines for Creating User Roles on AWS](#).
- For all other fields, accept the default values.

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances ⓘ

Purchasing option ⓘ ☐ Request Spot Instances

Network ⓘ ⓘ Create new VPC

Subnet ⓘ ⓘ Create new subnet
250 IP Addresses available

Auto-assign Public IP ⓘ

IAM role ⓘ ⓘ Create new IAM role

Shutdown behavior ⓘ

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy ⓘ ⓘ Additional charges will apply for dedicated tenancy.

13. Click **Next: Add Storage** and adjust the **Size (GiB)** value. The default persistent disk value is 50 GB. Pivotal recommends increasing this value to a minimum of 100 GB.

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

| Type | Device | Snapshot | Size (GiB) | Volume Type | IOPS | Delete on Termination | Encrypted |
|------------------|-----------|---------------|----------------------------------|-----------------------|------------|-------------------------------------|---------------|
| Root | /dev/sda1 | snap-f1ce6d7e | <input type="text" value="100"/> | General Purpose (SSD) | 150 / 3000 | <input checked="" type="checkbox"/> | Not Encrypted |
| Instance Store 0 | /dev/sdb | N/A | N/A | N/A | N/A | N/A | Not Encrypted |

14. Click **Next: Tag Instance**

15. On the **Add Tags** page, add a tag with the key `Name` and value `pcf-ops-manager`.

16. Click **Next: Configure Security Group**.

17. Select the `pcf-ops-manager-security-group` that you created in [Step 5: Configure a Security Group for Ops Manager](#).

18. Click **Review and Launch** and confirm the instance launch details.

19. Click **Launch**.
20. Select the `pcf-ops-manager-key` key pair, confirm that you have access to the private key file, and click **Launch Instances**. You use this key pair to access the Ops Manager VM.

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

pcf

☒ I acknowledge that I have access to the selected private key file (pcf.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

21. Click **View Instances** to access the **Instances** page on the EC2 Dashboard.

Step 13: Create Web Load Balancer

1. On the EC2 Dashboard, click **Load Balancers**.
2. Click **Create Load Balancer**.
3. Under **Application Load Balancer**, click **Create**.
4. For **Step 1: Configure Load Balancer**, do the following:
 - a. Under **Basic Configuration**, do the following:
 - For **Name**, enter `pcf-web-elb`.
 - For **Scheme**, select **internet-facing** to allow traffic from public IP addresses, or **internal** to allow traffic only from private IP addresses.
 - For **IP address type**, select the type of IP addresses you want to allow.
 - b. Under **Listeners**, click **Add listener**. For **Load Balancer Protocol**, select **HTTPS**.
 - c. Under **Availability Zones**, select all availability zones.
 - d. Click **Next: Configure Security Settings**.
5. For **Step 2: Configure Security Settings**, do the following:
 - a. Under **Select default certificate**, do one of the following:
 - If you already have a certificate from AWS Certificate Manager (ACM), select **Choose a certificate from ACM**.
 - If you do not have a certificate from ACM, select **Upload a certificate to ACM**. For more information, see [Importing Certificates into AWS Certificate Manager](#) in the AWS documentation.

Note: For a production or production-like environment, use a certificate from a Certificate Authority (CA). This can be an internal certificate or a purchased certificate. For a sandbox environment, you can use a self-signed certificate.

 - b. For **Certificate Name**, select the desired certificate.
 - c. For **Security Policy**, select the policy you created in [Step 3: Create an IAM User for PCF](#).
 - d. Click **Next: Configure Security Groups**.
6. For **Step 3: Configure Security Groups**, do the following:
 - a. Under **Assign a security group**, select **Select an existing security group**.
 - b. From the list of security groups, select the `pcf-web-elb-security-group` security group that you configured in [Step 7: Configure a Security Group for the Web ELB](#).
 - c. Click **Next: Configure Routing**.

7. For **Step 4: Configure Routing**, do the following:

a. Under **Target Group**, enter the following values:

- **Name:** Enter `pcf-web-elb-target-group`.
- **Protocol:** Select **HTTP**.

b. Under **Health checks**, set **Path** to `/health`.

c. Under **Advanced health check settings**, enter the following values:

- **Port:** Set to `8080`.
- **Interval:** Set to `5` seconds.
- **Timeout:** Set to `3` seconds.
- **Unhealthy threshold:** Set to `3`.
- **Health threshold:** Set to `6`.

d. Click **Next: Register Targets**.

8. For **Step 5: Register Targets**, accept the default values and click **Next: Review**.

9. For **Step 6: Review**, review the load balancer details and then click **Create**. A message appears to confirm AWS successfully created the load balancer.

Step 14: Create SSH Load Balancer

1. From the **Load Balancers** page, click **Create Load Balancer**.

2. Select **Classic Load Balancer**.

3. Configure the load balancer with the following information:

- **Load Balancer name:** Enter `pcf-ssh-elb`.
- **Create LB Inside:** Select the `pcf-vpc` VPC that you created in [Step 4: Create a VPC](#).
- Ensure that the **Create an internal load balancer** checkbox is not selected.

1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

Create LB Inside:

Create an internal load balancer: ☐ [\(what's this?\)](#)

Enable advanced VPC configuration: ☒

Listener Configuration:

| Load Balancer Protocol | Load Balancer Port | Instance Protocol | Instance Port |
|------------------------|--------------------|-------------------|---------------|
| HTTP | 80 | HTTP | 80 |

[Add](#)

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC `vpc-e2210d87 (10.0.0.0/16) | pcf-vpc`

Please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

Available Subnets

| Actions | Availability Zone | Subnet ID | Subnet CIDR | Name |
|---------|-------------------|-----------------|-------------|----------------|
| | us-east-1c | subnet-ac5fc2f5 | 10.0.1.0/24 | Private subnet |

Selected Subnets

| Actions | Availability Zone | Subnet ID | Subnet CIDR | Name |
|---------|-------------------|-----------------|-------------|---------------|
| | us-east-1c | subnet-af5fc2f6 | 10.0.0.0/24 | Public subnet |

- Under **Listener Configuration**, add the following rules:

| Load Balancer Protocol | Load Balancer Port | Instance Protocol | Instance Port |
|------------------------|--------------------|-------------------|---------------|
| TCP | 2222 | TCP | 2222 |

- Under **Select Subnets**, select the public subnets you configured in [Step 4: Create a VPC](#), and click **Next: Assign Security Groups**.
- On the **Assign Security Groups** page, select the security group `pcf-ssh-elb-security-group` you configured in [Step 8: Configure a Security Group for the SSH ELB](#), and click **Next: Configure Security Settings**.

1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time.

Assign a security group: ☐ Create a **new** security group
☒ Select an **existing** security group

Filter `VPC security groups`

| Security Group ID | Name | Description | Actions |
|---|-----------------------|----------------------------|-----------------------------|
| <input type="checkbox"/> sg-41693b25 | default | default VPC security group | Copy to new |
| <input type="checkbox"/> sg-f6c29092 | MySQL | MySQL | Copy to new |
| <input type="checkbox"/> sg-10dd8f74 | OpsManager | OpsManager | Copy to new |
| <input type="checkbox"/> sg-3ec2905a | OutboundNAT | OutboundNAT | Copy to new |
| <input type="checkbox"/> sg-88dd8fec | PCF VMs | PCF VMs | Copy to new |
| <input checked="" type="checkbox"/> sg-48c2902c | PCF_ELB_SecurityGroup | PCF_ELB_SecurityGroup | Copy to new |

- On the **Configure Security Settings** page, ignore the **Improve your load balancer's security** error message and click **Next: Configure Health Check**.
- On the **Configure Health Check** page, enter the following values:
 - Ping Protocol:** Select `TCP`.
 - Ping Port:** Set to `2222`.
 - Interval:** Set to `5` seconds.
 - Response Timeout:** Set to `3` seconds.
 - Unhealthy threshold:** Set to `3`.
 - Health threshold:** Set to `6`.

- Click **Next: Add EC2 Instances**.

1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol `TCP`

Ping Port `80`

Advanced Details

| | | |
|--------------------------------|-----------------|---------|
| Response Timeout ⓘ | <code>5</code> | seconds |
| Health Check Interval ⓘ | <code>10</code> | seconds |
| Unhealthy Threshold ⓘ | <code>2</code> | |
| Healthy Threshold ⓘ | <code>10</code> | |

- Accept the defaults on the **Add EC2 Instances** page and click **Next: Add Tags**.
- Accept the defaults on the **Add Tags** page and click **Review and Create**.
- Review and confirm the load balancer details, and click **Create**.

Step 15: Create TCP Load Balancer

1. From the **Load Balancers** page, click **Create Load Balancer**.
2. Select **Classic Load Balancer**.
3. Configure the load balancer with the following information:
 - **Load Balancer name:** Enter `pcf-tcp-elb`.
 - **Create LB Inside:** Select the `pcf-vpc` VPC that you created in [Step 4: Create a VPC](#).
 - Ensure that the **Create an internal load balancer** checkbox is not selected.

1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

Create LB Inside:

Create an internal load balancer: ☐ (what's this?)

Enable advanced VPC configuration: ☒

Listener Configuration:

| Load Balancer Protocol | Load Balancer Port | Instance Protocol | Instance Port |
|------------------------|--------------------|-------------------|---------------|
| HTTP | 80 | HTTP | 80 |

Add

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-e2210d87 (10.0.0.0/16) | pcf-vpc

Please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

Available Subnets

| Actions | Availability Zone | Subnet ID | Subnet CIDR | Name |
|---------|-------------------|-----------------|-------------|----------------|
| + | us-east-1c | subnet-ac5fc2f5 | 10.0.1.0/24 | Private subnet |

Selected Subnets

| Actions | Availability Zone | Subnet ID | Subnet CIDR | Name |
|---------|-------------------|-----------------|-------------|---------------|
| - | us-east-1c | subnet-af5fc2f6 | 10.0.0.0/24 | Public subnet |

4. Under **Listener Configuration**, add the following rules:

| Load Balancer Protocol | Load Balancer Port | Instance Protocol | Instance Port |
|------------------------|--------------------|-------------------|---------------|
| TCP | 1024 | TCP | 1024 |
| TCP | 1025 | TCP | 1025 |
| TCP | 1026 | TCP | 1026 |
| ... | ... | ... | ... |
| TCP | 1123 | TCP | 1123 |

The `...` entry above indicates that you must add listening rules for each port between 1026 and 1123.

5. Under **Select Subnets**, select the public subnets you configured in [Step 4: Create a VPC](#), and click **Next: Assign Security Groups**.
6. On the **Assign Security Groups** page, select the security group `pcf-tcp-elb-security-group` you configured in [Step 9: Configure a Security Group for the TCP ELB](#), and click **Next: Configure Security Settings**.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Filter **VPC security groups**

| Security Group ID | Name | Description | Actions |
|---|-----------------------|----------------------------|-----------------------------|
| <input type="checkbox"/> sg-41693b25 | default | default VPC security group | Copy to new |
| <input type="checkbox"/> sg-f6c29092 | MySQL | MySQL | Copy to new |
| <input type="checkbox"/> sg-10dd8f74 | OpsManager | OpsManager | Copy to new |
| <input type="checkbox"/> sg-3ec2905a | OutboundNAT | OutboundNAT | Copy to new |
| <input type="checkbox"/> sg-88dd8fec | PCF VMs | PCF VMs | Copy to new |
| <input checked="" type="checkbox"/> sg-48c2902c | PCF_ELB_SecurityGroup | PCF_ELB_SecurityGroup | Copy to new |

7. On the **Configure Security Settings** page, ignore the **Improve your load balancer's security** error message and click **Next: Configure Health Check**.

8. On the **Configure Health Check** page, enter the following values:

- o **Ping Protocol:** Select **TCP**.
- o **Ping Port:** Set to **80**.
- o **Interval:** Set to **5** seconds.
- o **Response Timeout:** Set to **3** seconds.
- o **Unhealthy threshold:** Set to **3**.
- o **Health threshold:** Set to **6**.

9. Click **Next: Add EC2 Instances**.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol **TCP**

Ping Port **80**

Advanced Details

Response Timeout **5** seconds

Health Check Interval **10** seconds

Unhealthy Threshold **2**

Healthy Threshold **10**

10. Accept the defaults on the **Add EC2 Instances** page and click **Next: Add Tags**.

11. Accept the defaults on the **Add Tags** page and click **Review and Create**.

12. Review and confirm the load balancer details, and click **Create**.

Step 16: Configure DNS Records

- Perform the following steps for all three of the load balancers you created in previous steps, named **pcf-web-elb**, **pcf-ssh-elb**, and **pcf-tcp-elb**:
 - From the **Load Balancers** page, select the load balancer.
 - On the **Description** tab, locate the **Basic Configuration** section and record the **DNS name** of the load balancer.
- Click **Instances** on the left navigation to view your EC2 instances.
- Select the **PcfOpsManInstance** instance created by Cloudformation.
- On the **Description** tab, record the value for **IPv4 Public IP**.

5. Navigate to your DNS provider and create the following CNAME and A records:

- o CNAME: `*.apps.YOUR-SYSTEM-DOMAIN.com` and `*.system.YOUR-SYSTEM-DOMAIN.com` points to the DNS name of the `pcf-web-elb` load balancer.
- o CNAME: `ssh.YOUR-SYSTEM-DOMAIN.com` points to the DNS name of the `pcf-ssh-elb` load balancer.
- o CNAME: `tcp.YOUR-SYSTEM-DOMAIN.com` points to the DNS name of the `pcf-tcp-elb` load balancer.
- o A: `pcf.YOUR-SYSTEM-DOMAIN.com` points to the public IP address of the `pcf-ops-manager` EC2 instance.

Step 17: Secure the NAT Instance

1. On the EC2 Dashboard, click **Instances**.
2. Select the NAT instance, which has an instance type of `t2.medium`.
3. From the **Actions** menu, select **Networking>Change Security Groups**.
4. Change the NAT security group from the default group to the `pcf-nat-security-group` NAT security group that you created in [Step 10: Configure a](#)

Change Security Groups

Instance ID: i-be6cbb69
Interface ID: eni-9e3bdfb2

Select Security Group(s) to associate with your instance

| Security Group ID | Name | Description |
|---|-----------------------|----------------------------|
| <input type="checkbox"/> sg-04bdda60 | default | default VPC security group |
| <input type="checkbox"/> sg-6d85e209 | ElasticRuntime | ElasticRuntime |
| <input type="checkbox"/> sg-7e80e71a | MySQL | MySQL |
| <input type="checkbox"/> sg-37b8df53 | OpsManager | OpsManager |
| <input checked="" type="checkbox"/> sg-1482e570 | OutboundNAT | OutboundNAT |
| <input type="checkbox"/> sg-0283e466 | PCF_ELB_SecurityGroup | PCF_ELB_SecurityGroup |

[Security Group for the Outbound NAT.](#)

[Cancel](#) [Assign Security Groups](#)

5. Click **Assign Security Groups**.

Step 18: Create RDS Subnet Group

1. Navigate to the RDS Dashboard.
2. Perform the following steps to create a RDS Subnet Group for the two RDS subnets:
 - a. Click **Subnet Groups>Create DB Subnet Group**.
 - b. Enter the following values:
 - **Name:** Enter `pcf-rds-subnet-group`.
 - **Description:** Enter a description to identify this subnet group.
 - **VPC ID:** Select `pcf-vpc`.
 - **Availability Zone and Subnet ID:** Choose the AZ and subnet for `pcf-rds-subnet-az0` and click **Add**.
 - c. Repeat the steps above to add `pcf-rds-subnet-az1` and `pcf-rds-subnet-az2` to the group.
 - d. Click **Create**.

The following screenshot shows a completed subnet group.

Create DB Subnet Group

To create a new Subnet Group give it a name, description, and select an existing VPC below. Once you select an existing VPC, you will be able to add subnets related to that VPC.

Name ⓘ

Description ⓘ


VPC ID ⓘ

Add Subnet(s) to this Subnet Group. You may add subnets one at a time below or [add all the subnets](#) related to this VPC. You may make additions/edits after this group is created. A minimum of 2 subnets is required.


Availability Zone ⓘ

Subnet ID ⓘ


| Availability Zone | Subnet ID | CIDR Block | Action |
|-------------------|-----------------|-------------|---------------------------------------|
| us-east-1b | subnet-970765e0 | 10.0.3.0/24 | <input type="button" value="Remove"/> |
| us-east-1a | subnet-119c343a | 10.0.2.0/24 | <input type="button" value="Remove"/> |

 **Note:** On the Subnet Group page, you may need to refresh the page to view the new group.

Step 19: Create a MySQL Database Using AWS RDS

 **Note:** You must have an empty MySQL database when you install or reinstall PCF on AWS.

1. Navigate to the RDS Dashboard.
2. Click **Instances>Launch DB Instance** to launch the wizard.
3. Select **MySQL**.
4. Select the **MySQL** radio button under **Production** to create a database for production environments.
5. Click **Next Step**.
6. Specify the following database details:
 - **DB Instance Class:** Select **db.m3.large - 2 vCPU, 7.5 GiB RAM**.
 - **Multi-AZ Deployment:** Select **Yes**.
 - **Storage Type:** Select **Provisioned IOPS (SSD)**.
 - **Allocated Storage:** Enter **100 GB**.
 - **DB Instance Identifier:** Enter **pcf-ops-manager-director**.
 - Enter a secure **Master Username** and **Master Password**.

 **Note:** Record the username and password. You need these credentials later when configuring the **Director Config** page in the BOSH Director tile.

Specify DB Details

Instance Specifications

DB Engine

mysql

License Model

general-public-license

DB Engine Version

5.6.22

Review the **Known Issues/Limitations** to learn about potential compatibility issues with specific database versions.

DB Instance Class

db.m3.large — 2 vCPU, 7.5 GiB RA

Multi-AZ Deployment

Yes

Storage Type

General Purpose (SSD)

Allocated Storage*

100

GB

Settings

DB Instance Identifier*

pcf-bosh

Master Username*

admin

Master Password*

.....

Confirm Password*

.....

Retype the value you specified for Master Password.

* Required

Cancel

Previous

Next Step

7. Click **Next Step**.

8. On the **Configure Advanced Settings** page, enter the following values:

- **VPC:** Select `pcf-vpc`.
- **Subnet Group:** Select the `pcf-rds-subnet-group` you created in [Step 18: Create RDS Subnet Group](#).
- **Publicly Accessible:** Select **No**.
- **VPC Security Groups:** Select the `pcf-rds-security-group` that you created in [Step 11: Configure a Security Group for MySQL](#).
- **Database Name:** Enter `bosh`.
- Accept the default values for the remaining fields.

Configure Advanced Settings

Network & Security

This instance will be created with the new Certificate Authority rds-ca-2015. If you are using SSL to connect to this instance, you should use the [new certificate bundle](#). Learn more [here](#)

VPC*

pcf-vpc (vpc-e2210d87)

Subnet Group

pcf_rdsgroup

Publicly Accessible

No

Availability Zone

No Preference

VPC Security Group(s)

Create new Security Group

MySQL (VPC)

OpsManager (VPC)

OutboundNAT (VPC)

Database Options

Database Name

bosh

Note: if no database name is specified then no initial MySQL database will be created on the DB Instance.

Database Port

3306

DB Parameter Group

default.mysql5.6

Option Group

default:mysql-5-6

Enable Encryption

No

Backup

Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to detail [here](#).

Backup Retention Period

7 days

Backup Window

No Preference

Maintenance

Auto Minor Version Upgrade

Yes

Maintenance Window

No Preference

* Required

Cancel

Previous

Launch DB Instance

Select to encrypt the given instance. Master key ids and aliases appear in the list after they have been created using the Key Management Service(KMS) console. [Learn More](#).

- Click **Launch DB Instance**. Launching the instance may take several minutes.
- When the instance has launched, proceed to [Configuring BOSH Director on AWS](#) to continue deploying PCF.

Required AWS Objects

This section describes the AWS objects you create in the procedures above in order to deploy PCF.

Use this section to determine the resource requirements of PCF on AWS, or to verify that you created the correct resources after completing the procedures above.

S3 Buckets for Ops Manager and PAS

You must create the following S3 buckets from the S3 Dashboard:

- `pcf-ops-manager-bucket`
- `pcf-buildpacks-bucket`
- `pcf-packages-bucket`
- `pcf-resources-bucket`
- `pcf-droplets-bucket`

These buckets must be empty when you install or reinstall PCF.

See [Step 2: Create S3 Buckets](#).

IAM User for PCF

You must create an IAM user for PCF named `pcf-user` from the Identity and Access Management Dashboard, using the policy document included in the [Pivotal Cloud Foundry for AWS Policy Document](#) [topic](#).

See [Step 3: Create an IAM User for PCF](#).

Key Pair

You must generate a key pair named `pcf-ops-manager-key`. For more information about setting up a key pair, see [Amazon EC2 Key Pairs](#) [in the AWS documentation](#).

VPC (Public and Private Subnets)

You must create a VPC with public and private subnets from the VPC Dashboard.

The following table lists the subnets in CIDR block `10.0.0.0/16`.

| Name | AZ | IPv4 CIDR block |
|--|---|----------------------------|
| <code>pcf-public-subnet-az0</code> | REGION-#a (for example, <code>us-west-2a</code>) | <code>10.0.0.0/24</code> |
| <code>pcf-public-subnet-az1</code> | REGION-#b (for example, <code>us-west-2b</code>) | <code>10.0.1.0/24</code> |
| <code>pcf-public-subnet-az2</code> | REGION-#c (for example, <code>us-west-2c</code>) | <code>10.0.2.0/24</code> |
| <code>pcf-management-subnet-az0</code> | REGION-#a (for example, <code>us-west-2a</code>) | <code>10.0.16.0/28</code> |
| <code>pcf-management-subnet-az1</code> | REGION-#b (for example, <code>us-west-2b</code>) | <code>10.0.16.16/28</code> |
| <code>pcf-management-subnet-az2</code> | REGION-#c (for example, <code>us-west-2c</code>) | <code>10.0.16.32/28</code> |
| <code>pcf-ert-subnet-az0</code> | REGION-#a (for example, <code>us-west-2a</code>) | <code>10.0.4.0/24</code> |
| <code>pcf-ert-subnet-az1</code> | REGION-#b (for example, <code>us-west-2b</code>) | <code>10.0.5.0/24</code> |
| <code>pcf-ert-subnet-az2</code> | REGION-#c (for example, <code>us-west-2c</code>) | <code>10.0.6.0/24</code> |
| <code>pcf-services-subnet-az0</code> | REGION-#a (for example, <code>us-west-2a</code>) | <code>10.0.8.0/24</code> |
| <code>pcf-services-subnet-az1</code> | REGION-#b (for example, <code>us-west-2b</code>) | <code>10.0.9.0/24</code> |
| <code>pcf-services-subnet-az2</code> | REGION-#c (for example, <code>us-west-2c</code>) | <code>10.0.10.0/24</code> |
| <code>pcf-rds-subnet-az0</code> | REGION-#a (for example, <code>us-west-2a</code>) | <code>10.0.12.0/24</code> |
| <code>pcf-rds-subnet-az1</code> | REGION-#b (for example, <code>us-west-2b</code>) | <code>10.0.13.0/24</code> |
| <code>pcf-rds-subnet-az2</code> | REGION-#c (for example, <code>us-west-2c</code>) | <code>10.0.14.0/24</code> |

See [Step 4: Create a VPC](#).

NAT Instance

You must create a NAT instance when creating a VPC. The NAT instance must have the following configuration:

- **Instance type:** `t2.medium`
- **Key pair name:** `pcf-ops-manager-key`
- **Enable DNS hostnames:** Yes
- **Hardware tenancy:** Default

See [Step 4: Create a VPC](#).

You must also assign the NAT instance to the `pcf-nat-security-group`. See [Step 17: Secure the NAT Instance](#).

Security Groups

The following sections describe the security groups you must create from the EC2 Dashboard.

Ops Manager

The Ops Manager Security Group must be named `pcf-ops-manager-security-group` and have the following inbound rules:

| Type | Protocol | Port Range | Source |
|---------------|----------|------------|-------------|
| HTTP | TCP | 80 | My IP |
| HTTPS | TCP | 443 | My IP |
| SSH | TCP | 22 | My IP |
| BOSH Agent | TCP | 6868 | 10.0.0.0/16 |
| BOSH Director | TCP | 25555 | 10.0.0.0/16 |

See [Step 5: Configure a Security Group for Ops Manager](#).

PCF VMs

The PCV VMs Security Group must be named `pcf-vms-security-group` and have the following inbound rule:

| Type | Protocol | Port Range | Source |
|-------------|----------|------------|--------------------------|
| All traffic | All | 0 - 65535 | Custom IP 10.0.0.0/16 |

See [Step 6: Configure a Security Group for PCF VMs](#).

Web ELB

The Web ELB Security Group must be named `pcf-web-elb-security-group` and have the following inbound rules:

| Type | Protocol | Port Range | Source |
|-----------------|----------|------------|-----------------------|
| Custom TCP rule | TCP | 4443 | Anywhere 0.0.0.0/0 |
| HTTP | TCP | 80 | Anywhere 0.0.0.0/0 |
| HTTPS | TCP | 443 | Anywhere 0.0.0.0/0 |

See [Step 7: Configure a Security Group for the Web ELB](#).

SSH ELB

The SSH ELB Security Group must be named `pcf-ssh-elb-security-group` and have the following inbound rule:

| Type | Protocol | Port Range | Source |
|------|----------|------------|--------|
| | | | |

| | | | | |
|-----------------|-----|------|----------|-----------|
| Custom TCP rule | TCP | 2222 | Anywhere | 0.0.0.0/0 |
|-----------------|-----|------|----------|-----------|

The SSH ELB Security Group must have the following outbound rule:

| Type | Protocol | Port Range | Source | |
|-------------|----------|------------|----------|-----------|
| All traffic | All | All | Anywhere | 0.0.0.0/0 |

See [Step 8: Configure a Security Group for the SSH ELB](#).

TCP ELB

The TCP ELB Security Group must be named `pcf-tcp-elb-security-group` and have the following inbound rule:

| Type | Protocol | Port Range | Source | |
|-----------------|----------|-------------|----------|-----------|
| Custom TCP rule | TCP | 1024 - 1123 | Anywhere | 0.0.0.0/0 |

The TCP ELB Security Group must have the following outbound rule:

| Type | Protocol | Port Range | Source | |
|-------------|----------|------------|----------|-----------|
| All traffic | All | All | Anywhere | 0.0.0.0/0 |

See [Step 9: Configure a Security Group for the TCP ELB](#).

Outbound NAT

The Outbound NAT Security Group must be named `pcf-nat-security-group` and have the following inbound rule:

| Type | Protocol | Port Range | Source | |
|-------------|----------|------------|-----------|-------------|
| All traffic | All | All | Custom IP | 10.0.0.0/16 |

See [Step 10: Configure a Security Group for the Outbound NAT](#).

MySQL

The MySQL Security Group must be named `pcf-mysql-security-group` and have the following inbound rules:

| Type | Protocol | Port Range | Source | |
|-------|----------|------------|-----------|-------------|
| MySQL | TCP | 3306 | Custom IP | 10.0.0.0/16 |

The MySQL Security Group must have the following outbound rules:

| Type | Protocol | Port Range | Destination | |
|-------------|----------|------------|-------------|-------------|
| All traffic | All | All | Custom IP | 10.0.0.0/16 |

See [Step 11: Configure a Security Group for MySQL](#).

Ops Manager AMI

You must locate the public Ops Manager AMI using the AMI ID provided by the PDF downloaded when clicking **Pivotal Cloud Foundry Ops Manager for AWS** on Pivotal Network.

See [Step 12: Launch a Pivotal Ops Manager AMI](#).

ELBs

The following sections describe the ELBs you must create from the EC2 Dashboard.

Web ELB

You must create a web ELB with the following configuration:

- **Name:** `pcf-web-elb`
- **LB Inside:** `pcf-vpc`
- **Selected Subnet:** `pcf-public-subnet-az0`, `pcf-public-subnet-az1`, `pcf-public-subnet-az2`
- **Security Group:** `pcf-elb-security-group`
- **Health Check:** TCP Port 8080, Path: `/health`

See [Step 13: Create Web Load Balancer](#).

SSH ELB

- **Name:** `pcf-ssh-elb`
- **LB Inside:** `pcf-vpc`
- **Selected Subnet:** `pcf-public-subnet-az0`, `pcf-public-subnet-az1`, `pcf-public-subnet-az2`
- **Security Group:** `pcf-ssh-security-group`
- **Health Check:** TCP Port 2222

See [Step 14: Create SSH Load Balancer](#).

TCP ELB

- **Name:** `pcf-tcp-elb`
- **LB Inside:** `pcf-vpc`
- **Selected Subnet:** `pcf-public-subnet-az0`, `pcf-public-subnet-az1`, `pcf-public-subnet-az2`
- **Security Group:** `pcf-tcp-security-group`
- **Health Check:** TCP Port 80

See [Step 15: Create TCP Load Balancer](#).

DNS Configuration

You must navigate to your DNS provider and create CNAME and A records for all three of your load balancers.

See [Step 16: Configure DNS Records](#).

RDS Subnet Group

You must create a subnet group for RDS named `pcf-rds-subnet-group` from the RDS Dashboard.

See [Step 18: Create RDS Subnet Group](#).

MySQL Database

You must create a MySQL database from the RDS Dashboard.

See [Step 19: Create a MySQL Database using AWS RDS](#).

Configuring BOSH Director on AWS

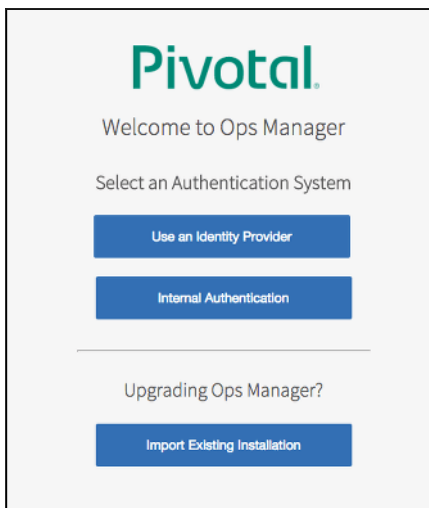
Page last updated:

This topic describes how to configure Ops Manager to deploy Pivotal Cloud Foundry (PCF) on Amazon Web Services (AWS).

Before beginning this procedure, ensure that you have successfully completed all of the steps in the [Installing PCF on AWS Manually](#) topic.

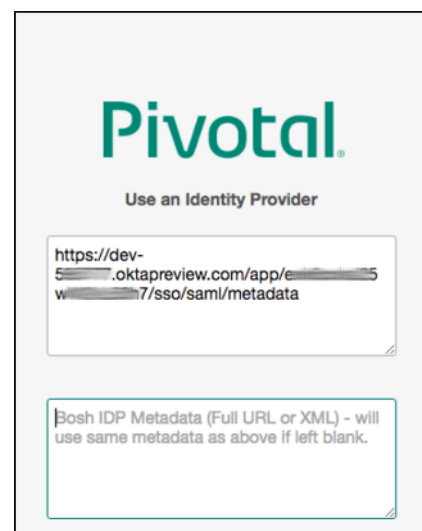
Step 1: Access Ops Manager

1. In a web browser, navigate to the fully qualified domain you created in the [Configure DNS Records](#) step of *Installing PCF on AWS Manually*.
2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you use an Identity Provider, an external identity server maintains your user database.
 - [Internal Authentication](#): If you use Internal Authentication, Ops Manager maintains your user database.



Use an Identity Provider (IdP)

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.




2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.



Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or

URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a 500 error.

 **Note:** These attributes are case-sensitive.


- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.

5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.

6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

 **Note:** To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.

- **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
- **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
- **Name ID:** Email Address
- SAML authentication requests are always signed

8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.

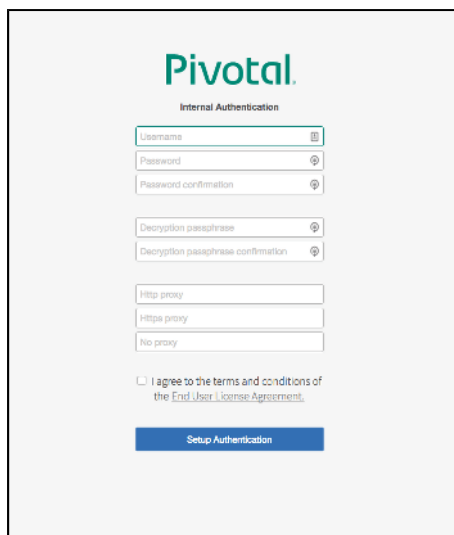
- **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
- **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
- **Name ID:** Email Address
- SAML authentication requests are always signed

9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

Internal Authentication

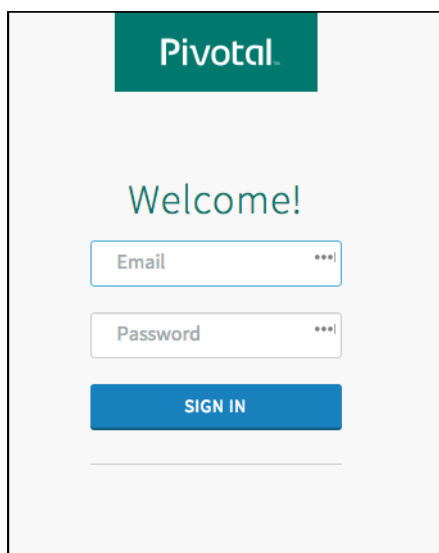
1. When redirected to the **Internal Authentication** page, do the following:

- Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
- Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not recoverable.
- If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in the [Configuring Proxy Settings for the BOSH CPI](#) topic.
- Read the **End User License Agreement**, and select the checkbox to accept the terms.
- Click **Setup Authentication**.



The image shows the 'Internal Authentication' setup page in Pivotal. It features the Pivotal logo at the top. Below the logo, the text 'Internal Authentication' is displayed. The form includes several input fields: 'Username', 'Password', 'Password confirmation', 'Decryption passphrase', and 'Decryption passphrase confirmation'. Each of these fields has a small icon to its right. Below these fields are three radio button options for 'Http proxy', 'Https proxy', and 'No proxy'. At the bottom of the form, there is a checkbox labeled 'I agree to the terms and conditions of the End User License Agreement.' and a blue button labeled 'Setup Authentication'.

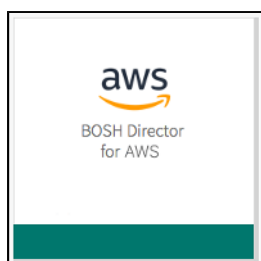
2. Log in to Ops Manager with the Admin username and password you created in the previous step.



The image shows the 'Welcome!' login page in Pivotal. It features the Pivotal logo at the top. Below the logo, the text 'Welcome!' is displayed. The form includes two input fields: 'Email' and 'Password'. Each field has a small icon to its right. Below these fields is a blue button labeled 'SIGN IN'.

Step 2: AWS Config Page

1. Click the **BOSH Director** tile.



2. Select **AWS Config**.

3. Select **Use AWS Keys** or **Use AWS Instance Profile**.

- **Access Key ID** and **AWS Secret Key**: To retrieve your AWS key information, use the AWS Identity and Access Management (IAM) credentials that you generated in the [Step 3: Create an IAM User for PCF](#) section of the *Installing PCF on AWS Manually* topic.
- **AWS IAM Instance Profile**: Enter the name of the IAM profile you created in the [Step 3: Create an IAM User for PCF](#) section of the *Installing PCF on AWS Manually* topic.

4. Complete the rest of the **AWS Management Console Config** page:

- **Security Group ID**: Enter the **Group ID** of the `pcf-vms-security-group` you created for your PCF VMs in the [Step 6: Configure a Security Group for PCF VMs](#) section of the *Installing PCF on AWS Manually* topic. Locate the Group ID in the **Security Groups** tab of your EC2 Dashboard.
- **Key Pair Name**: Enter `pcf-ops-manager-key`.
- **SSH Private Key**: Open the AWS key pair `pcf-ops-manager-keys.pem` file you generated in the [Step 3: Create an IAM User for PCF](#) section of the *Installing PCF on AWS Manually* topic. Copy the contents of the `.pem` file and paste it into the **SSH Private Key** field.
- **Region**: Select the region where you deployed Ops Manager.
- **Encrypt EBS Volumes**: Select this checkbox to enable full encryption on persistent disks of all BOSH-deployed VMs except the Ops Manager VM and Director VM. See the [Configuring Amazon EBS Encryption for PCF on AWS](#) topic for details about using EBS encryption.

Note: Enabling EBS encryption only encrypts Linux VMs. The Windows VMs deployed with Pivotal Application Service (PAS) for Windows or PAS for Windows 2012R2 are not encrypted.

5. Click **Save**.

Step 3: Director Config Page

1. Select **Director Config**.

Director Config

NTP Servers (comma delimited) *

JMX Provider IP Address

Bosh HM Forwarder IP Address

☐ Enable VM Resurrector Plugin

☐ Enable Post Deploy Scripts

☐ Recreate all VMs

This will force BOSH to recreate all VMs on the next deploy. Persistent disk will be preserved

☐ Enable bosh deploy retries

This will attempt to re-deploy a failed deployment up to 5 times.

☐ Keep Unreachable Director VMs

2. Enter at least two of the following NTP servers in the **NTP Servers (comma delimited)** field, separated by a comma:

0.amazon.pool.ntp.org, 1.amazon.pool.ntp.org, 2.amazon.pool.ntp.org, 3.amazon.pool.ntp.org



Note: The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify the value of this field.

3. Leave the **JMX Provider IP Address** field blank.



Note: Starting from PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use PCF JMX Bridge for consuming them outside of the Firehose, you may receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

4. Leave the **Bosh HM Forwarder IP Address** field blank.



Note: Starting from PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use the BOSH HM Forwarder for consuming them, you may receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

5. Select the **Enable VM Resurrector Plugin** checkbox to enable the Ops Manager Resurrector functionality and increase Pivotal Application Service (PAS) availability. For more information, see the [Using Ops Manager Resurrector on VMware vSphere](#) topic.
6. Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.



Note: You must enable post-deploy scripts to install PKS.

7. Select **Recreate all VMs** to force BOSH to recreate all VMs on the next deploy. This process does not destroy any persistent disk data.
8. Select **Enable bosh deploy retries** if you want Ops Manager to retry failed BOSH operations up to five times.
9. (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS secure communications.
10. Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.

11. (Optional) Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.

☒ HM Pager Duty Plugin

Service Key*

HTTP Proxy

- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.

12. (Optional) Select **HM Email Plugin** to enable Health Monitor integration with email.

☒ HM Email Plugin

Host*

Port*

Domain*

From*

Recipients*

Username


Password

☒ Enable TLS

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter your username's password.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

13. For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

 **Note:** After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*


HSM Port Address*

Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**
 9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal
☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature
☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- o **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- o **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.

- **GCS Blobstore:** Select this option to use an external GCS endpoint. To create a GCS bucket, you must have a GCS account. Follow the procedures in [Creating Storage Buckets](#) in the GCS documentation to create a GCS bucket. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Follow the steps in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually* to download a JSON file with a private key. Enter the contents of the JSON file into the field.

15. For **Database Location**, select **External MySQL Database** and complete the following steps:

Database Location

☒ Internal

☐ External MySQL Database

Host*

Port*

Username*

Password*

Database*

- From the AWS Console, navigate to the RDS Dashboard.
- Select **Instances**, then click the arrow to the left of your instance and select the second icon to display the **Details** information.
- Refer to the following table to retrieve the values for the **Director Config** page:

| RDS Instance Field | BOSH Director Field |
|--------------------|--|
| Endpoint | Host |
| Port | Port, which is <code>3306</code> . |
| DB Name | Database, which is <code>bosh</code> . |
| Username | Username |

- For **Password**, enter the password that you defined for your MySQL database when you created in the [Step 19: Create a MySQL Database using AWS RDS](#) section of the *Installing PCF on AWS Manually* topic. In addition, if you selected the **Enable TLS for Director Database** checkbox, you can fill out the following optional fields:
- **Enable TLS:** Selecting this checkbox enables TLS communication between the BOSH Director and the database.

- **TLS CA:** Enter the Certificate Authority for the TLS Certificate.
- **TLS Certificate:** Enter the client certificate for mutual TLS connections to the database.
- **TLS Private Key:** Enter the client private key for mutual TLS connections to the database.
- **Advanced DB Connection Options:** If you would like to provide additional options for the database, use this field to provide a JSON-formatted options string.

- (Optional) **Director Workers** sets the number of workers available to execute Director tasks. This field defaults to 5.
- (Optional) **Max Threads** sets the maximum number of threads that the BOSH Director can run simultaneously. For AWS, the default value is 6. Leave this field blank to use this default value. Pivotal recommends that you use the default value unless doing so results in rate limiting or errors on your IaaS.
- (Optional) To add a custom URL for your BOSH Director, enter a valid hostname in **Director Hostname**. You can also use this field to configure [a load balancer in front of your BOSH Director](#).

Warning: In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, you can cause downtime. Changing the hostname triggers all VMs to be recreated. This issue is resolved in [Ops Manager v2.2.8](#) and later.

- (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.
- (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.

Breaking Change: Do not disable BOSH DNS without consulting Pivotal Support.

- (Optional) To set a custom banner that users see when logging in to the Director using SSH, enter text in the **Custom SSH Banner** field.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

- (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1, hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.
- Click **Save**.

Step 4: Create Availability Zones Page

Note: Pivotal recommends at least three availability zones (AZs) for a highly available installation of PAS. The procedures in [Installing PCF on AWS Manually](#) use 3 AZs.

- Select **Create Availability Zones**.

Create Availability Zones

Availability Zones

Add

▼ us-west-1c

Amazon Availability Zone*

us-west-1c

The Amazon Availability Zone name (ex: 'us-east-1b')

Save

2. To add the three AZs you specified in the [Step 4: Create a VPC](#) section of the *Installing PCF on AWS Manually* topic, do the following:
 - a. Click **Add**.
 - b. For **Amazon Availability Zone**, enter the name of the AZ.
 - c. Repeat until you have entered all three AZs, in the format `REGION-#a`, `REGION-#b`, and `REGION-#c`. For example, `us-west-2a`, `us-west-2b`, and `us-west-2c`.
3. Click **Save**.

Step 5: Create Networks Page

Create Networks

Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future.
Contact Pivotal support for help completing such a change.

Verification Settings

☐ Enable ICMP checks

Networks

One or many IP ranges upon which your products will be deployed

▼ Infrastructure 🗑️

Name*

Add Network

Subnets

Add Subnet

VPC Subnet ID*

CIDR*

Reserved IP Ranges

DNS*

Gateway*

Availability Zones*

☒ us-west-2a

☐ us-west-2b

☐ us-west-2c

1. Select **Create Networks**.
2. (Optional) Select **Enable ICMP checks** to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
3. Perform the following steps to add the network configuration that you created for your VPC in the [Create a VPC](#) section of *Installing PCF on AWS Manually*. Record your VPC CIDR if you set a CIDR other than the recommendation!
 - a. Click **Add Network**.
 - b. For **Name**, enter `infrastructure`.
 - c. Create a subnet for each availability zone by clicking **Add Subnet**. Refer to the table below for the information required to create all three subnets:

| | | |
|--------------|--------------------|--|
| First Subnet | VPC Subnet ID | <code>pcf-infrastructure-subnet-az0</code> |
| | CIDR | <code>10.0.16.0/28</code> |
| | Reserved IP Ranges | <code>10.0.16.0-10.0.16.4</code> |
| | DNS | <code>10.0.0.2</code> * |
| | Gateway | <code>10.0.16.1</code> |
| | Availability Zones | REGION-#a . For example, <code>us-west-2a</code> . |

| | | |
|---------------|--------------------|-------------------------------------|
| Second Subnet | VPC Subnet ID | pcf-infrastructure-subnet-az1 |
| | CIDR | 10.0.16.16/28 |
| | Reserved IP Ranges | 10.0.16.16-10.0.16.20 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.16.17 |
| Third Subnet | Availability Zones | REGION-#b . For example, us-west-2b |
| | VPC Subnet ID | pcf-infrastructure-subnet-az2 |
| | CIDR | 10.0.16.32/28 |
| | Reserved IP Ranges | 10.0.16.32-10.0.16.36 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.16.33 |
| | Availability Zones | REGION-#c . For example, us-west-2c |

* If you set a VPC CIDR other than recommended, enter the second IP in your VPC CIDR. For example, for a 10.0.0.0/24 VPC CIDR, enter 10.0.0.2 in each subnet.

- d. Click **Add Network**.
- e. For **Name**, enter the name of your runtime. For example, pas .
- f. Create a subnet for each availability zone by clicking **Add Subnet**. See the table below for the information required to create all three subnets:

| | | |
|---------------|--------------------|-------------------------------------|
| First Subnet | VPC Subnet ID | pcf-pas-subnet-az0 |
| | CIDR | 10.0.4.0/24 |
| | Reserved IP Ranges | 10.0.4.0-10.0.4.4 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.4.1 |
| | Availability Zones | REGION-#a . For example, us-west-2a |
| Second Subnet | VPC Subnet ID | pcf-pas-subnet-az1 |
| | CIDR | 10.0.5.0/24 |
| | Reserved IP Ranges | 10.0.5.0-10.0.5.4 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.5.1 |
| | Availability Zones | REGION-#b . For example, us-west-2b |
| Third Subnet | VPC Subnet ID | pcf-pas-subnet-az2 |
| | CIDR | 10.0.6.0/24 |
| | Reserved IP Ranges | 10.0.6.0-10.0.6.4 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.6.1 |
| | Availability Zones | REGION-#c . For example, us-west-2c |

* If you set a VPC CIDR other than recommended, enter the second IP in your VPC CIDR. For example, for a 10.0.0.0/24 VPC CIDR, enter 10.0.0.2 in each subnet.


- g. Click **Add Network**.
- h. For **Name**, enter services .
- i. Create a subnet for each availability zone by clicking **Add Subnet**. Refer to the table below for the information required to create all three subnets:


| | | |
|--------------|--------------------|---------------------------------------|
| First Subnet | VPC Subnet ID | pcf-services-subnet-az0 |
| | CIDR | 10.0.8.0/24 |
| | Reserved IP Ranges | 10.0.8.0-10.0.8.3 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.8.1 |
| | Availability Zones | REGION-#a . For example, us-west-2a . |

| | | |
|---------------|--------------------|---------------------------------------|
| Second Subnet | VPC Subnet ID | pcf-services-subnet-az1 |
| | CIDR | 10.0.9.0/24 |
| | Reserved IP Ranges | 10.0.9.0-10.0.9.3 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.9.1 |
| | Availability Zones | REGION-#b . For example, us-west-2b . |
| Third Subnet | VPC Subnet ID | pcf-services-subnet-az2 |
| | CIDR | 10.0.10.0/24 |
| | Reserved IP Ranges | 10.0.10.0-10.0.10.3 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.10.1 |
| | Availability Zones | REGION-#c . For example, us-west-2c . |

* If you set a VPC CIDR other than recommended, enter the second IP in your VPC CIDR. For example, for a 10.0.0.0/24 VPC CIDR, enter 10.0.0.2 in each subnet.

- Click **Save**.

 **Note:** If you are deploying PKS with a PKS workload load balancer, you must tag each AWS subnet with your PKS Kubernetes cluster unique identifier before you create the load balancer. For more information about tagging subnets with a PKS cluster unique identifier, see [AWS Prerequisites](#).

 **Note:** After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

Step 6: Assign AZs and Networks

- Select **Assign AZs and Networks**.

Assign AZs and Networks

The BOSH Director is a single instance.

Choose the availability zone in which to place that instance. It is highly recommended that you backup this VM on a regular basis to preserve settings.

Singleton Availability Zone

AZ-MGMT

Network

infrastructure

Save

- Use the dropdown to select a **Singleton Availability Zone**. The BOSH Director is deployed into this AZ.
- Use the dropdown to select **infrastructure** under **Network**. The BOSH Director is deployed into this network.
- Click **Save**.

Step 7: Security Page

[illegible]

1. Select **Security**.
2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:

```

-----BEGIN CERTIFICATE-----
ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678AB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BCDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABBB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----

```

 Note: If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#) for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 8: Syslog Page

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
 ☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

⌵

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save

- (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
- In the **Address** field, enter the IP address or DNS name for the remote server.
- In the **Port** field, enter the port number that the remote server listens on.
- In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
- (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
 - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
- Click **Save**.

Step 9: Resource Config Page

- Select **Resource Config**.

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|------------------------|--------------|----------------------|---|----------------|-------------------------------------|
| BOSH Director | Automatic: 1 | Automatic: 50 GB | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Master Compilation Job | 1 | None | small (cpu: 1, ram: 2 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |

[Save](#)

- Adjust any values as necessary for your deployment. Under the **Instances**, **Persistent Disk Type**, and **VM Type** fields, choose **Automatic** from the dropdown to allocate the recommended resources for the job. If the **Persistent Disk Type** field reads **None**, the job does not require persistent disk space.

Note: Pivotal recommends provisioning a BOSH Director VM with at least 8 GB memory.

Note: If you set a field to **Automatic** and the recommended resource allocation changes in a future version, Ops Manager automatically uses the new recommended allocation.

Note: If you install PAS for Windows, provision your **Master Compilation Job** with at least 128 GB of disk space.

- (Optional) Enter your AWS target group name in the **Load Balancers** column for each job. Prepend the name with `alb:`. For example, enter `alb:target-group-name`. To create an Application Load Balancer (ALB) and target group, follow the procedures in [Getting Started with Application Load Balancers](#) in the AWS documentation. Then navigate to **Target Groups** in the **EC2 Dashboard** menu to find your target group **Name**.

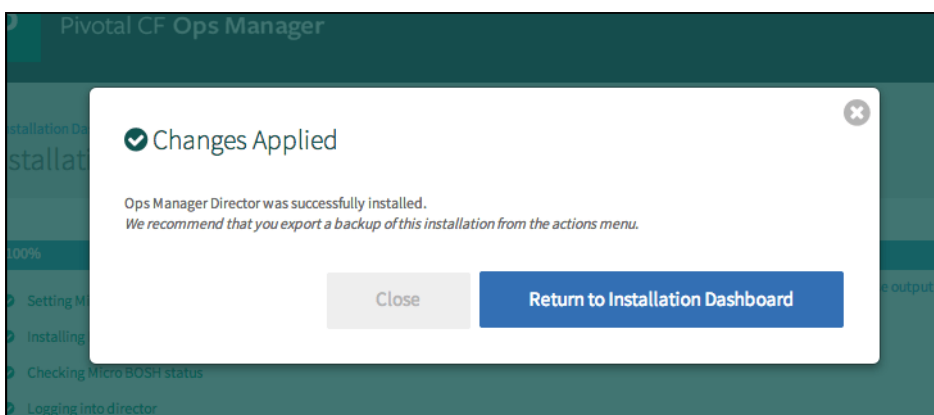
Note: To configure an ALB, you must have the following AWS IAM permissions.

```
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:RegisterTargets"
```

- Click **Save**.

Step 10: Complete the BOSH Director Installation

- Return to the **Installation Dashboard**.
- Click **Apply Changes**.
- BOSH Director begins to install. The **Changes Applied** window displays when the installation process successfully completes.



Next Steps

After completing the procedures in this topic, you must configure a runtime for PCF. You can install PCF on AWS with the Pivotal Application Service (PAS) or Pivotal Container Service (PKS) runtime.

To configure a runtime, do one of the following:

- Configure PAS. See [Deploying PAS on AWS Using Terraform](#).
- Configure PKS. See [Installing PKS on AWS](#) [↗](#).

Deploying PAS on AWS

Page last updated:

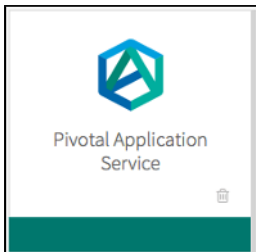
This topic describes how to configure Pivotal Application Service (PAS) components as part of deploying [Pivotal Cloud Foundry](#) (PCF) on Amazon Web Services (AWS).

Before beginning this procedure, ensure that you have successfully completed all steps in the [Installing PCF on AWS Manually](#) and [Configuring BOSH Director on AWS](#).

Note: If you plan to [install the PCF IPsec add-on](#), you must do so before installing any other tiles. Pivotal recommends installing IPsec immediately after Ops Manager, and before installing the PAS Runtime tile.

Step 1: Add PAS to Ops Manager

1. If you have not already downloaded PAS, log in to [Pivotal Network](#), and click on PAS.
2. From the **Releases** dropdown, select the release to install and choose one of the following:
 - a. Click PAS download the PAS `.pivotal` file.
 - b. Click **PCF Small Footprint Runtime** to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).
3. Navigate to the Pivotal Cloud Foundry Operations Manager Installation Dashboard.
4. Click **Import a Product** to add your tile to Ops Manager. For more information, refer to the [Adding and Deleting Products](#) topic.
5. Click the PAS tile in the Installation Dashboard.



Step 2: Assign Availability Zones and Networks

1. Select **Assign AZs and Networks**. These are the Availability Zones that you create when configuring BOSH Director.

AZ and Network Assignments

Place singleton jobs in

☒ us-west-2a
☐ us-west-2b
☐ us-west-2c

Balance other jobs in


☒ us-west-2a
☒ us-west-2b
☒ us-west-2c

Network

docs-exploration-ert-network

Save

2. Select an Availability Zone under **Place singleton jobs**. Ops Manager runs any job with a single instance in this Availability Zone.
3. Select all Availability Zones under **Balance other jobs**. Ops Manager balances instances of jobs with more than one instance across the Availability Zones that you specify.

 **Note:** Pivotal recommends at least three Availability Zones for a highly available installation of PAS.

4. For **Network**, select the `pas` network that you created in the [Step 5: Create Networks Page](#) section of the *Configuring BOSH Director on AWS* topic.
5. Click **Save**.

Step 3: Configure Domains

1. Select **Domains**.

Application Service hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain *

sys.metallicseaweed.cf-app.com

Apps Domain *

apps.metallicseaweed.cf-app.com

Save

2. Enter the system and application domains.
 - The **System Domain** defines your target when you push apps to PAS. This the `system.YOUR-SYSTEM-DOMAIN.com` domain that you created in [Installing PCF on AWS Manually](#).
 - The **Apps Domain** defines where PAS should serve your apps. This the `apps.YOUR-SYSTEM-DOMAIN.com` domain that you created in [Installing PCF on AWS Manually](#).
3. Click **Save**.

Step 4: Configure Networking

1. Select **Networking**.

2. Leave the **Router IPs**, **SSH Proxy IPs**, **HAProxy IPs**, and **TCP Router IPs** fields blank. You do not need to complete these fields when deploying PCF to AWS with Elastic Load Balancers (ELBs).

Note: You specify load balancers in the **Resource Config** section of Pivotal Application Service (PAS) later in the installation process. See the [Configure Router to Elastic Load Balancer](#) section of this topic for more information.

3. Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate and Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.
 - a. Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

Certificates and Private Keys for HAProxy and Router

example-cert

Name *

example-cert

A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

```
-----BEGIN CERTIFICATE-----
MIIE...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```

[Generate RSA Certificate](#)

example-cert-2

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *

```
-----BEGIN CERTIFICATE-----
MIIE...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager.

- b. If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see `Configure Front End` in [Preparing to Deploy Ops Manager on GCP Manually](https://docs.pivotal.io/pcf/om/2-2/gcp/prepare-env-manual.html#config-frontend).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

4. (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Router** field, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

- ☐ TLSv1.0
- ☐ TLSv1.1
- ☒ TLSv1.2

- Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

- ☒ Log client IPs
- ☐ Disable logging of X-Forwarded-For header only
- ☐ Disable logging of both source IP and X-Forwarded-For header
- To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.

- Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.



Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

- ☒ TLS terminated for the first time at infrastructure load balancer
- ☐ TLS terminated for the first time at HAProxy
- ☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|---|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to | TLS terminated for | HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header. |

| | | |
|--|--|---|
| <ul style="list-style-type: none"> the instances of HAProxy, and HAProxy instance count is > 0 | the first time at HAProxy. |  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | TLS terminated for the first time at the Gorouter. | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |


For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).

8. To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

- ☒ HAProxy does not request client certificates.
- ☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.


 **warning:** Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

9. To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*


- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

 **warning:** Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client**

Certificate Validation in the **Networking** pane.

- In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`.


 **Note:** AWS Classic Load Balancers do not support PCF's default cipher suites. See [TLS Cipher Suite Support by AWS Load Balancers](#) for information about configuring your AWS load balancers and Gorouter.

If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.

 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:


`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384` If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format.

Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable

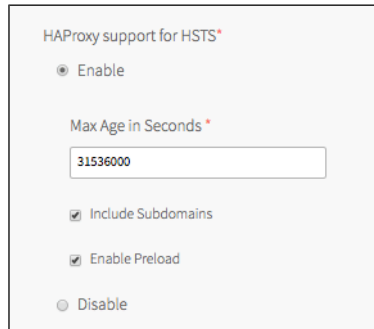
◦ Enable HAProxy forwarding of requests to Router over TLS

| If you want to: | Encrypt communication between HAProxy and the Gorouter |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

◦ Disable HAProxy forwarding of requests to Router over TLS

| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |

13. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field, and complete



HAProxy support for HSTS*

☒ Enable

Max Age in Seconds*

31536000

☒ Include Subdomains


☒ Enable Preload

☐ Disable

the following optional configuration steps:

- (Optional) Enter a **Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
- (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
- (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from HAProxy.

- If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

- (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

- (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
- (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
- (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
- By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#)

- (Optional) By default, Gorouter support for the PROXY protocol is disabled. To enable the PROXY protocol, select **Enable support for PROXY protocol in CF Router**. When enabled, client-side load balancers that terminate TLS but do not support HTTP can pass along information from the originating client. Enabling this option may impact Gorouter performance. For more information about enabling the PROXY protocol in Gorouter, see the *HTTP Header Forwarding* sections in the [Securing Traffic in Cloud Foundry](#) topic.
- In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details. 1. If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
- (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can

determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

500

23. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router*

☒ Enable
 ☐ Disable

24. (Optional) To accommodate larger uploads over connections with high latency, increase the number of seconds in the **Router Timeout to Backends** field.
25. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

26. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
27. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

Load Balancer Healthy Threshold *

28. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

29. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

30. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.

HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.


HAProxy Trusted CIDRs

31. The **Loggregator Port** defaults to if left blank. For AWS environments that are not using an Application Load Balancer, enter .


Container Network Interface Plugin*

 Silk


32. For **Container Network Interface Plugin**, ensure **Silk** is selected and review the following fields:

 **Note:** The **External** option exists to support NSX-T integration for vSphere deployments.

- (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to . Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses .

 **warning:** The overlay network IP range must not conflict with any other IP addresses in your network.

- Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to .
- For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to .
- To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- By default, containers use the same DNS servers as the host. If you want to override the DNS servers to be used in containers, enter a comma-separated list of servers in **DNS Servers**.

 **Note:** If your deployment uses BOSH DNS, which is the default, you cannot use this field to override the DNS servers used in containers.

33. For **DNS Search Domains**, enter DNS search domains as a comma-separated list. Your containers append these search domains to hostnames to resolve them into full domain names.

DNS Search Domains

DNS search domains to be used in containers. A comma-separated list can be specified.

34. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is . You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

35. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:
 - a. Select **Enable TCP Routing**
 - b. For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. If you [configured AWS for PCF manually](#), enter `1024-1123` which corresponds to the rules you created for `pcf-tcp-elb`.
 - To support multiple TCP routes, Pivotal recommends allocating multiple ports.
 - To allocate a list of ports rather than a range:
 1. Enter a single port in the **TCP Routing Ports** field.
 2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.
 - c. For AWS, you also need to specify the name of a TCP ELB in the **LOAD BALANCER** column of TCP Router job of the `Resource Config` screen. You configure this later on in PAS. For more information, see the [Configure Router to Elastic Load Balancer](#) topic.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time

☒ Enable TCP Routing

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

1024-1123

36. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) topic.

37. Click **Save**

Step 5: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC
- ☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888


Docker Images Disk-Cleanup Scheduling on Cell VMs*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) *


10240


- The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.
- The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
- If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
- If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.


- To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting](#) in *HTTP Routing*.

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

 **Warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

7. You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
8. Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
9. Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
10. Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.

 **Note:** In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

11. (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs*

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

12. By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.

13. Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
14. You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is `60` seconds and the maximum configurable timeout is `600` seconds.
15. Click **Save**.

Step 6: Configure Application Developer Controls

1. Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *


Staging Timeout (Seconds) *

☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.
4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.
5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.

 **Note:** If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system

upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of seconds you specify in this field.
9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 7: Review Application Security Groups

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 8: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *

2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.

3. Click **Save**.

Step 9: Configure UAA

1. Select **UAA**.
2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

3. Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN`.

 **Note:** The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN`.

4. If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
M
U
H
M
-----END CERTIFICATE-----

[Change](#)

SAML Service Provider Key Password

Secret

Password.

- (Optional) To override the default value, enter a custom SAML Entity ID in the **SAML Entity ID Override** field. By default, the SAML Entity ID is `http://login.YOUR-SYSTEM-DOMAIN` where `YOUR-SYSTEM-DOMAIN` is set in the **Domains > System Domain** field.
- For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
- (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line Interface (cf CLI) login access and refresh. Most deployments use the defaults.

Apps Manager Access Token Lifetime (in seconds) *

1209600

Apps Manager Refresh Token Lifetime (in seconds) *

1209600

Cloud Foundry CLI Access Token Lifetime (in seconds) *

7200

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

1209600

Global Login Session Max Timeout (in seconds) *

1800

Global Login Session Idle Timeout (in seconds) *

1800

Customize Username Label (on login page) *

Email

Customize Password Label (on login page) *

Password


Proxy IPs Regular Expression *

10\.\d{1,3}\.\d{1,3}\.\d{1,3}|192\.\d{1,3}\.\d{1,3}

[Save](#)

- (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:

- **Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - **Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan
9. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
 10. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Gorouter or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
 11. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#) for help.

Internal Database Configuration


When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane. See the [Configure Internal Databases](#) section for details.

1. Select **Internal MySQL**.

Choose the location of your UAA database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use AWS RDS)

 **Note:** If you configure your system databases as external in the **Databases** pane, selecting Internal MySQL in the **UAA** pane has no effect.

2. Click **Save**.
3. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

1. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)

☒ External (preferred if, for example, you use AWS RDS)

Hostname *


TCP Port *

Username *


Password *

- For **Hostname**, enter the hostname of the database server.
- For **TCP Port**, enter the port of the database server.
- For **User Account and Authentication database username**, specify a unique username that can access this specific database on the database server.
- For **User Account and Authentication database password**, specify a password for the provided username.
- Click **Save**.

Step 10: Configure CredHub

 **Note:** Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

- Select **CredHub**.
- Choose the location of your CredHub database. PAS includes this CredHub database for services to store their service instance credentials.

 **Note:** You cannot choose **Internal** for the CredHub database if you choose **External** for your System Databases. See [Configure System Databases](#) below.

Configure the CredHub Server

Choose the location of your CredHub database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use Google Cloud SQL)

If you chose **External**, enter the following:

- Hostname.** This is the IP address of your database server.
- TCP Port.** This is the port of your database server, such as `3306`.
- Username.** This is a unique username that can access your CredHub database on the database server.
- Password.** This is the password for the provided username.
- Database CA Certificate.** This certificate is used when encrypting traffic to and from the database.

- Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys

▼

Name *

Provider*

Internal

▲

▼

Key *


Secret

🔒

☐ Primary

Name of the encryption key.

- **Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- **Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- **Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- **Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.

 **Note:** For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

4. (Optional) To configure CredHub to use an HSM, complete the following fields:

- **HSM Provider Partition.** This is the name of the HSM provider partition.
- **HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- **HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#) [↗](#) in the

HSM Provider Partition

HSM Provider Partition Password

Secret

HSM Provider Client Certificate

Certificate PEM

Private Key PEM

Generate RSA Certificate


Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

- If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.
- Click **Save**.
- Select the **Resource Config** pane.
- Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.
- Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).


Step 11: Configure System Databases You can configure PAS to use an internal MySQL database provided with PCF, or you can configure an external database provider for the databases required by PAS.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration

If you want to use internal databases for your deployment, perform the following steps:

- Select **Databases**.
- Select one of the **Internal Databases** options:
 - **Internal Databases - MySQL - Percona XtraDB Cluster** uses [Percona Server](#) with TLS encryption between server cluster nodes.
 - **Internal Databases - MySQL - MariaDB Galera Cluster** uses [MariaDB](#) with cluster nodes communicating over plaintext.

 **warning:** Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

3. Click **Save**.

Then proceed to [Step 12: (Optional) Configure Internal MySQL](#internal-mysql) to configure high availability for your internal MySQL databases. ###
Create External System Databases

⚠ warning: Protect whichever database you use in your deployment with a password.

To create your Pivotal Application Service (PAS) databases, follow the procedure below.

💡 Note: Exact configurations depend on your database provider. The following procedure uses AWS RDS as an example.

1. Add the `ubuntu` account key pair from your IaaS deployment to your local SSH profile so you can access the Ops Manager VM. For example, in AWS, you add a key pair created in AWS:

```
$ ssh-add aws-keypair.pem
```

2. SSH in to your Ops Manager using the Ops Manager FQDN and the username `ubuntu`:

```
$ ssh ubuntu@OPS-MANAGER-FQDN
```

3. Log in to your MySQL database instance using the appropriate hostname and user login values configured in your IaaS account. For example, to log in to your AWS RDS instance, run the following MySQL command:

```
$ mysql --host=RDSHOSTNAME --user=RDSUSERNAME --password=RDSPASSWORD
```

4. Run the following MySQL commands to create databases for the PAS components that require a relational database:

```
CREATE database cedb;
CREATE database notifications;
CREATE database autoscale;
CREATE database app_usage_service;
CREATE database routing;
CREATE database diego;
CREATE database account;
CREATE database nfsvolume;
CREATE database networkpolicyserver;
CREATE database silk;
CREATE database locket;
CREATE database uaa;
CREATE database credhub;
```

💡 Note: The command `CREATE database credhub;` is optional if you have no CredHub instances. By default, CredHub has `0` instances.

5. Type `exit` to quit the MySQL client, and `exit` again to close your connection to the Ops Manager VM.

6. In PAS, select **Databases**.

7. Select the **External Databases** option.

💡 Note: If you configure databases as external, you cannot configure an internal database in the **UAA** pane.


8. For **Hostname**, enter the hostname of the database server.

9. For **TCP Port**, enter the port of the database server.
10. Each component that requires a relational database has two corresponding fields: one for the database username and one for the database password. For each set of fields, specify a unique username that can access this specific database on the database server and a password for the provided username.

 **Note:** Ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.


11. Click **Save**.

Step 12: (Optional) Configure Internal MySQL

 **Note:** You only need to configure this section if you have selected one of the **Internal Databases - MySQL** options in the **Databases** section.

To use internal MySQL in High Availability configuration, you define a load balancer rule that lets PAS components send queries a single hostname backed by two redundant proxies. Each proxy then directs query traffic to three MySQL server nodes.

1. Allocate an internal load balancer rule to balance traffic between two static IP addresses. The static IP addresses cannot be within the range that that you have reserved for PAS.
The load balancer rule is separate from the software provided by Pivotal, and you need to define it within your infrastructure.
 - **Make your idle time out long enough to not interrupt long-running queries.** When queries take a long time, the load balancer can time out and interrupt the query.
For example, [AWS's Elastic Load Balancer](#) has a default idle timeout of 60 seconds, so queries that take longer than this duration sever the MySQL connection and return an error.
 - **Configure a healthcheck or monitor, using TCP against port 1936.** This defaults to TCP port `1936`, to maintain backwards compatibility with previous releases. This port is not configurable. Unauthenticated healthchecks against port 3306 may cause the service to become unavailable and require manual intervention to fix.
 - **Configure the load balancer to route traffic for TCP port 3306 to the IPs of all proxy instances on TCP port 3306.**
 - Record the hostname of the load balancer rule and the two static IP addresses.

 **warning:** You must configure a load balancer to achieve complete high availability.

2. From the PAS tile in Ops Manager, Select **Internal MySQL**.
3. In the **MySQL Proxy IPs** field, enter the static IP addresses used by the internal MySQL load balancer rule.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.

A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.


The automated backups functionality works with any S3-compatible file store that can receive your backup files.

MySQL Proxy IPs

MySQL Service Hostname

4. For **MySQL Service Hostname**, enter the IP address or hostname for your load balancer. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.
5. In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
6. In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.

7. (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
8. To prohibit the creation of command line history files on the MySQL nodes, disable the **Allow Command History** checkbox.
9. To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

10. For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the default value is 10 seconds.

Replication canary time period *

Replication canary read delay *

E-mail address (required) *

☒ Allow Command History

Cluster Probe Timeout

11. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.
12. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.
 - a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.

Server Activity Logging *

☐ Disable server activity logging
☒ Enable server activity logging

Event types *

Load Balancer Healthy Threshold *

Load Balancer Unhealthy Threshold *

13. Enter values for the following fields:


- **Load Balancer Healthy Threshold:** Specifies the amount of time, in seconds, to wait until declaring the MySQL Proxy instance started. This allows an external load balancer time to register the instance as healthy.
- **Load Balancer Unhealthy Threshold:** Specifies the amount of time, in seconds, that the MySQL Proxy continues to accept connections before shutting down. During this period, the Healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.

14. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.

15. Click **Save**.

For more information on how to monitor the node health of your MySQL Proxy instances, see [Using the MySQL Proxy](#).

Step 13: Configure File Storage

 **Note:** If you followed the instructions in [Installing PCF on AWS Manually](#), you created the necessary resources for [external S3-compatible file storage](#).

To minimize system downtime, Pivotal recommends using highly resilient and redundant *external* filestores for your Pivotal Application Service (PAS) file storage.

When configuring file storage for the Cloud Controller in PAS, you can select one of the following:

- Internal WebDAV filestore
- External S3-compatible or Ceph-compatible filestore
- External Google Cloud Storage with Access Key and Secret Key
- External Google Cloud Storage with Service Account
- External Azure Cloud Storage

For production-level PCF deployments on AWS, Pivotal recommends selecting the **External S3-Compatible File Store**. For more information about production-level PCF deployments on AWS, see the [Reference Architecture for Pivotal Cloud Foundry on AWS](#).

For more factors to consider when selecting file storage, see the [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#) topic.

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External S3 or Ceph Filestore

To use an external S3-compatible filestore for PAS file storage, perform the following steps:

1. In the PAS tile, select **File Storage**.
2. Select the **External S3-Compatible Filestore** option and complete the following fields:
 - Enter the `https://` **URL Endpoint** for your region.
For example, in the **us-west-2** region, enter `https://s3-us-west-2.amazonaws.com/`.
 - If you use an AWS instance profile to manage role information for your filestore, select the **S3 AWS with Instance Profile** checkbox. For more information, see [AWS Identity and Access Management](#) in the AWS documentation.

☒ S3 AWS with Instance Profile

Access Key (required if not using S3 AWS with Instance Profile)

Secret Key (required if not using S3 AWS with Instance Profile)

- Alternatively, enter the **Access Key** and **Secret Key** of the `pcf-user` you created when configuring AWS for PCF. If you select the **S3 AWS with Instance Profile** checkbox and also enter an **Access Key** and **Secret Key**, the instance profile will overrule the Access Key and Secret Key.
- From the **S3 Signature Version** dropdown, select **V4 Signature**. For more information about S4 signatures, see [Signing AWS API Requests](#) in the AWS documentation.
- For **Region**, enter the region in which your S3 buckets are located. `us-west-2` is an example of an acceptable value for this field.
- Select **Server-side Encryption** to encrypt the contents of your S3 filestore. This option is only available for AWS S3.
- (Optional) If you selected **Server-side Encryption**, you can also specify a **KMS Key ID**. PAS uses the KMS key to encrypt files uploaded to the blobstore. If you do not provide a KMS Key ID, PAS uses the default AWS key. For more information, see [Protecting Data Using Server-Side Encryption with AWS KMS-Managed Keys \(SSE-KMS\)](#).
- Enter names for your S3 buckets:

| Ops Manager Field | Value | Description |
|------------------------|-----------------------|---|
| Buildpacks Bucket Name | pcf-buildpacks-bucket | This S3 bucket stores app buildpacks. |
| Droplets Bucket Name | pcf-droplets-bucket | This S3 bucket stores app droplets. Pivotal recommends that you use a unique bucket name for droplets, but you can also use the same name as above. |
| Packages Bucket Name | pcf-packages-bucket | This S3 bucket stores app packages. Pivotal recommends that you use a unique bucket name for packages, but you can also use the same name as above. |
| Resources Bucket Name | pcf-resources-bucket | This S3 bucket stores app resources. Pivotal recommends that you use a unique bucket name for app resources, but you can also use the same name as above. |

- Configure the following depending on whether your S3 buckets have versioning enabled:
 - Versioned S3 buckets:** Enable the **Use versioning for backup and restore** checkbox to archive each bucket to a version.
 - Unversioned S3 buckets:** Disable the **Use versioning for backup and restore** checkbox, and enter a backup bucket name for each active bucket. The backup bucket name must be different from the name of the active bucket it backs up.

☐ Use versioning for backup and restore.
 (All of the above buckets must have versioning enabled and use the V4 S3 Signature Version).

If versioning is not enabled or supported, you can configure separate buckets below for backups. More information at <https://docs.pivotal.io/pivotalcf/2-1/customizing/backup-restore/backup-pcf-bbr.html>.

Backup Region



Backup Buildpacks Bucket Name

Backup Droplets Bucket Name

Backup Packages Bucket Name

For more information about setting up external S3 blobstores, see the [Backup and Restore with External Blobstores](#) topic in the Cloud Foundry documentation.

3. Click **Save**.


 **Note:** For more information regarding AWS S3 Signatures, see the [Authenticating Requests](#)  topic in the AWS documentation.

Other IaaS Storage Options

[Google Cloud Storage](#) and [Azure Storage](#) are also available as file storage options, but are not recommended for typical PCF on AWS installations.

Step 14: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

 **Note:** The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

- ☒ No
☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging


☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration


Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.

 **Note:** The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.

 **Note:** Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 15: (Optional) Customize Apps

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑️
- ▶ Docs 🗑️
- ▶ Tools 🗑️

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

- Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
- Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
- Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
- Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
- The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
- The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 16: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret

Save

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

Note: If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 17: (Optional) Configure App Autoscaler

To use App Autoscaler, you must create an instance of the service and bind it to an app. To create an instance of App Autoscaler and bind it to an app, see [Set Up App Autoscaler](#) in the *Scaling an Application Using App Autoscaler* topic.

- Click **App Autoscaler**.

Configure the App Autoscaler

Autoscaler Instance Count (min: 1) *

Autoscaler API Instance Count (min: 1) *

Metric Collection Interval (min: 60, max: 3600) (min: 60, max: 3600) *

Scaling Interval (min: 15, max: 120) (min: 15, max: 120) *

☐ Verbose Logging

☐ Disable API Connection Pooling

☒ Enable Notifications

Save

- Review the following settings:

- Autoscaler Instance Count:** How many instances of the App Autoscaler service you want to deploy. The default value is `3`. For high availability, set this number to `3` or higher. You should set the instance count to an odd number to avoid split-brain scenarios during leadership elections. Larger environments may require more instances than the default number.
- Autoscaler API Instance Count:** How many instances of the App Autoscaler API you want to deploy. The default value is `1`. Larger environments may require more instances than the default number.
- Metric Collection Interval:** How many seconds of data collection you want App Autoscaler to evaluate when making scaling decisions. The minimum interval is 60 seconds, and the maximum interval is 3600 seconds. The default value is `120`. Increase this number if the metrics you use in your scaling rules are emitted less frequently than the existing Metric Collection Interval.
- Scaling Interval:** How frequently App Autoscaler evaluates an app for scaling. The minimum interval is 15 seconds, and the maximum interval is 120 seconds. The default value is `35`.
- Verbose Logging** (checkbox): Enables verbose logging for App Autoscaler. Verbose logging is disabled by default. Select this checkbox to see more detailed logs. Verbose logs show specific reasons why App Autoscaler scaled the app, including information about minimum and maximum instance limits, App Autoscaler's status. For more information about App Autoscaler logs, see [App Autoscaler Events and Notifications](#).
- Disable API Connection Pooling:** API connection pooling increases performance by reducing the cost associated with establishing new connections. If you do not want to keep connections open for reuse, select this option.

3. Click **Save**.

Step 18: Configure Cloud Controller

1. Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
 ☒ Disable

Save

2. Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

3. CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

4. Click **Save**.

Step 19: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

1. Select **Smoke Tests**.
2. If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

- ☐ Temporary space within the system organization (This is deleted after smoke tests finish.)
- ☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.

Step 20: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

Note: Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.

Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.

Whitelist for non-RFC-1918 Private Networks *

allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.

CF CLI Connection Timeout

15

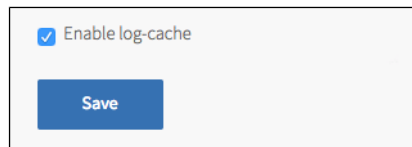
2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PASTopic*.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

⚠ warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 21: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

💡 Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.


- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

💡 Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.

- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.
- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

Step 22: (Optional) Disable Unused Resources

💡 Note: The **Resource Config** pane has fewer VMs if you are installing the [Small Footprint Runtime](#).

 **Note:** The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to instances and scale the **Control** VM to instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by navigating to the **Resource Config** section and using the dropdowns under **Instances** for each job.

By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding system-provided resources in Ops Manager to reduce costs and administrative overhead.

To disable specific VMs in Ops Manager, do the following:

1. Click **Resource Config**.
2. If you configured PAS to use an external S3-compatible filestore, enter in **Instances** in the **File Storage** field.
3. If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:
 - **MySQL Proxy:** Enter in **Instances**.
 - **MySQL Server:** Enter in **Instances**.
 - **MySQL Monitor:** Enter in **Instances**.
4. If you disabled TCP routing, enter **Instances** in the **TCP Router** field.
5. If you are not using HAProxy, enter **Instances** in the **HAProxy** field.
6. Click **Save**.

Step 23: Configure Router to Elastic Load Balancers

1. Record the names of your ELBs. If you followed the procedures in the [Installing PCF on AWS Manually](#) topic, you created the following:
 - `pcf-ssh-elb`: A SSH load balancer. This is a Classic Load Balancer.
 - `pcf-tcp-elb`: A TCP load balancer. This is a Classic Load Balancer.
 - `pcf-web-elb`: A web load balancer. This is an Application Load Balancer.
 - `pcf-web-elb-target-group`: a target group for the web load balancer
2. In the PAS tile, click **Resource Config**.

Resource Config

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|-------------------------------|--------------|----------------------|---|----------------|-------------------------------------|
| Consul | 1 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| NATS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| File Storage | Automatic: 1 | Automatic: 100 GB | Automatic: medium.mem (cpu: 1, ram: 6 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Proxy | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Server | 1 | Automatic: 100 GB | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 64 GB) | | <input checked="" type="checkbox"/> |
| Backup Prepare Node | Automatic: 1 | Automatic: 200 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego BBS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| UAA | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| HAProxy | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Router | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-web-elb | <input checked="" type="checkbox"/> |
| MySQL Monitor | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Clock Global | Automatic: 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller Worker | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego Brain | 1 | Automatic: 1 GB | Automatic: small (cpu: 1, ram: 2 GB, disk: 8 GB) | pcf-ssh-elb | <input checked="" type="checkbox"/> |
| Diego Cell | 1 | None | Automatic: xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB) | | <input checked="" type="checkbox"/> |
| Loggregator Trafficcontroller | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Adapter | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Scheduler | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Doppler Server | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| TCP Router | 0 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-tcp-elb | <input checked="" type="checkbox"/> |
| CredHub | Automatic: 0 | None | Automatic: large (cpu: 2, ram: 8 GB, disk: 16 GB) | | <input checked="" type="checkbox"/> |


Save

3. Enter the name of your SSH load balancer depending on which release you are using.

- **PAS:** In the **Load Balancers** field of the **Diego Brain** row, enter the name of your SSH load balancer: `pcf-ssh-elb`.
- **Small Footprint Runtime:** In the **Load Balancers** field of the **Control** row, enter the name of your SSH load balancer: `pcf-ssh-elb`.

4. In the **Load Balancers** field of the **Router** row, enter the value determined by the type of load balancer you are using:

- **Application Load Balancer:** Enter the name of the target group of your web load balancer, prefixed with `alb:`: `alb:pcf-web-elb-target-group`. The prefix indicates to Ops Manager that you entered the name of a target group, and is required for AWS Application Load Balancers or Network Load Balancers.
- **Classic Load Balancer:** Enter the name of the load balancer: `pcf-web-elb`.

 **Note:** If you are using HAProxy in your deployment, then put the name of the load balancers in the **Load Balancers** field of the **HAProxy** row instead of the **Router** row. For a high availability configuration, scale up the HAProxy job to more than one instance.

5. In the **Load Balancers** field of the **TCP Router** row, enter the name of your TCP load balancer if you enabled TCP routing: `pcf-tcp-elb`.

Step 24: Download Stemcell

This step is only required if your Ops Manager does not already have the stemcell version required by PAS. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

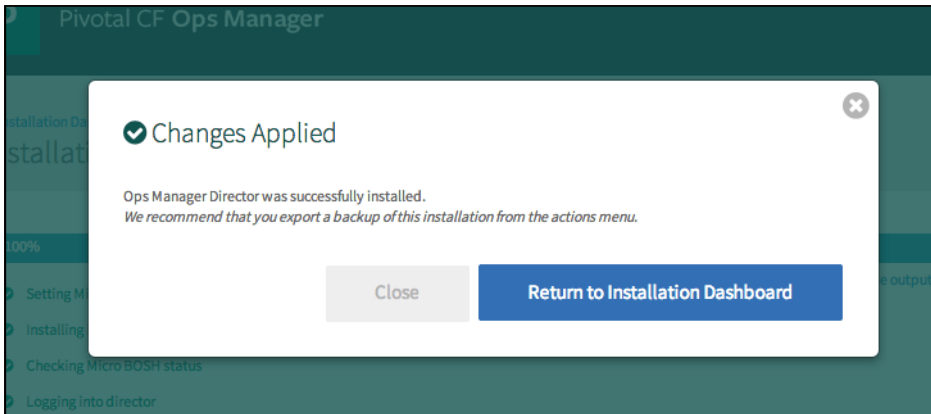
1. Open the [Stemcell product page](#) in the Pivotal Network. *Note, you may have to log in.*
2. Download the appropriate stemcell version targeted for your IaaS.
3. Navigate to **Stemcell Library** in the **Installation Dashboard**.
4. Click **Import Stemcell** to import the downloaded stemcell `.tgz` file.
5. When prompted, enable the Ops Manager product checkbox to stage your stemcell.

6. Click **Apply Stemcell to Products**.

Step 25: Complete the PAS Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes** to begin your installation of PAS.

The install process generally requires a minimum of 90 minutes to complete. The image shows the **Changes Applied** window that displays when the installation process successfully completes.



Installing PCF on AWS using Terraform

This topic explains how to install PCF on AWS using Terraform.

Overview

You can install PCF on AWS with either the Pivotal Application Service (PAS) or Pivotal Container Service (PKS) runtime.

To install PCF on AWS using Terraform, do one of the following:

- Install with PAS. See [Install with PAS Using Terraform](#).
- Install with PKS. See [Install with PKS Using Terraform](#).

Install with PAS Using Terraform

To install with PAS using Terraform, do the following:

1. Deploy Ops Manager. See [Deploying Ops Manager on AWS Using Terraform](#).
2. Configure BOSH Director. See [Configuring BOSH Director on AWS Using Terraform](#).
3. Configure PAS. See [Deploying PAS on AWS Using Terraform](#).

Install with PKS Using Terraform

To install with PKS using Terraform, do the following:

1. Deploy Ops Manager. See [Deploying Ops Manager on AWS Using Terraform](#).
2. Configure BOSH Director. See [Configuring BOSH Director on AWS Using Terraform](#).
3. Configure PKS. See [Installing PKS on AWS](#) ↗.

Deploying Ops Manager on AWS Using Terraform

Page last updated:

This guide describes the preparation steps required to deploy Ops Manager on Amazon Web Services (AWS) using Terraform templates.

The Terraform template for Ops Manager on AWS describes a set of AWS resources and properties. For more information about how Terraform creates resources in AWS, see the [AWS Provider](#) topic on the Terraform site.

If you are deploying Pivotal Application Service (PAS), you may also find it helpful to review different deployment options in the [Reference Architecture for Pivotal Cloud Foundry on AWS](#).

Prerequisites

Before you deploy Ops Manager on AWS, review the following:

- If you intend to install PAS, see [PCF on AWS Requirements](#).
- If you intend to install Pivotal Container Service (PKS), see [AWS Prerequisites and Resource Requirements](#).

In addition to reviewing the prerequisites for your runtime, ensure you have the following:

- The [Terraform CLI](#)
- In your AWS account, ensure you have an IAM user with the following permissions:
 - AmazonEC2FullAccess
 - AmazonRDSFullAccess
 - AmazonRoute53FullAccess
 - AmazonS3FullAccess
 - AmazonVPCFullAccess
 - IAMFullAccess
 - AWSKeyManagementServicePowerUser

Step 1: Download Templates and Edit Variables File

Before you can run Terraform commands to provision infrastructure resources, you must download the AWS Terraform templates and create a Terraform template variables file as described below:

1. On [Pivotal Network](#), navigate to the **Pivotal Application Service (formerly Elastic Runtime)** release.
2. Download the AWS Terraform templates ZIP file.
3. Extract the contents of the ZIP file.
4. Move the extracted folder to the `workspace` directory on your local machine.
5. On the command line, navigate to the directory. For example:

```
$ cd ~/workspace/pivotal-cf-terraforming-aws
```




6. Navigate to the `terraforming-pas` or `terraforming-pks` directory that contains the Terraform files for your runtime.
7. In the runtime directory, create a text file named `terraform.tfvars`.
8. Open the `terraform.tfvars` file and add the following:

```
env_name      = "YOUR-ENVIRONMENT-NAME"
access_key    = "YOUR-ACCESS-KEY"
secret_key    = "YOUR-SECRET-KEY"
region        = "YOUR-AWS-REGION"
availability_zones = ["YOUR-AZ-1", "YOUR-AZ-2", "YOUR-AZ-3"]
ops_manager_ami = "YOUR-OPS-MAN-IMAGE-AMI"
dns_suffix    = "YOUR-DNS-SUFFIX"

ssl_cert = <<SSL_CERT
-----BEGIN CERTIFICATE-----
YOUR-CERTIFICATE
-----END CERTIFICATE-----
SSL_CERT

ssl_private_key = <<SSL_KEY
-----BEGIN EXAMPLE RSA PRIVATE KEY-----
YOUR-PRIVATE-KEY
-----END EXAMPLE RSA PRIVATE KEY-----
SSL_KEY
```

9. Edit the values in the file according to the table below.

| Value to replace | Guidance |
|--|--|
| <code>YOUR-ENVIRONMENT-NAME</code> | <p>Enter a name to use to identify resources in AWS. Terraform prepends the names of the resources it creates with this environment name.</p> <p> Note: You can only enter lowercase alphanumeric characters and hyphens. Examples include <code>pcf</code>, <code>pas</code>, and <code>pks</code>.</p> |
| <code>YOUR-ACCESS-KEY</code> | Enter your AWS Access Key ID of the AWS account in which you want Terraform to create resources. |
| <code>YOUR-SECRET-KEY</code> | Enter your AWS Secret Access Key of the AWS account in which you want Terraform to create resources. |
| <code>YOUR-AWS-REGION</code> | Enter the name of the AWS region in which you want Terraform to create resources. Example: <code>us-central1</code> . |
| <code>YOUR-AZ-1</code> <code>YOUR-AZ-2</code> <code>YOUR-AZ-3</code> | Enter three availability zones from your region. Example: <code>us-central-1a</code> , <code>us-central-1b</code> , <code>us-central-1c</code> . |
| <code>YOUR-OPS-MAN-IMAGE-AMI</code> | <p>Enter the source code for the Ops Manager Amazon Machine Image (AMI) you want to boot. You can find this code in the PDF included with the Ops Manager release on Pivotal Network .</p> <p>If you want to encrypt your Ops Manager VM, create an encrypted AMI copy from the AWS EC2 dashboard and enter the source code for the copied Ops Manager image instead. For more information about copying an AMI, see step 9 of Launch an Ops Manager AMI in the manual AWS configuration topic.</p> <p>To prevent the creation of an Ops Manager VM, set this value to an empty string (<code>" "</code>). When using Platform Automation, you must disable the creation of the Ops Manager VM from Terraform. For more information, see Platform Automation .</p> |
| <code>YOUR-DNS-SUFFIX</code> | Enter a domain name to use as part of the system domain for your deployment. Terraform creates DNS records in AWS using <code>YOUR-ENVIRONMENT-NAME</code> and <code>YOUR-DNS-SUFFIX</code> . For example, if you enter <code>example.com</code> for your DNS suffix and have <code>pcf</code> as your environment name, Terraform will create DNS records at <code>pcf.example.com</code> . |
| <code>YOUR-CERTIFICATE</code> | <p>Enter a certificate to use for HTTP load balancing. For production environments, use a certificate from a Certificate Authority (CA). For test environments, you can use a self-signed certificate.</p> <p>Your certificate must specify your system domain as the common name. Your system domain is <code>YOUR-ENVIRONMENT-NAME.YOUR-DNS-SUFFIX</code>.</p> <p>It also must include the following subdomains: <code>*.sys.YOUR-SYSTEM-DOMAIN</code>, <code>*.login.sys.YOUR-SYSTEM-DOMAIN</code>, <code>*.uaa.sys.YOUR-SYSTEM-DOMAIN</code>, <code>*.apps.YOUR-SYSTEM-DOMAIN</code>.</p> |
| <code>YOUR-PRIVATE-KEY</code> | Enter a private key for the certificate you entered. |

Step 2: Add Optional Variables

Complete this step if you want to do any of the following in PAS:

- Use an AWS Relational Database Service (RDS) for your deployment. For more information, see [Getting started with Amazon RDS](#) in Amazon RDS resources.
- Deploy the Isolation Segment tile.

In your `terraform.tfvars` file, specify the appropriate variables from the sections below.

 **Note:** You can see the configurable options by opening the `variables.tf` file and looking for variables with default values.

Isolation Segments

If you plan to deploy the Isolation Segment tile, add the following variables to your `terraform.tfvars` file, replacing `YOUR-CERTIFICATE` and `YOUR-PRIVATE-KEY` with a certificate and private key. This causes terraform to create an additional HTTP load balancer across three availability zones to use for the Isolation Segment tile.

```
create_isoseg_resources = 1

iso_seg_ssl_cert = <<ISO_SEG_SSL_CERT
-----BEGIN CERTIFICATE-----
YOUR-CERTIFICATE
-----END CERTIFICATE-----
ISO_SEG_SSL_CERT

iso_seg_ssl_cert_private_key = <<ISO_SEG_SSL_KEY
-----BEGIN EXAMPLE RSA PRIVATE KEY-----
YOUR-PRIVATE-KEY
-----END EXAMPLE RSA PRIVATE KEY-----
ISO_SEG_SSL_KEY
```

RDS

1. If you want to use an RDS for Ops Manager and PAS, add the following to your `terraform.tfvars` file:

```
rds_instance_count = 1
```

2. If you want to specify a username for RDS authentication, add the following variable to your `terraform.tfvars` file.

```
rds_db_username = "your-database-name"
```

Step 3: Create AWS Resources with Terraform

Follow these steps to use the Terraform CLI to create resources on AWS:

1. From the directory that contains the Terraform files, run `terraform init` to initialize the directory based on the information you specified in the `terraform.tfvars` file.

```
terraform init
```

1. Run `terraform plan -out=plan` to create the execution plan for Terraform.

```
terraform plan -out=plan
```

1. Run `terraform apply plan` to execute the plan from the previous step. It may take several minutes for Terraform to create all the resources in AWS.

```
terraform apply plan
```

Step 4: Create DNS Record

1. In a browser, navigate to the DNS provider for the DNS suffix you entered in your `terraform.tfvars` file.
2. Create a new NS record for your system domain. Your system domain is `YOUR-ENVIRONMENT-NAME.YOUR-DNS-SUFFIX`.
3. In this record, enter the name servers included in `env_dns_zone_name_servers` from your Terraform output.


What to Do Next

Proceed to the next step in the deployment, [Configuring BOSH Director on AWS Using Terraform](#).

Configuring BOSH Director on AWS Using Terraform

Page last updated:

This topic describes how to configure the BOSH Director tile in Ops Manager on Amazon Web Services (AWS) after [Deploying Ops Manager on AWS Using Terraform](#).

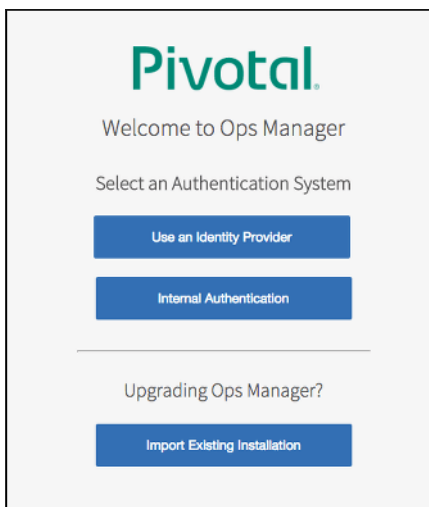
 **Note:** You can also perform the procedures in this topic using the Ops Manager API. For more information, see the [Using the Ops Manager API](#) topic.

Prerequisites

To complete the procedures in this topic, you must have access to the output from when you ran `terraform apply` to create resources for this deployment. You can view this output at any time by running `terraform output`. You use the values in your Terraform output to configure the BOSH Director tile.

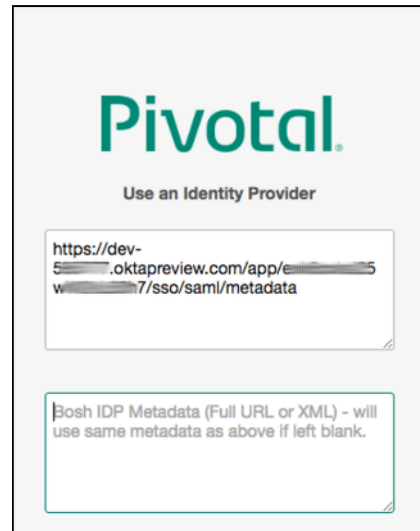
Step 1: Access Ops Manager

1. In a web browser, navigate to the fully qualified domain name (FQDN) of Ops Manager. Use the `ops_manager_dns` value from running `terraform output`.
2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you use an Identity Provider, an external identity server maintains your user database.
 - [Internal Authentication](#): If you use Internal Authentication, Ops Manager maintains your user database.



Use an Identity Provider (IdP)

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.



2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.

Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a `500` error.

Note: These attributes are case-sensitive.

- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.

5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.

6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

Note: To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.

- **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
- **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
- **Name ID:** Email Address
- SAML authentication requests are always signed

8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.

- **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
- **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
- **Name ID:** Email Address
- SAML authentication requests are always signed

9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

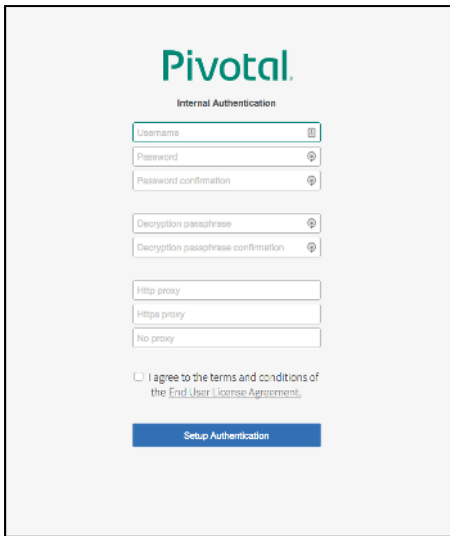
Internal Authentication

1. When redirected to the **Internal Authentication** page, you must complete the following steps:

- Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
- Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not

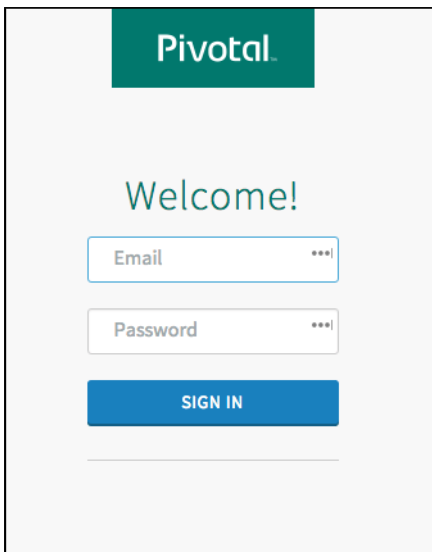
recoverable if lost.

- If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in the [Configuring Proxy Settings for the BOSH CPI](#) topic.
- Read the **End User License Agreement**, and select the checkbox to accept the terms.
- Click **Setup Authentication**.



The image shows the 'Internal Authentication' setup page in Pivotal. At the top is the Pivotal logo. Below it, the title 'Internal Authentication' is centered. The form contains several input fields: 'Username', 'Password', 'Password confirmation', 'Decryption passphrase', and 'Decryption passphrase confirmation'. Each of these fields has a small icon to its right. Below these are three radio button options for 'Http proxy', 'Https proxy', and 'No proxy'. At the bottom, there is a checkbox labeled 'I agree to the terms and conditions of the End User License Agreement' and a blue button labeled 'Setup Authentication'.

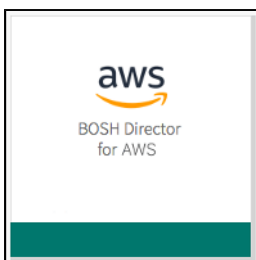
2. Log in to Ops Manager with the Admin username and password that you created in the previous step.



The image shows the Pivotal 'Welcome!' login page. At the top is the Pivotal logo. Below it, the word 'Welcome!' is displayed in a large, teal font. Underneath are two input fields: 'Email' and 'Password', both with masked characters (***). Below the password field is a blue button labeled 'SIGN IN'. At the bottom of the page, there is a thin horizontal line.

Step 2: AWS Config Page

1. Click the **BOSH Director** tile.



2. Select **AWS Config** to open the **AWS Management Console Config** page.

3. Select **Use AWS Keys** or **Use AWS Instance Profile**.

- If you choose to use AWS keys, complete the following fields:
 - **Access Key ID:** Enter the value of `ops_manager_iam_user_access_key` from the Terraform output.
 - **AWS Secret Key:** Enter the value of `ops_manager_iam_user_secret_key` from the Terraform output.
- If you choose to use an AWS instance profile, enter the name of your AWS Identity and Access Management (IAM) profile or enter the value of `ops_manager_iam_instance_profile_name` from the Terraform output.

4. Complete the remainder of the **AWS Management Console Config** page with the following information.

- **Security Group ID:** Enter the value of `vms_security_group_id` from the Terraform output.
- **Key Pair Name:** Enter the value of `ops_manager_ssh_public_key_name` from the Terraform output.
- **SSH Private Key:** Run `terraform output` to view the value of `ops_manager_ssh_private_key` and enter it into this field. `ops_manager_ssh_private_key` is a sensitive value and does not display when you run `terraform apply`.
- **Region:** Select the region where you deployed Ops Manager.
- **Encrypt EBS Volumes:** Select this checkbox to enable full encryption on persistent disks of all BOSH-deployed virtual machines (VMs), except for the Ops Manager VM and BOSH Director VM. See the [Configuring Amazon EBS Encryption](#) topic for details about using Elastic Block Store (EBS) encryption.

Note: Enabling EBS encryption only encrypts Linux VMs. The Windows VMs deployed with Pivotal Application Service for Windows (PASW) are not encrypted.

- **Custom Encryption Key (Optional)** Once you enable EBS encryption, you may want to specify a custom Key Management Service (KMS) encryption key. If you don't enter a value, your custom encryption key will default to the account key. For more information, see [Configuring Amazon EBS Encryption](#).

5. Click **Save**.

Step 3: Director Config Page

1. Select **Director Config** to open the **Director Config** page.

Director Config

NTP Servers (comma delimited)*

0.amazon.pool.ntp.org, 1.amazon.pool.ntp.org

JMX Provider IP Address

Bosh HM Forwarder IP Address

☐ Enable VM Resurrector Plugin

☐ Enable Post Deploy Scripts

☐ Recreate all VMs

This will force BOSH to recreate all VMs on the next deploy. Persistent disk will be preserved

☐ Enable bosh deploy retries

This will attempt to re-deploy a failed deployment up to 5 times.

☐ Keep Unreachable Director VMs

2. Enter at least two of the following NTP servers in the **NTP Servers (comma delimited)** field, separated by a comma:

0.amazon.pool.ntp.org, 1.amazon.pool.ntp.org, 2.amazon.pool.ntp.org, 3.amazon.pool.ntp.org



Note: The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify the value of this field.

3. Leave the **JMX Provider IP Address** field blank.



Note: Starting in PAS v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use PCF JMX Bridge for consuming them outside of the Firehose, you may receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

4. Leave the **Bosh HM Forwarder IP Address** field blank.



Note: Starting in PAS v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use the BOSH HM Forwarder for consuming them, you may receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

5. Select the **Enable VM Resurrector Plugin** checkbox to enable the Ops Manager Resurrector functionality and increase your runtime availability.
6. Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.



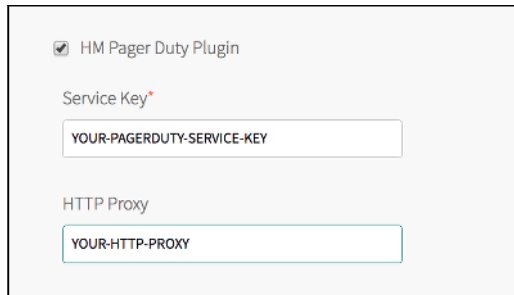
Note: You must enable post-deploy scripts to install PKS.

7. Select **Recreate all VMs** to force BOSH to recreate all VMs on the next deploy. This process does not destroy any persistent disk data.
8. Select **Enable bosh deploy retries** if you want Ops Manager to retry failed BOSH operations up to five times.
9. (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS

secure communications.

10. Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.

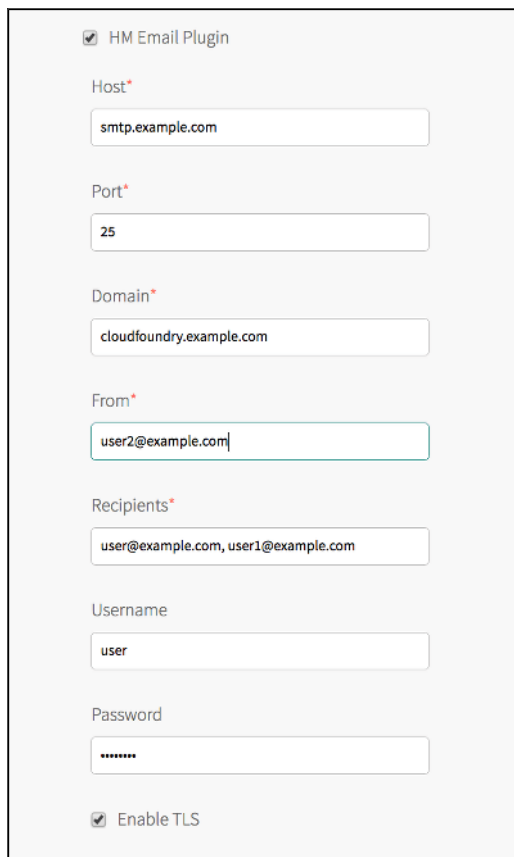
11. Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.



The screenshot shows a configuration form for the 'HM Pager Duty Plugin'. It includes a checked checkbox for the plugin name. Below it, there is a 'Service Key' field with a red asterisk, containing the placeholder text 'YOUR-PAGERDUTY-SERVICE-KEY'. Further down is an 'HTTP Proxy' field containing the placeholder text 'YOUR-HTTP-PROXY'.

- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.

12. Select **HM Email Plugin** to enable Health Monitor integration with email.




The screenshot shows a configuration form for the 'HM Email Plugin'. It includes a checked checkbox for the plugin name. Below it are several fields: 'Host' (smtp.example.com), 'Port' (25), 'Domain' (cloudfoundry.example.com), 'From' (user2@example.com), 'Recipients' (user@example.com, user1@example.com), 'Username' (user), and 'Password' (masked with dots). At the bottom, there is a checked checkbox for 'Enable TLS'.

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma-separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter the password for your email server.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

13. For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

 **Note:** After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*

HSM Port Address*


Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**

9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal

☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature

☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.

- **GCS Blobstore:** Select this option to use an external GCS endpoint. To create a GCS bucket, you must have a GCS account. Follow the procedures in [Creating Storage Buckets](#) in the GCS documentation to create a GCS bucket. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Follow the steps in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually* to download a JSON file with a private key. Enter the contents of the JSON file into the field.


15. For **Database Location**, if you choose to configure an external MySQL database with Amazon Relational Database Service (RDS) or another service, select **External MySQL Database** and complete the fields below. Otherwise, select **Internal**. For more information about creating a RDS MySQL instance, see [Creating a MySQL DB Instance](#) in the AWS documentation.

- **Host:** Enter the value of your host.
- **Port:** Enter your port number. For example, `3306`.
- **Username:** Enter your username.
- **Password:** Enter your password.
- **Database:** Enter your database name.


In addition, if you selected the **Enable TLS for Director Database** checkbox, you can fill out the following optional fields:

- **Enable TLS:** Selecting this checkbox enables TLS communication between the BOSH Director and the database.
- **TLS CA:** Enter the Certificate Authority for the TLS Certificate.
- **TLS Certificate:** Enter the client certificate for mutual TLS connections to the database.
- **TLS Private Key:** Enter the client private key for mutual TLS connections to the database.
- **Advanced DB Connection Options:** If you would like to provide additional options for the database, use this field to provide a JSON-formatted options string.

16. (Optional) **Director Workers** sets the number of workers available to execute Director tasks. This field defaults to `5`.
17. (Optional) **Max Threads** sets the maximum number of threads that the BOSH Director can run simultaneously. Pivotal recommends that you leave the field blank to use the default value, unless doing so results in rate limiting or errors on your IaaS.
18. (Optional) To add a custom URL for your BOSH Director, enter a valid hostname in **Director Hostname**. You can also use this field to configure a load balancer in front of your BOSH Director. For more information, see [How to set up a load balancer in front of BOSH Director](#) in the Pivotal Knowledge Base.

 **warning:** In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, VMs become unavailable. This causes downtime. To restore VM availability, enable **Recreate All VMs** and redeploy. This issue is resolved in [Ops Manager v2.2.8](#) and later.

19. (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.
20. (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.

 **Breaking Change:** Do not disable BOSH DNS without consulting Pivotal Support.



21. (Optional) To set a custom banner that users see when logging in to the Director using SSH, enter text in the **Custom SSH Banner** field.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

22. (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1, hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.

23. Click **Save**.

 **Note:** For more information about AWS S3 Signatures, see the AWS [Authenticating Requests](#)  documentation.

Step 4: Create Availability Zones Page

1. Select **Create Availability Zones**.

Create Availability Zones

Availability Zones

Add

▼ us-west-1c

Amazon Availability Zone*

us-west-1c

The Amazon Availability Zone name (ex: 'us-east-1b')

Save

2. Use the following steps to create three Availability Zones for your apps to use:
 - a. Click **Add** three times.
 - b. For **Amazon Availability Zone**, enter the values corresponding to the key `infrastructure_subnet_availability_zones` from the Terraform output.
 - c. Click **Save**.

Step 5: Create Networks Page

Create Networks

Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future.
Contact Pivotal support for help completing such a change.

Verification Settings

☐ Enable ICMP checks

Networks

One or many IP ranges upon which your products will be deployed

▼ Infrastructure

Name*

Subnets

VPC Subnet ID*

CIDR*

Reserved IP Ranges

DNS*

Gateway*

Availability Zones*

☒ us-west-2a
 ☐ us-west-2b
 ☐ us-west-2c

- Select **Create Networks**.
- (Optional) Select **Enable ICMP checks** to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
- To add the network configuration you created for your VPC, do the following:
 - Click **Add Network**.
 - For **Name**, enter `infrastructure`.
 - Create a subnet for each availability zone by clicking **Add Subnet**. Refer to the table below for the information required to create all three subnets:

| | | |
|--------------|--------------------|---|
| First Subnet | VPC Subnet ID | The first value of <code>infrastructure_subnet_ids</code> from the Terraform output. |
| | CIDR | <code>10.0.16.0/28</code> |
| | Reserved IP Ranges | <code>10.0.16.0-10.0.16.4</code> |
| | DNS | <code>10.0.0.2</code> * |
| | Gateway | <code>10.0.16.1</code> |
| | Availability Zones | The first value of <code>infrastructure_subnet_availability_zones</code> from the Terraform output. |

| | | |
|---------------|--------------------|--|
| Second Subnet | VPC Subnet ID | The second value of <code>infrastructure_subnet_ids</code> from the Terraform output. |
| | CIDR | <code>10.0.16.16/28</code> |
| | Reserved IP Ranges | <code>10.0.16.16–10.0.16.20</code> |
| | DNS | <code>10.0.0.2</code> * |
| | Gateway | <code>10.0.16.17</code> |
| | Availability Zones | The second value of <code>infrastructure_subnet_availability_zones</code> from the Terraform output. |
| Third Subnet | VPC Subnet ID | The third value of <code>infrastructure_subnet_ids</code> from the Terraform output. |
| | CIDR | <code>10.0.16.32/28</code> |
| | Reserved IP Ranges | <code>10.0.16.32–10.0.16.36</code> |
| | DNS | <code>10.0.0.2</code> * |
| | Gateway | <code>10.0.16.33</code> |
| | Availability Zones | The third value of <code>infrastructure_subnet_availability_zones</code> from the Terraform output. |

* If you set a VPC CIDR other than recommended, enter the second IP in your VPC CIDR. For example, for a `10.0.0.0/24` VPC CIDR, enter `10.0.0.2` in each subnet.

- d. Click **Add Network**.
- e. For **Name**, enter the name of your runtime. For example, `pas`.
- f. Create a subnet for each availability zone by clicking **Add Subnet**. Refer to the table below for the information required to create all three subnets:

| | | |
|---------------|--------------------|---|
| First Subnet | VPC Subnet ID | The first value of <code>pas_subnet_ids</code> from the Terraform output. |
| | CIDR | <code>10.0.4.0/24</code> |
| | Reserved IP Ranges | <code>10.0.4.0–10.0.4.4</code> |
| | DNS | <code>10.0.0.2</code> * |
| | Gateway | <code>10.0.4.1</code> |
| | Availability Zones | The first value of <code>pas_subnet_availability_zones</code> from the Terraform output. |
| Second Subnet | VPC Subnet ID | The second value of <code>pas_subnet_ids</code> from the Terraform output. |
| | CIDR | <code>10.0.5.0/24</code> |
| | Reserved IP Ranges | <code>10.0.5.0–10.0.5.4</code> |
| | DNS | <code>10.0.0.2</code> * |
| | Gateway | <code>10.0.5.1</code> |
| | Availability Zones | The second value of <code>pas_subnet_availability_zones</code> from the Terraform output. |
| Third Subnet | VPC Subnet ID | The third value of <code>pas_subnet_ids</code> from the Terraform output. |
| | CIDR | <code>10.0.6.0/24</code> |
| | Reserved IP Ranges | <code>10.0.6.0–10.0.6.4</code> |
| | DNS | <code>10.0.0.2</code> * |
| | Gateway | <code>10.0.6.1</code> |
| | Availability Zones | The third value of <code>pas_subnet_availability_zones</code> from the Terraform output. |

* If you set a VPC CIDR other than recommended, enter the second IP in your VPC CIDR. For example, for a `10.0.0.0/24` VPC CIDR, enter `10.0.0.2` in each subnet.


- g. Click **Add Network**.
- h. For **Name**, enter `services`.
- i. Create a subnet for each availability zone by clicking **Add Subnet**. Refer to the table below for the information required to create all three subnets:


| | | |
|-------|--------------------|--|
| First | VPC Subnet ID | The first value of <code>services_subnet_ids</code> from the Terraform output. |
| | CIDR | <code>10.0.8.0/24</code> |
| | Reserved IP Ranges | <code>10.0.8.0–10.0.8.3</code> |

| | | |
|---------------|--------------------|--|
| Subnet | DNS | 10.0.0.2 * |
| | Gateway | 10.0.8.1 |
| | Availability Zones | The first value of <code>services_subnet_availability_zones</code> from the Terraform output. |
| Second Subnet | VPC Subnet ID | The second value of <code>services_subnet_ids</code> from the Terraform output. |
| | CIDR | 10.0.9.0/24 |
| | Reserved IP Ranges | 10.0.9.0-10.0.9.3 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.9.1 |
| | Availability Zones | The second value of <code>services_subnet_availability_zones</code> from the Terraform output. |
| Third Subnet | VPC Subnet ID | The third value of <code>services_subnet_ids</code> from the Terraform output. |
| | CIDR | 10.0.10.0/24 |
| | Reserved IP Ranges | 10.0.10.0-10.0.10.3 |
| | DNS | 10.0.0.2 * |
| | Gateway | 10.0.10.1 |
| | Availability Zones | The third value of <code>services_subnet_availability_zones</code> from the Terraform output. |

* If you set a VPC CIDR other than recommended, enter the second IP in your VPC CIDR. For example, for a 10.0.0.0/24 VPC CIDR, enter 10.0.0.2 in each subnet.

- Click **Save**.

 **Note:** If you are deploying PKS with a PKS workload load balancer, you must tag each AWS subnet with your PKS Kubernetes cluster unique identifier before you create the load balancer. For more information about tagging subnets with a PKS cluster unique identifier, see [AWS Prerequisites](#).

 **Note:** After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

Step 6: Assign AZs and Networks Page

- Select **Assign AZs and Networks**.
- Use the dropdown to select a **Singleton Availability Zone**. The BOSH Director installs in this availability zone (AZ).
- Use the dropdown to select the `infrastructure` network for your BOSH Director.
- Click **Save**.

Step 7: Security Page

[illegible]

1. Select **Security**.
2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:

```

-----BEGIN CERTIFICATE-----
ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678AB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDE
FGH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
BCDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDE
FGH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
CDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABBB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDE
FGH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----

```

 Note: If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#) for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 8: Syslog Page

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
 ☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

⌵

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save

- (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
- In the **Address** field, enter the IP address or DNS name for the remote server.
- In the **Port** field, enter the port number that the remote server listens on.
- In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
- (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
 - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
- Click **Save**.

Step 9: Resource Config Page

- Select **Resource Config**.

Resource Config

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|------------------------|--------------|----------------------|--|----------------|-------------------------------------|
| BOSH Director | Automatic: 1 | Automatic: 50 GB | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 50 GB) | | <input checked="" type="checkbox"/> |
| Master Compilation Job | 1 | None | small (cpu: 1, ram: 2 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |

Save

- Adjust any values as necessary for your deployment. Under the **Instances**, **Persistent Disk Type**, and **VM Type** fields, choose **Automatic** from the dropdown to allocate the recommended resources for the job. If the **Persistent Disk Type** field reads **None**, the job does not require persistent disk space.

Note: Pivotal recommends provisioning a BOSH Director VM with at least 8 GB memory.

Note: If you set a field to **Automatic** and the recommended resource allocation changes in a future version, Ops Manager automatically uses the new recommended allocation.

Note: If you install PASW, provision your **Master Compilation Job** with at least 100 GB of disk space.

- (Optional) Enter your AWS target group name in the **Load Balancers** column for each job. Prepend the name with `alb:`. For example, enter `alb:target-group-name`. To create an Application Load Balancer (ALB) and target group, follow the procedures in [Getting Started with Application Load Balancers](#) in the AWS documentation. Then navigate to **Target Groups** in the **EC2 Dashboard** menu to find your target group **Name**.

Note: To configure an ALB, you must have the following AWS IAM permissions.

```
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:RegisterTargets"
```

- Click **Save**.

Step 10: (Optional) Add Custom VM Extensions

Use the Ops Manager API to add custom properties to your VMs such as associated security groups and load balancers. For more information, see [Managing Custom VM Extensions](#).

Step 11: Complete the BOSH Director Installation

- Click the **Installation Dashboard** link to return to the Installation Dashboard.
- Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.

PCF Ops Manager

pivotal-cli

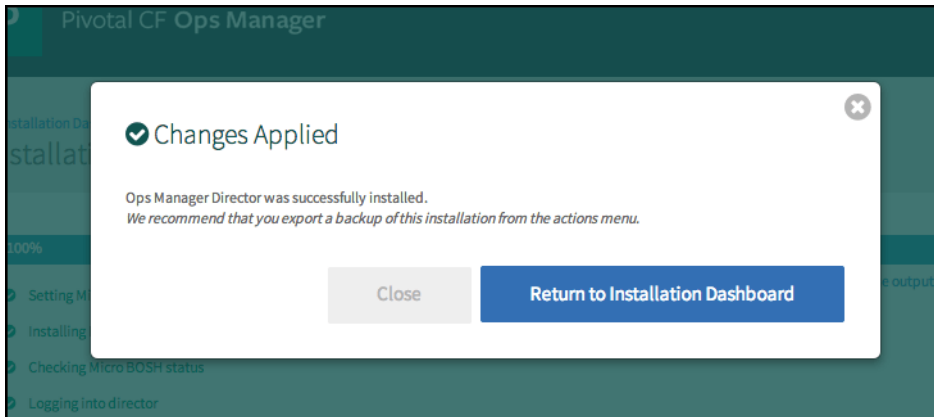
Please review the errors below

- Cannot reach gateway with IP 10.0.0.16.1 (ignorable if ICMP is disabled)
- Cannot reach DNS with IP 10.0.0.2 (ignorable if ICMP is disabled)

Ignore errors and start the install

Stop and fix errors

- BOSH Director installs. This may take a few moments. When the installation process successfully completes, the **Changes Applied** window appears.



4. After you complete this procedure, continue to the topic for the runtime you are installing:

- PAS: [Deploying PAS on AWS Using Terraform](#)
- PKS v1.2: [Installing PKS on AWS](#) 

Deploying PAS on AWS Using Terraform

Page last updated:

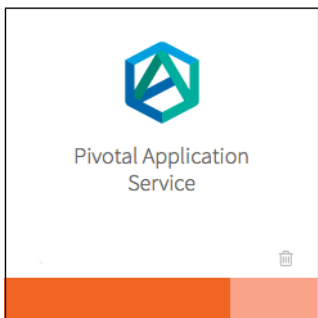
This topic describes how to install and configure Pivotal Application Service (PAS) on Amazon Web Services (AWS).

Before beginning this procedure, ensure that you have successfully completed the [Configuring BOSH Director on AWS Using Terraform](#) topic.

Note: If you plan to [install the PCF IPsec add-on](#), you must do so before installing any other tiles. Pivotal recommends installing IPsec immediately after Ops Manager, and before installing the PAS tile.

Step 1: Add PAS to Ops Manager

1. If you have not already downloaded PAS, log in to [Pivotal Network](#), and click PAS.
2. From the **Releases** dropdown, select the release to install and choose one of the following:
 - a. Click PAS to download the PAS `.pivotal` file.
 - b. Click **PCF Small Footprint Runtime** to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).
3. Navigate to the Pivotal Cloud Foundry Operations Manager Installation Dashboard.
4. Click **Import a Product** to add your tile to Ops Manager. For more information, refer to the [Adding and Deleting Products](#) topic.
5. Click the PAS tile in the Installation Dashboard.



Step 2: Assign Availability Zones and Networks

1. Select **Assign AZ and Networks**.
2. Select an Availability Zone under **Place singleton jobs**. Ops Manager runs any job with a single instance in this Availability Zone.
3. Select all three Availability Zones under **Balance other jobs**. Ops Manager balances instances of jobs with more than one instance across the Availability Zones that you specify.
4. From the **Network** dropdown, choose the `pas` network you created when configuring the BOSH Director tile.

Installation Dashboard

Pivotal Application Service

Settings Status Credentials Logs

Assign AZs and Networks

AZ and Network Assignments

Place singleton jobs in

☐ first-az

Balance other jobs in

☒ first-az

Network

first-network

Save

Domains

Networking

Application Containers

Application Developer Controls

Application Security Groups

Authentication and Enterprise SSO

Databases

5. Click **Save**.

Note: When you save this form, a verification error displays because the PCF security group blocks ICMP. You can ignore this error.

PCF Ops Manager

Please review the errors below

- Cannot reach gateway with IP 10.0.16.1 (ignorable if ICMP is disabled)
- Cannot reach DNS with IP 10.0.0.2 (ignorable if ICMP is disabled)

All errors will be reverified before installation.

Step 3: Configure Domains

1. Select **Domains**.

Application Service hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain *

sys.metallicseaweed.cf-app.com

Apps Domain *

apps.metallicseaweed.cf-app.com

Save

2. Enter the system and application domains.

- For **System Domain**, enter the value of `sys_domain` from the Terraform output. This defines your target when you push apps to PAS.
- For **Apps Domain**, enter the value of `apps_domain` from the Terraform output. This defines where PAS should serve your apps.

Note: You configured a wildcard DNS record for these domains in an earlier step.

3. Click **Save**.

Step 4: Configure Networking

1. Select **Networking**.
2. Leave the **Router IPs**, **SSH Proxy IPs**, **HAProxy IPs**, and **TCP Router IPs** fields blank. You do not need to complete these fields when deploying PCF to AWS with Elastic Load Balancers (ELBs).

Note: You specify load balancers in the **Resource Config** section of Pivotal Application Service (PAS) later in the installation process. See the [Configure Router to Elastic Load Balancer](#) section of this topic for more information.

3. Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate** and **Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.
 - a. Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

The screenshot displays the 'Certificates and Private Keys for HAProxy and Router' configuration interface. It features two expandable sections, 'example-cert' and 'example-cert-2'. Each section contains a 'Name' input field and a large text area for the certificate and private key. The 'example-cert' section shows a pre-generated RSA certificate and private key, with a 'Generate RSA Certificate' link below it. The 'example-cert-2' section is currently empty, showing only the input fields. An 'Add' button is located in the top right corner of the configuration area.

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager.

- b. If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see [Configure Front End](https://docs.pivotal.io/pcf/om/2-2/gcp/prepare-env-manual.html#config-frontend) in [Preparing to Deploy Ops Manager on GCP Manually](https://docs.pivotal.io/pcf/om/2-2/gcp/prepare-env-manual.html#config-frontend).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

- (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Router** field, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

☐ TLSv1.0
 ☐ TLSv1.1
 ☒ TLSv1.2

- Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

☒ Log client IPs
 ☐ Disable logging of X-Forwarded-For header only
 ☐ Disable logging of both source IP and X-Forwarded-For header

To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.

- Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.



Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

☒ TLS terminated for the first time at infrastructure load balancer
 ☐ TLS terminated for the first time at HAProxy
 ☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|---|-----------------------------------|-------------------|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and | TLS terminated for | |

| | | |
|--|--|--|
| <ul style="list-style-type: none"> Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | <p>the first time at infrastructure load balancer (default).</p> | <p>Both HAProxy and the Gorouter forward the XFCC header when included in the request.</p> |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to the instances of HAProxy, and HAProxy instance count is > 0 | <p>TLS terminated for the first time at HAProxy.</p> | <p>HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header.</p> <div>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. </div> |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | <p>TLS terminated for the first time at the Gorouter.</p> | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p> <div>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. </div> |


For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).

8. To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

- ☒ HAProxy does not request client certificates.
- ☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.

 **warning:** Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

9. To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client

certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.

- **Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- **Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

⚠ warning: Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client Certificate Validation** in the **Networking** pane.

10. In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`.

💡 Note: AWS Classic Load Balancers do not support PCF's default cipher suites. See [TLS Cipher Suite Support by AWS Load Balancers](#) for information about configuring your AWS load balancers and Gorouter.

If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

`ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384`

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.

💡 Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

11. In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:
`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384` If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384`

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

💡 Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

12. Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable

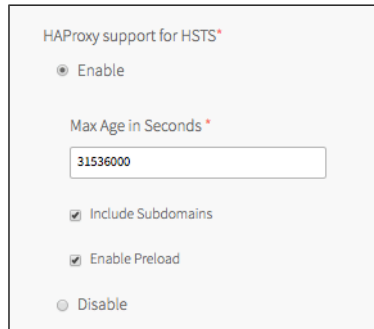
◦ Enable HAProxy forwarding of requests to Router over TLS

| If you want to: | Encrypt communication between HAProxy and the Gorouter |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

◦ Disable HAProxy forwarding of requests to Router over TLS

| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |


13. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field, and complete



the following optional configuration steps:

- (Optional) Enter a **Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
- (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
- (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from HAProxy.

- If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

- (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

- (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
- (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
- (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
- By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#)

- (Optional) By default, Gorouter support for the PROXY protocol is disabled. To enable the PROXY protocol, select **Enable support for PROXY protocol in CF Router**. When enabled, client-side load balancers that terminate TLS but do not support HTTP can pass along information from the originating client. Enabling this option may impact Gorouter performance. For more information about enabling the PROXY protocol in Gorouter, see the *HTTP Header Forwarding* sections in the [Securing Traffic in Cloud Foundry](#) topic.
- In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details. 1. If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
- (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can

determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

500

23. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router*


☒ Enable
 ☐ Disable

24. (Optional) To accommodate larger uploads over connections with high latency, increase the number of seconds in the **Router Timeout to Backends** field.
25. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

26. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
27. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

Load Balancer Healthy Threshold *

28. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

29. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

30. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.

HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.

HAProxy Trusted CIDRs

31. The **Loggregator Port** defaults to if left blank. For AWS environments that are not using an Application Load Balancer, enter .

Container Network Interface Plugin*



32. For **Container Network Interface Plugin**, ensure **Silk** is selected and review the following fields:

Note: The **External** option exists to support NSX-T integration for vSphere deployments.

- (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to . Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses .

warning: The overlay network IP range must not conflict with any other IP addresses in your network.

- Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to .
- For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to .
- To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- By default, containers use the same DNS servers as the host. If you want to override the DNS servers to be used in containers, enter a comma-separated list of servers in **DNS Servers**.

Note: If your deployment uses BOSH DNS, which is the default, you cannot use this field to override the DNS servers used in containers.

33. For **DNS Search Domains**, enter DNS search domains as a comma-separated list. Your containers append these search domains to hostnames to resolve them into full domain names.

DNS Search Domains

example.com, myapps.com

DNS search domains to be used in containers. A comma-separated list can be specified.

34. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is . You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

35. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:
 - a. Select **Enable TCP Routing**
 - b. For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. If you [configured AWS for PCF manually](#), enter `1024-1123` which corresponds to the rules you created for `pcf-tcp-elb`.
 - To support multiple TCP routes, Pivotal recommends allocating multiple ports.
 - To allocate a list of ports rather than a range:
 1. Enter a single port in the **TCP Routing Ports** field.
 2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.
 - c. For AWS, you also need to specify the name of a TCP ELB in the **LOAD BALANCER** column of TCP Router job of the `Resource Config` screen. You configure this later on in PAS. For more information, see the [Configure Router to Elastic Load Balancer](#) topic.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time

☒ Enable TCP Routing

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

1024-1123

36. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) [↗](#) topic.

37. Click **Save**

Step 5: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC

☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888


Docker Images Disk-Cleanup Scheduling on Cell VMs*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) *


10240


- The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.
- The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
- If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
- If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.


- To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting](#) in *HTTP Routing*.

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

 **Warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

- You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
- Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
- Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
- Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.

 **Note:** In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

- (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs*

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

- By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.

13. Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
14. You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is seconds and the maximum configurable timeout is seconds.
15. Click **Save**.

Step 6: Configure Application Developer Controls

1. Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *


Staging Timeout (Seconds) *

☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.
4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.
5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.

 **Note:** If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system

upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of seconds you specify in this field.
9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 7: Review Application Security Groups

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 8: Configure UAA

1. Select **UAA**.
2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

3. Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN` .



Note: The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN` .

4. If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
M
U
H
M
-----END CERTIFICATE-----

Change

SAML Service Provider Key Password

Secret

Password.

5. For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
6. (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line

Apps Manager Access Token Lifetime (in seconds) *

1209600

Apps Manager Refresh Token Lifetime (in seconds) *

1209600

Cloud Foundry CLI Access Token Lifetime (in seconds) *

7200

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

1209600

Global Login Session Max Timeout (in seconds) *

1800

Global Login Session Idle Timeout (in seconds) *

1800

Customize Username Label (on login page) *

Email

Customize Password Label (on login page) *

Password

Proxy IPs Regular Expression *


10\.\d{1,3}\.\d{1,3}\.\d{1,3}|192\.168\.\d{1,3}

Save

Interface (cf CLI) login access and refresh. Most deployments use the defaults.

7. (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:
 - **Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - **Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan

8. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
9. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Gorouter or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
10. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#) for help.

Internal Database Configuration

When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane, which can be one of two options. See [Migrate to Internal Percona MySQL](#) for details.

1. Select **Internal MySQL**.


Choose the location of your UAA database *


☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use AWS RDS)

1. Click **Save**.
2. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

 **Note:** The exact procedure to create databases depends upon the database provider you select for your deployment. The following procedure uses AWS RDS as an example, but UAA also supports Azure SQL Server.

 **warning:** Protect whichever database you use in your deployment with a password.

To create your UAA database, perform the following steps:

1. Add the `ubuntu` account key pair from your IaaS deployment to your local SSH profile so you can access the Ops Manager VM. This is the value of the `ops_manager_ssh_private_key` from the Terraform output.

```
$ ssh-add aws-keypair.pem
```

2. SSH in to your Ops Manager using the Ops Manager FQDN and the username `ubuntu`:

```
$ ssh ubuntu@OPS-MANAGER-FQDN
```

3. Log in to your MySQL database instance using the appropriate hostname and user login values configured in your IaaS account. For example, to log in to your AWS RDS instance, run the following MySQL command:

```
$ mysql --host=RDSHOSTNAME --user=RDSUSERNAME --password=RDSPASSWORD
```

4. Run the following MySQL commands to create a database for UAA:

```
CREATE database uaa;
```

5. Type `exit` to quit the MySQL client, and `exit` again to close your connection to the Ops Manager VM.
6. Reboot the RDS instance in the AWS console.
7. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)
 ☒ External (preferred if, for example, you use AWS RDS)

Hostname *

TCP Port *

Username *

Password *

8. For **Hostname**, enter the hostname of the database server. This is the value from the `rds_address` key in the Terraform output.
9. For **TCP Port**, enter the port of the database server. This is the value from the `rds_port` key in the Terraform output.
10. For **User Account and Authentication database username**, specify the username that can access this database on the database server. This is the value from the `rds_username` key in the Terraform output.
11. For **User Account and Authentication database password**, specify a password for the provided username. This is the value from the `rds_password` key in the Terraform output.
12. Click **Save**.

Step 9: Configure CredHub

Note: Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

1. Select **CredHub**.
2. Choose the location of your CredHub database. PAS includes this CredHub database for services to store their service instance credentials.

Note: You cannot choose **Internal** for the CredHub database if you choose **External** for your System Databases. See [Configure System Databases](#) below.

Configure the CredHub Server

Choose the location of your CredHub database *

☒ Internal MySQL (preferred for complete high-availability)
 ☐ External (preferred if, for example, you use Google Cloud SQL)

If you chose **External**, enter the following:

- **Hostname.** This is the IP address of your database server. See the value from the `PcfRdsAddress` key in the AWS output.
- **TCP Port.** This is the port of your database server. See the value from the `PcfRdsPort` key in the AWS output.
- **Username.** This is the value from the `PcfRdsUsername` key in the AWS output.
- **Password.** This is the value from the `PcfRdsPassword` key in the AWS output.
- **Database CA Certificate.** This certificate is used when encrypting traffic to and from the database.

3. Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys

Name *

Name of the encryption key.

Provider*


Internal

Key *

Secret

☐ Primary

- **Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- **Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- **Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- **Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.

 **Note:** For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

4. (Optional) To configure CredHub to use an HSM, complete the following fields:

- **HSM Provider Partition.** This is the name of the HSM provider partition.
- **HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- **HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#) in the

Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

5. If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.
6. Click **Save**.
7. Select the **Resource Config** pane.
8. Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.
9. Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).

Step 10: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *


2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.

3. Click **Save**.

Step 11: Configure System Databases

You can configure PAS to use an internal MySQL database provided with PCF, or you can configure an external database provider for the databases required by PAS.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration

If you want to use internal databases for your deployment, perform the following steps:

1. Select **Databases**.
2. Select one of the **Internal Databases** options:

- Internal Databases - MySQL - Percona XtraDB Cluster uses [Percona Server](#) with TLS encryption between server cluster nodes.
- Internal Databases - MySQL - MariaDB Galera Cluster uses [MariaDB](#) with cluster nodes communicating over plaintext.

⚠ warning: Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

3. Click **Save**.

Then proceed to [Step 13: \(Optional\) Configure Internal MySQL](#) to configure high availability for your internal MySQL databases.

Create External System Databases

If you want to use an external database provider for your PAS databases, you must first create the databases on the RDS instance provided by the Terraform templates.

To create the required databases on an AWS RDS instance, perform the following steps.

1. Add the AWS-provided key pair to your SSH profile so that you can access the Ops Manager VM. This is the value of the `ops_manager_ssh_private_key` from the Terraform output.

```
ssh-add aws-keypair.pem
```

2. SSH in to your Ops Manager using the Ops Manager FQDN and the username `ubuntu`:

```
ssh ubuntu@OPS_MANAGER_FQDN
```

3. Run the following terminal command to log in to your RDS instance through the MySQL client, using values from the terraform output to fill in the following keys:

```
mysql --host=rds_address --user=rds_username --password=rds_password
```

4. Run the following MySQL commands to create databases for the seven PAS components that require a relational database:

```
CREATE database ccdb;
CREATE database notifications;
CREATE database autoscale;
CREATE database app_usage_service;
CREATE database routing;
CREATE database diego;
CREATE database account;
CREATE database nfsvolume;
CREATE database networkpolicyserver;
CREATE database silk;
CREATE database locket;
CREATE database credhub;
```

5. Type `exit` to quit the MySQL client, and `exit` again to close your connection to the Ops Manager VM.
6. Reboot the RDS instance in the AWS console.
7. In PAS, select **Databases**.
8. Select the **External Databases** option.

Place the databases used by Application Service components.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☐ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☒ External Databases - (e.g. AWS RDS)

Hostname *

TCP Port *

App Usage Service Database Username *


App Usage Service Database Password *

9. For the **Hostname** and **TCP Port** fields, complete the following fields:

| PAS Field | terraform output |
|-----------|--------------------------|
| Hostname | <code>rds_address</code> |
| TCP Port | <code>rds_port</code> |


10. For each **database username** and **database password** field, complete the following fields:

| PAS Field | terraform output |
|---------------------------------|---------------------------|
| DATABASE-NAME database username | <code>rds_username</code> |
| DATABASE-NAME database password | <code>rds_password</code> |

 **Note:** Ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.

1. Click **Save**.


Step 13: (Optional) Configure Internal MySQL

 **Note:** You only need to configure this section if you have selected one of the **Internal Databases - MySQL** options in the **Databases** section.

To use internal MySQL in High Availability configuration, you define a load balancer rule that lets PAS components send queries a single hostname backed by two redundant proxies. Each proxy then directs query traffic to three MySQL server nodes.

1. Allocate an internal load balancer rule to balance traffic between two static IP addresses. The static IP addresses cannot be within the range that that you have reserved for PAS.
The load balancer rule is separate from the software provided by Pivotal, and you need to define it within your infrastructure.
 - **Make your idle time out long enough to not interrupt long-running queries.** When queries take a long time, the load balancer can time out and interrupt the query.
For example, [AWS's Elastic Load Balancer](#) has a default idle timeout of 60 seconds, so queries that take longer than this duration sever the MySQL connection and return an error.
 - **Configure a healthcheck or monitor, using TCP against port 1936.** This defaults to TCP port `1936`, to maintain backwards compatibility with previous releases. This port is not configurable. Unauthenticated healthchecks against port 3306 may cause the service to become unavailable and require manual intervention to fix.
 - **Configure the load balancer to route traffic for TCP port 3306 to the IPs of all proxy instances on TCP port 3306.**

- Record the hostname of the load balancer rule and the two static IP addresses.

 **warning:** You must configure a load balancer to achieve complete high availability.

- From the PAS tile in Ops Manager, Select **Internal MySQL**.
- In the **MySQL Proxy IPs** field, enter the static IP addresses used by the internal MySQL load balancer rule.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.


A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.

The automated backups functionality works with any S3-compatible file store that can receive your backup files.

MySQL Proxy IPs

MySQL Service Hostname

- For **MySQL Service Hostname**, enter the IP address or hostname for your load balancer. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.
- In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
- In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.
- (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
- To prohibit the creation of command line history files on the MySQL nodes, disable the **Allow Command History** checkbox.
- To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

- For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the default value is 10 seconds.

Replication canary time period *

Replication canary read delay *

E-mail address (required) *

☒ Allow Command History

Cluster Probe Timeout

11. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.
12. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.
 - a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.

Server Activity Logging *

☐ Disable server activity logging

☒ Enable server activity logging

Event types *

Load Balancer Healthy Threshold *

Load Balancer Unhealthy Threshold *

Save

13. Enter values for the following fields:
 - **Load Balancer Healthy Threshold:** Specifies the amount of time, in seconds, to wait until declaring the MySQL Proxy instance started. This allows an external load balancer time to register the instance as healthy.
 - **Load Balancer Unhealthy Threshold:** Specifies the amount of time, in seconds, that the MySQL Proxy continues to accept connections before shutting down. During this period, the Healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.
14. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.
15. Click **Save**.

For more information on how to monitor the node health of your MySQL Proxy instances, see [Using the MySQL Proxy](#).

Step 14: Configure File Storage

To minimize system downtime, Pivotal recommends using highly resilient and redundant *external* filestores for your Pivotal Application Service (PAS) file storage.

When configuring file storage for the Cloud Controller in PAS, you can select one of the following:

- Internal WebDAV filestore
- External S3-compatible or Ceph-compatible filestore
- External Google Cloud Storage with Access Key and Secret Key
- External Google Cloud Storage with Service Account
- External Azure Cloud Storage

For production-level PCF deployments on AWS, Pivotal recommends selecting the **External S3-Compatible File Store**. For more information about production-level PCF deployments on AWS, see the [Reference Architecture for Pivotal Cloud Foundry on AWS](#).

For additional factors to consider when selecting file storage, see the [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#) topic.

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External S3 or Ceph Filestore

To use an external S3-compatible filestore for PAS file storage, perform the following steps:

1. In the PAS tile, select **File Storage**.
2. Select the **External S3-Compatible Filestore** option and complete the following fields:
 - Enter the `https://` **URL Endpoint** for your region.
For example, in the **us-west-2** region, enter `https://s3-us-west-2.amazonaws.com/`.
 - If you use an AWS instance profile to manage role information for your filestore, select the **S3 AWS with Instance Profile** checkbox. For more information, see [AWS Identity and Access Management](#) in the AWS documentation.

- Alternatively, enter the **Access Key** and **Secret Key** of the `pcf-user` you created when configuring AWS for PCF. If you select the **S3 AWS with Instance Profile** checkbox and also enter an **Access Key** and **Secret Key**, the instance profile will overrule the Access Key and Secret Key.
- From the **S3 Signature Version** dropdown, select **V4 Signature**. For more information about S4 signatures, see [Signing AWS API Requests](#) in the AWS documentation.
- For **Region**, enter the region in which your S3 buckets are located. `us-west-2` is an example of an acceptable value for this field.
- Select **Server-side Encryption** to encrypt the contents of your S3 filestore. This option is only available for AWS S3.
- (Optional) If you selected **Server-side Encryption**, you can also specify a **KMS Key ID**. PAS uses the KMS key to encrypt files uploaded to the

blobstore. If you do not provide a KMS Key ID, PAS uses the default AWS key. For more information, see [Protecting Data Using Server-Side Encryption with AWS KMS–Managed Keys \(SSE-KMS\)](#).

- Enter names for your S3 buckets:

| Ops Manager Field | Value | Description |
|------------------------|-----------------------|---|
| Buildpacks Bucket Name | pcf-buildpacks-bucket | This S3 bucket stores app buildpacks. |
| Droplets Bucket Name | pcf-droplets-bucket | This S3 bucket stores app droplets. Pivotal recommends that you use a unique bucket name for droplets, but you can also use the same name as above. |
| Packages Bucket Name | pcf-packages-bucket | This S3 bucket stores app packages. Pivotal recommends that you use a unique bucket name for packages, but you can also use the same name as above. |
| Resources Bucket Name | pcf-resources-bucket | This S3 bucket stores app resources. Pivotal recommends that you use a unique bucket name for app resources, but you can also use the same name as above. |

- Configure the following depending on whether your S3 buckets have versioning enabled:
 - Versioned S3 buckets:** Enable the **Use versioning for backup and restore** checkbox to archive each bucket to a version.
 - Unversioned S3 buckets:** Disable the **Use versioning for backup and restore** checkbox, and enter a backup bucket name for each active bucket. The backup bucket name must be different from the name of the active bucket it backs up.

☐ Use versioning for backup and restore.
 (All of the above buckets must have versioning enabled and use the V4 S3 Signature Version).

If versioning is not enabled or supported, you can configure separate buckets below for backups. More information at <https://docs.pivotal.io/pivotalcf/2-1/customizing/backup-restore/backup-pcf-bbr.html>.

Backup Region

Backup Buildpacks Bucket Name


Backup Droplets Bucket Name

Backup Packages Bucket Name

For more information

about setting up external S3 blobstores, see the [Backup and Restore with External Blobstores](#) topic in the Cloud Foundry documentation.

- Click **Save**.


 **Note:** For more information regarding AWS S3 Signatures, see the [Authenticating Requests](#) topic in the AWS documentation.

Other IaaS Storage Options

[Google Cloud Storage](#) and [Azure Storage](#) are also available as file storage options, but are not recommended for typical PCF on AWS installations.

Step 15: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

 **Note:** The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system

logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

☒ No

☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging


☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration


Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.

 **Note:** The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.

6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.
8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.

 **Note:** Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 16: (Optional) Customize Apps

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

Add

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑️
- ▶ Docs 🗑️
- ▶ Tools 🗑️

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

4. Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
5. Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
6. Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
7. Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
8. The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
9. The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 17: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

Note: If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 18: (Optional) Configure App Autoscaler

To use App Autoscaler, you must create an instance of the service and bind it to an app. To create an instance of App Autoscaler and bind it to an app, see [Set Up App Autoscaler](#) in the *Scaling an Application Using App Autoscaler* topic.

- Click **App Autoscaler**.

Configure the App Autoscaler

Autoscaler Instance Count (min: 1) *

Autoscaler API Instance Count (min: 1) *

Metric Collection Interval (min: 60, max: 3600) (min: 60, max: 3600) *

Scaling Interval (min: 15, max: 120) (min: 15, max: 120) *

☐ Verbose Logging

☐ Disable API Connection Pooling

☒ Enable Notifications

- Review the following settings:

- Autoscaler Instance Count:** How many instances of the App Autoscaler service you want to deploy. The default value is `3`. For high availability, set this number to `3` or higher. You should set the instance count to an odd number to avoid split-brain scenarios during leadership elections. Larger environments may require more instances than the default number.
- Autoscaler API Instance Count:** How many instances of the App Autoscaler API you want to deploy. The default value is `1`. Larger environments may require more instances than the default number.
- Metric Collection Interval:** How many seconds of data collection you want App Autoscaler to evaluate when making scaling decisions. The minimum interval is 60 seconds, and the maximum interval is 3600 seconds. The default value is `120`. Increase this number if the metrics you use in your scaling rules are emitted less frequently than the existing Metric Collection Interval.
- Scaling Interval:** How frequently App Autoscaler evaluates an app for scaling. The minimum interval is 15 seconds, and the maximum interval is 120 seconds. The default value is `35`.
- Verbose Logging** (checkbox): Enables verbose logging for App Autoscaler. Verbose logging is disabled by default. Select this checkbox to see more detailed logs. Verbose logs show specific reasons why App Autoscaler scaled the app, including information about minimum and maximum instance limits, App Autoscaler's status. For more information about App Autoscaler logs, see [App Autoscaler Events and Notifications](#).
- Disable API Connection Pooling:** API connection pooling increases performance by reducing the cost associated with establishing new connections. If you do not want to keep connections open for reuse, select this option.

3. Click **Save**.

Step 19: Configure Cloud Controller

1. Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
 ☒ Disable

Save

2. Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

3. CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

4. Click **Save**.

Step 20: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

1. Select **Smoke Tests**.
2. If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

- ☐ Temporary space within the system organization (This is deleted after smoke tests finish.)
- ☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.

Step 21: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

Note: Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.

Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.

Whitelist for non-RFC-1918 Private Networks *

allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.

CF CLI Connection Timeout

15

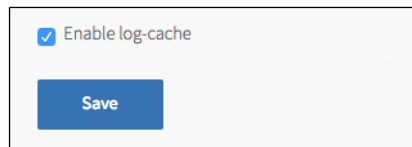
2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PASTopic*.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



A screenshot of a configuration panel. It contains a checkbox labeled 'Enable log-cache' which is checked. Below the checkbox is a blue button labeled 'Save'.

2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

⚠ warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 22: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

💡 Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.

- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

💡 Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.

- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.
- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

Step 23: Configure Router (or HAProxy) to Elastic Load Balancer

1. In the PAS tile, click **Resource Config**.

Resource Config

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|-------------------------------|--------------|----------------------|---|----------------|-------------------------------------|
| Consul | 1 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| NATS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| File Storage | Automatic: 1 | Automatic: 100 GB | Automatic: medium.mem (cpu: 1, ram: 6 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Proxy | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Server | 1 | Automatic: 100 GB | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 64 GB) | | <input checked="" type="checkbox"/> |
| Backup Prepare Node | Automatic: 1 | Automatic: 200 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego BBS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| UAA | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| HAProxy | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Router | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-web-elb | <input checked="" type="checkbox"/> |
| MySQL Monitor | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Clock Global | Automatic: 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller Worker | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego Brain | 1 | Automatic: 1 GB | Automatic: small (cpu: 1, ram: 2 GB, disk: 8 GB) | pcf-ssh-elb | <input checked="" type="checkbox"/> |
| Diego Cell | 1 | None | Automatic: xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB) | | <input checked="" type="checkbox"/> |
| Loggregator Trafficcontroller | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Adapter | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Scheduler | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Doppler Server | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| TCP Router | 0 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-tcp-elb | <input checked="" type="checkbox"/> |
| CredHub | Automatic: 0 | None | Automatic: large (cpu: 2, ram: 8 GB, disk: 16 GB) | | <input checked="" type="checkbox"/> |

Save

2. Enter the name of your SSH load balancer depending on which release you are using.

- **Pivotal Application Service (PAS):** In the **Load Balancers** field of the **Diego Brain** row, enter the value of `ssh_elb_name` from the Terraform output.
- **Small Footprint Runtime:** In the **Load Balancers** field of the **Control** row, enter the value of `ssh_elb_name` from the Terraform output.

3. In the **Load Balancers** field of the **Router** row, enter the value of `web_elb_name` from the Terraform output.

Note: If you are using HAProxy in your deployment, then put the name of the load balancers in the **Load Balancers** field of the **HAProxy** row instead of the **Router** row. For a high availability configuration, scale up the HAProxy job to more than one instance.

4. In the **Load Balancers** field of the **TCP Router** row, enter the value of `tcp_elb_name` from the Terraform output.

5. Click **Save**.

Step 24: (Optional) Scale Down and Disable Resources

Note: The **Resource Config** pane has fewer VMs if you are installing the **Small Footprint Runtime**.

Note: The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to `3` instances and scale the **Control** VM to `2` instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by navigating to the **Resource Config** section and using the dropdowns under **Instances** for each job.

By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding

system-provided resources in Ops Manager to reduce costs and administrative overhead.

To disable specific VMs in Ops Manager, do the following:

1. Click **Resource Config**.
2. If you configured PAS to use an external S3-compatible filestore, enter in **Instances** in the **File Storage** field.
3. If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:
 - **MySQL Proxy**: Enter in **Instances**.
 - **MySQL Server**: Enter in **Instances**.
 - **MySQL Monitor**: Enter in **Instances**.
4. If you disabled TCP routing, enter **Instances** in the **TCP Router** field.
5. If you are not using HAProxy, enter **Instances** in the **HAProxy** field.
6. Click **Save**.

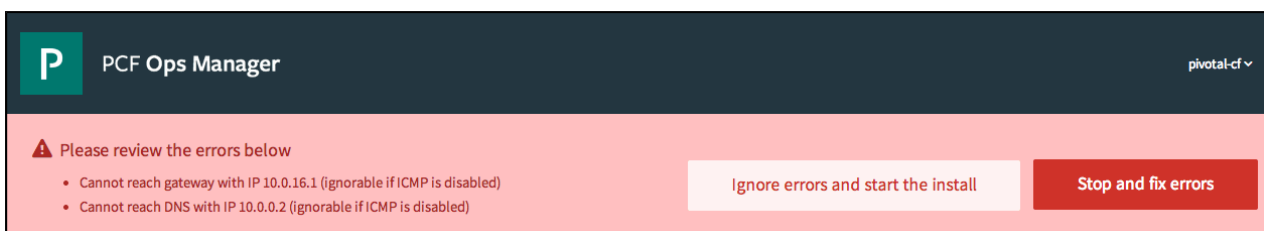
Step 25: Download Stemcell

This step is only required if your Ops Manager does not already have the stemcell version required by PAS. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

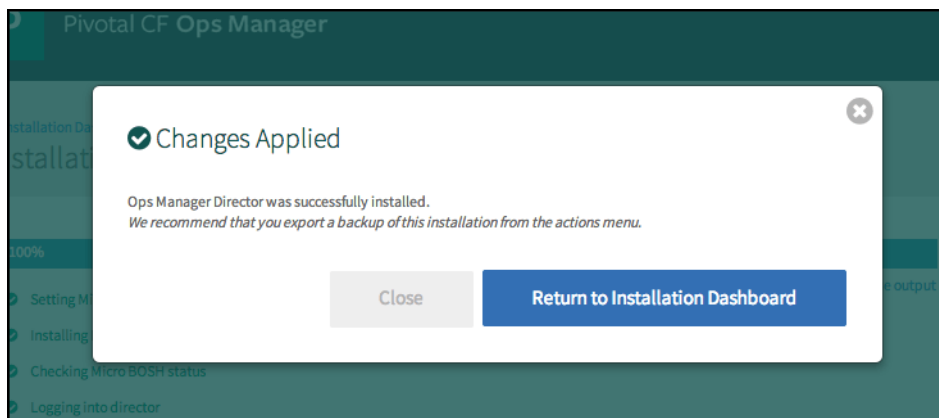
1. Open the [Stemcell product page](#) in the Pivotal Network. *Note, you may have to log in.*
2. Download the appropriate stemcell version targeted for your IaaS.
3. Navigate to **Stemcell Library** in the **Installation Dashboard**.
4. Click **Import Stemcell** to import the downloaded stemcell file.
5. When prompted, enable the Ops Manager product checkbox to stage your stemcell.
6. Click **Apply Stemcell to Products**.

Step 26: Complete the PAS Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.



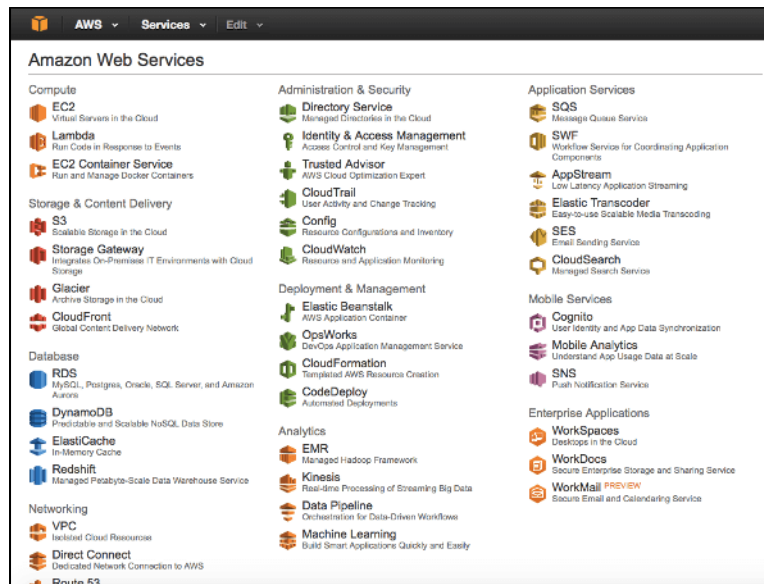
The install process generally requires a minimum of 90 minutes to complete. The image shows the Changes Applied window that displays when the installation process successfully completes.



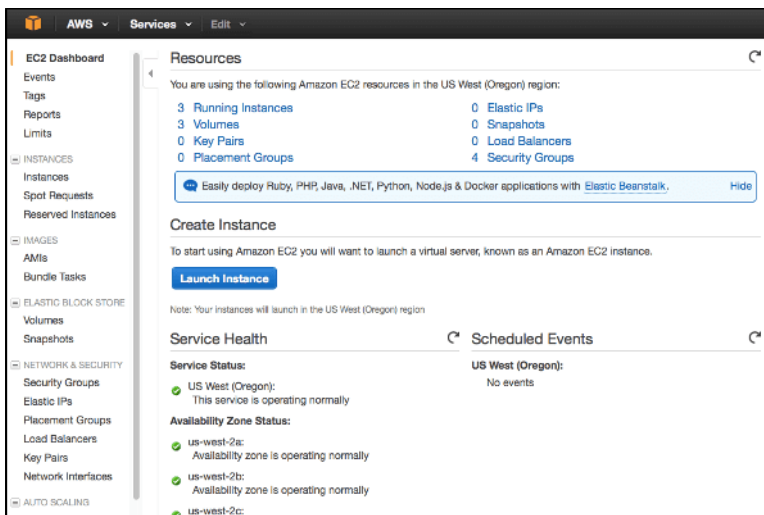
Deleting PCF from AWS

Page last updated:

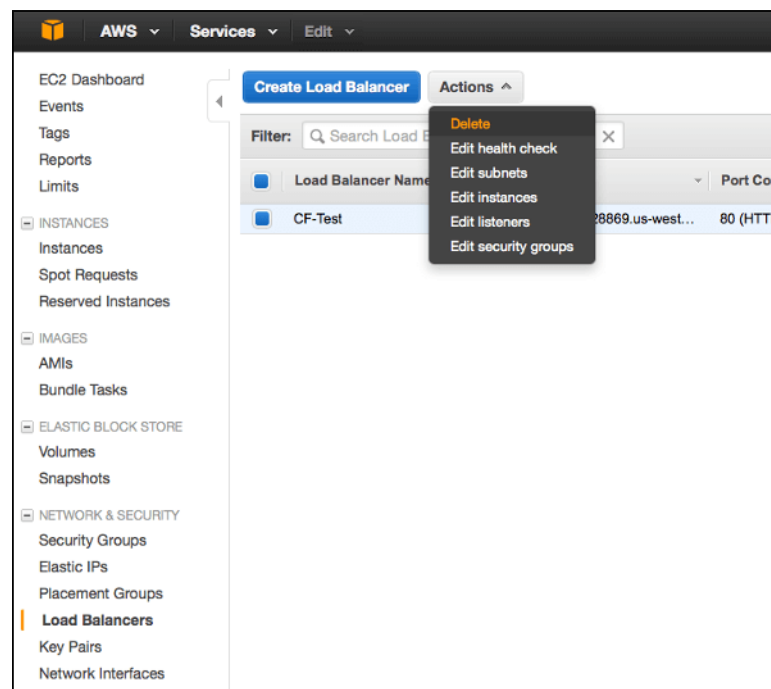
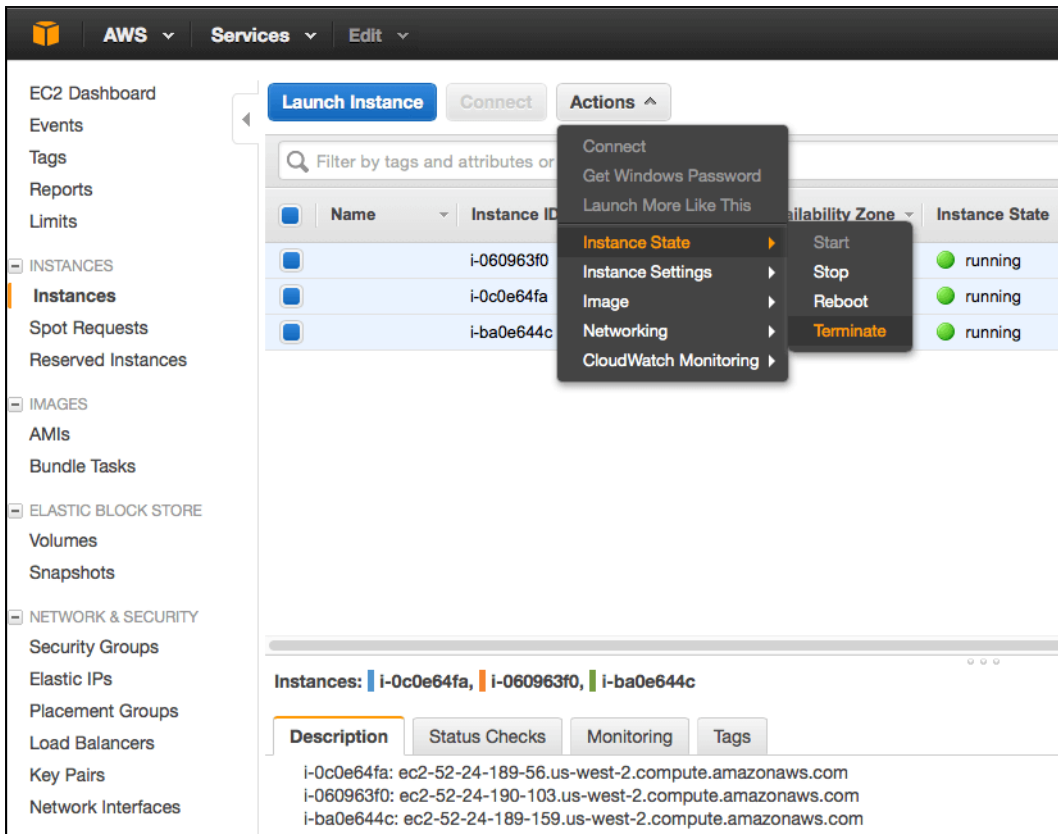
When you deploy [Pivotal Cloud Foundry](#) (PCF) to Amazon Web Services (AWS), you provision a set of resources. This topic describes how to delete the AWS resources associated with a PCF deployment. You can use the AWS console to remove an installation of all components, but retain the objects in your bucket for a future deployment.



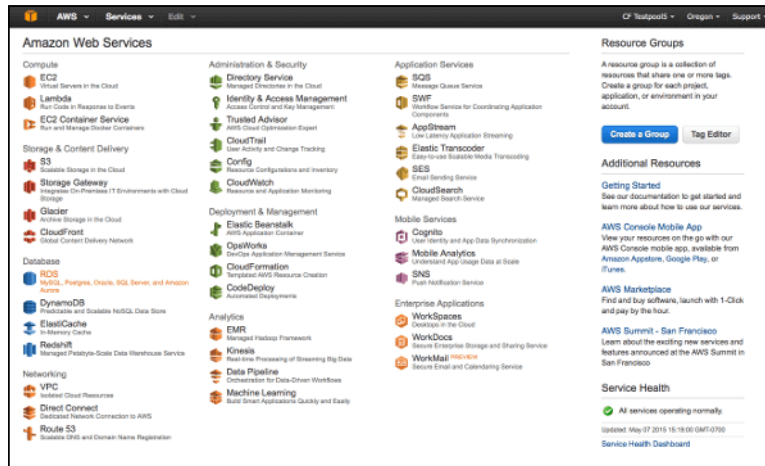
1. Log into your AWS Console.
2. Navigate to your EC2 dashboard. Select **Instances** from the menu on the left side.



3. Terminate all your instances.

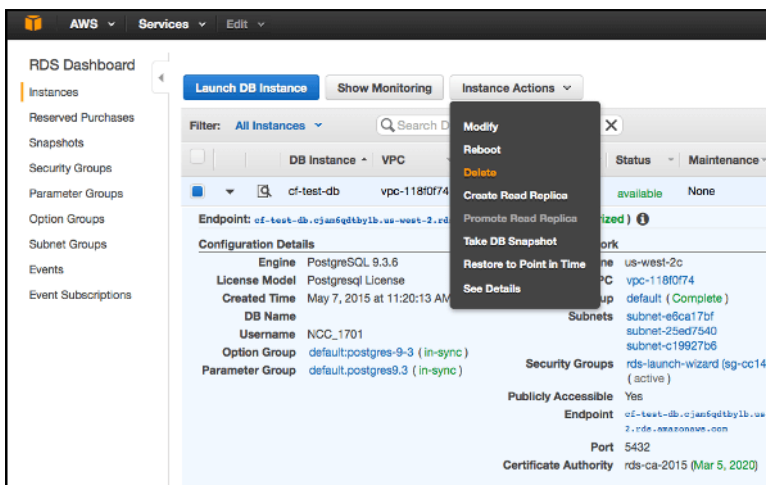


4. Select **Load Balancers**. Delete all load balancers.

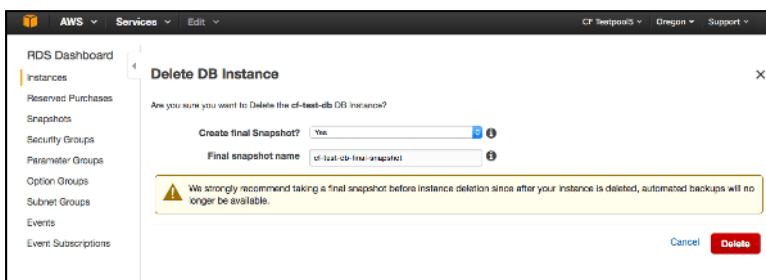


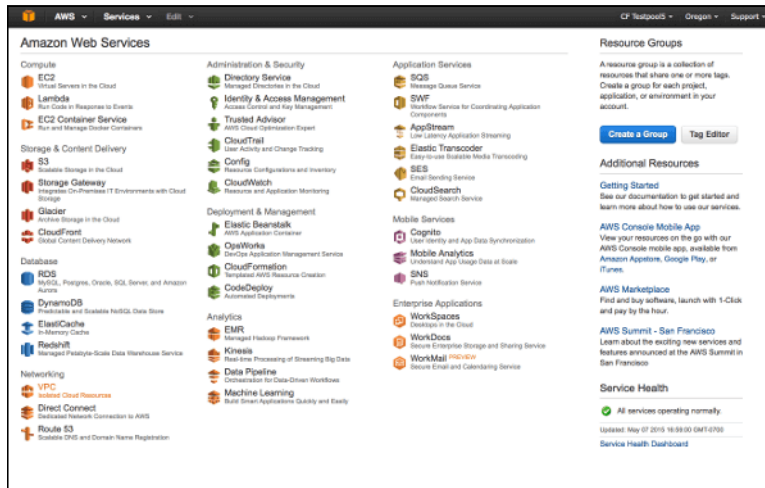
5. From the AWS Console, select RDS.

6. Select **Instances** from the menu on the left side. Delete the RDS instances.



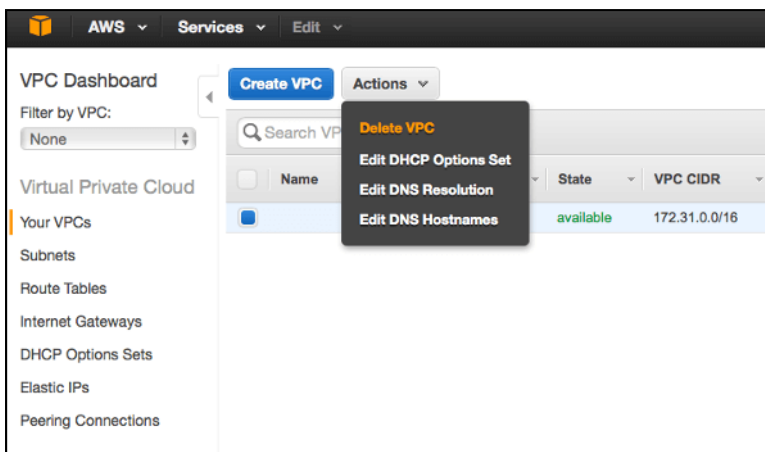
7. Select **Create final Snapshot** from the dropdown. Click **Delete**.



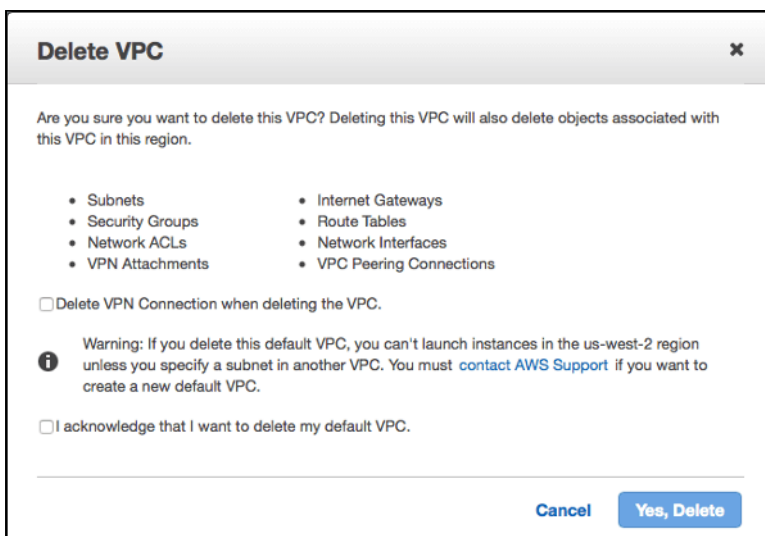


8. From the AWS Console, select VPC.

9. Select **Your VPCs** from the menu on the left. Delete the VPCs.



10. Check the box to acknowledge that you want to delete your default VPC. Click **Yes, Delete**.



Creating a Proxy ELB for Diego SSH

If you want to allow SSH connections to application containers, you may want to use an Elastic Load Balancer (ELB) as the SSH proxy.

Perform the steps below to create this ELB:

1. On the EC2 Dashboard, click **Load Balancers**.
2. Click **Create Load Balancer**, and configure a classic load balancer with the following information:

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name: my-SSH-ELB

Create LB Inside: vpc-4b38852e (10.0.0.0/16) | pcf-vpc

Create an internal load balancer: ☐ (what's this?)

Enable advanced VPC configuration: ☒

Listener Configuration:

| Load Balancer Protocol | Load Balancer Port | Instance Protocol | Instance Port |
|------------------------|--------------------|-------------------|---------------|
| TCP | 2222 | TCP | 2222 |

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

VPC vpc-4b38852e (10.0.0.0/16) | pcf-vpc

Please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.

Available Subnets

| Actions | Availability Zone | Subnet ID | Subnet CIDR | Name |
|---------|-------------------|-----------------|--------------|--------------------|
| + | us-west-1b | subnet-b63be1ef | 10.0.16.0/20 | pcf-private-subnet |
| + | us-west-1b | subnet-b73be1ee | 10.0.2.0/24 | pcf-rds-subnet-1 |
| + | us-west-1c | subnet-c8f095ad | 10.0.3.0/24 | pcf-rds-subnet-2 |

Selected Subnets

| Actions | Availability Zone | Subnet ID | Subnet CIDR | Name |
|---------|-------------------|-----------------|-------------|-------------------|
| - | us-west-1b | subnet-b43be1ed | 10.0.0.0/24 | pcf-public-subnet |

- Enter a load balancer name.
 - **Create LB Inside:** Select the **pcf-vpc** VPC where your PCF installation lives.
 - Ensure that the **Create an internal load balancer** checkbox is not selected.
3. Under **Load Balancer Protocol**, ensure that this ELB is listening on TCP port **2222** and forwarding to TCP port **2222**.
 4. Under **Select Subnets**, select the public subnet.
 5. On the **Assign Security Groups** page, create a new Security Group. This Security Group should allow inbound traffic on TCP port **2222**.

Create Security Group

Security group name: PCF_SSH_ELB_SecurityGroup

Description:

VPC: vpc-4b38852e (10.0.0.0/16) | pcf-vpc

* denotes default VPC

Security group rules:

Inbound | Outbound

| Type | Protocol | Port Range | Source |
|-----------------|----------|------------|----------------------|
| Custom TCP Rule | TCP | 2222 | Anywhere (0.0.0.0/0) |

Add Rule

Cancel Create

- The **Configure Security Settings** page displays a security warning because your load balancer is not using a secure listener. You can ignore this warning.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 3: Configure Security Settings

Improve your load balancer's security. Your load balancer is not using any secure listener.

If your traffic to the load balancer needs to be secure, use either the HTTPS or the SSL protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under [Basic Configuration](#) section. You can also continue with current settings.

- Click **Next: Configure Health Check**.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances. If an instance fails a health check, it is removed from the load balancer. Customize the health check to meet your needs.

Ping Protocol: TCP

Ping Port: 2222

Advanced Details

Response Timeout: 5 seconds

Health Check Interval: 30 seconds

Unhealthy Threshold: 2

Healthy Threshold: 10

- Select **TCP** in **Ping Protocol** on the **Configure Health Check** page. Ensure that the **Ping Port** value is **2222** and set the **Health Check Interval** to **30** seconds.

- Click **Next: Add EC2 Instances**.

- Accept the defaults on the **Add EC2 Instances** page and click **Next: Add Tags**.

- Accept the defaults on the **Add Tags** page and click **Review and Create**.

- Review and confirm the load balancer details, and click **Create**.

- With your DNS service (for example, Amazon Route 53), create an `ssh.system.YOUR-SYSTEM-DOMAIN` DNS record that points to this ELB that you just created.

Create Record Set

Name:

ssh.your-system-domain.com.

Type:

CNAME – Canonical name

Alias:

☐ Yes
 ☒ No

TTL (Seconds):

300

1m

5m

1h

1d

Value:

your-elb-domain

The domain name that you want to resolve to instead of the value in the Name field.

Example:

www.example.com

14. You can now use this ELB to the SSH Proxy of your Pivotal Application Service (PAS) installation.

15. In PAS, select **Resource Config**, and enter the ELB that you just created in the **Diego Brain** row, under the **Load Balancers** column.

| | | | | |
|-------------|---|-----------------|---|-------------|
| UAA | 1 | None | Automatic: t2.small (cpu: 1, ram: 2 GB, disk: 2 GB) | |
| Diego Brain | 1 | Automatic: 1 GB | Automatic: m3.medium (cpu: 1, ram: 3.75 GB, disk: 4 GB) | passion-elb |
| Diego Cell | 3 | None | m3.2xlarge (cpu: 8, ram: 30 GB, disk: 64 GB) | |

Upgrading BOSH Director on AWS

This topic describes how to upgrade BOSH Director for Pivotal Cloud Foundry (PCF) on Amazon Web Services (AWS).

Complete the tasks in this topic as part of the Ops Manager upgrade process. For more information, see [Upgrading Pivotal Cloud Foundry](#).

Overview

In this procedure, you create an Ops Manager VM instance to host the upgraded version of Ops Manager. Then, to complete the Ops Manager upgrade, you export your existing Ops Manager installation onto this new VM.

For PCF installations on AWS, the VM that hosts the new version of Ops Manager uses an Amazon Machine Image (AMI) specific to your region.

To create an Ops Manager VM instance, do the following:

1. Retrieve the Ops Manager AMI ID. See [Retrieve Ops Manager AMI ID](#).
2. Launch the AMI. See [Launch Ops Manager AMI](#).
3. Edit the Ops Manager DNS A Record. See [Edit Ops Manager DNS A Record](#).

Prerequisites

To complete the Ops Manager upgrade, you must have your Ops Manager decryption passphrase. You defined this decryption passphrase during the initial installation of Ops Manager.

Retrieve Ops Manager AMI ID

Ops Manager has a different AMI ID for each region. Retrieve and record the AMI ID for your region. You use this AMI ID when launching the Ops Manager AMI instance.

To retrieve the AMI ID for Ops Manager, perform the following steps:

1. Navigate to the **Pivotal Cloud Foundry Operations Manager** section of [Pivotal Network](#).
2. Select the version of PCF you want to install from the **Releases** dropdown.
3. In the **Release Download Files**, click the file named **Pivotal Cloud Foundry Ops Manager for AWS** to download a PDF.
4. Open the PDF and record the AMI ID for your region.

Launch Ops Manager AMI

Use the AMI ID for your region to launch an AMI instance that hosts the new version of Ops Manager.

To launch the AMI for Ops Manager, perform the following steps:

1. Navigate to your EC2 Dashboard.
2. Click **AMIs** from the **Images** menu.
3. Select **Public images** from the drop-down filter that says **Owned by me**.
4. Paste the AMI ID for your region into the search bar and press enter.



Note: There is a different AMI for each region. If you cannot locate the AMI for your region, verify that you have set your AWS Management Console to your desired region. If you still cannot locate the AMI, log in to the [Pivotal Network](#) and file a support ticket.

Launch Actions

Public images

AMI Name : pivotal-ops AMI ID :

| Name | AMI Name | AMI ID | Source |
|------|---|--------|------------------|
| | pivotal-ops-manager-20150323T224150-dcce5db | ami- | 152787392610/... |

5. (Optional) If you want to encrypt the VM that runs Ops Manager with AWS Key Management Service (KMS), perform the following additional steps:
 - a. Right click the row that lists your AMI and click **Copy AMI**.
 - b. Select your **Destination region**.
 - c. Enable **Encryption**. For more information about AMI encryption, see [Encryption and AMI Copy](#) from the *Copying an AMI* topic in the AWS documentation.
 - d. Select your **Master Key**. To create a new custom key, see [Creating Keys](#) in the AWS documentation.
 - e. Click **Copy AMI**. You can use the new AMI you copied for the following steps.
6. Select the row that lists your Ops Manager AMI and click **Launch**.
7. Choose **m3.large** for your instance type and click **Next: Configure Instance Details**.

| | Family | Type | vCPUs | Memory (GiB) | Instance Storage (GB) |
|-------------------------------------|-----------------|--------------------------------|-------|--------------|-----------------------|
| <input type="checkbox"/> | Micro instances | t1.micro Free tier eligible | 1 | 0.613 | EBS only |
| <input checked="" type="radio"/> | General purpose | t2.micro Free tier eligible | 1 | 1 | EBS only |
| <input checked="" type="radio"/> | General purpose | t2.small | 1 | 2 | EBS only |
| <input checked="" type="radio"/> | General purpose | t2.medium | 2 | 4 | EBS only |
| <input type="checkbox"/> | General purpose | m3.medium | 1 | 3.75 | 1 x 4 (SSD) |
| <input checked="" type="checkbox"/> | General purpose | m3.large | 2 | 7.5 | 1 x 32 (SSD) |

8. Configure the following for your instance:
 - **Network:** Select the VPC that you created.
 - **Subnet:** Select `pcf-public-subnet-az0`.
 - **Auto-assign for Public IP:** Select **Enable**.
 - **IAM role:** Select the IAM role associated with your pc-f-user profile. If you have not created one, click **Create new IAM role** and follow the [Guidelines for Creating User Roles on AWS](#).
 - For all other fields, accept the default values.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1

Purchasing option ☐ Request Spot Instances

Network vpc-8ec593eb (10.0.0.0/16) | pc-f-vpc [Create new VPC](#)

Subnet subnet-fe8129d5 (10.0.0.0/24) | public-az1 | 250 IP Addresses available [Create new subnet](#)

Auto-assign Public IP Enable

IAM role None [Create new IAM role](#)

Shutdown behavior Stop

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy Shared tenancy (multi-tenant hardware)
[Additional charges will apply for dedicated tenancy.](#)

9. Click **Next: Add Storage** and adjust the **Size (GiB)** value. The default persistent disk value is 50 GB. Pivotal recommends increasing this value to a minimum of 100 GB.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

| Type | Device | Snapshot | Size (GiB) | Volume Type | IOPS | Delete on Termination | Encrypted |
|------------------|-----------|---------------|------------|-----------------------|------------|-------------------------------------|---------------|
| Root | /dev/sda1 | snap-f1ce6d7e | 100 | General Purpose (SSD) | 150 / 3000 | <input checked="" type="checkbox"/> | Not Encrypted |
| Instance Store 0 | /dev/sdb | N/A | N/A | N/A | N/A | N/A | Not Encrypted |

[Add New Volume](#)

- Click **Next: Tag Instance**.
- On the **Add Tags** page, add a tag with the key `Name` and value `pcf-ops-manager`.
- Click **Next: Configure Security Group**.
- Select the `pcf-ops-manager-security-group` that you created in [Step 5: Configure a Security Group for Ops Manager](#).
- Click **Review and Launch** and confirm the instance launch details.
- Click **Launch**.
- Select the `pcf-ops-manager-key` key pair, confirm that you have access to the private key file, and click **Launch Instances**. You use this key pair to access the Ops Manager VM.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Choose an existing key pair

Select a key pair

pcf

☒ I acknowledge that I have access to the selected private key file (pcf.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Edit Ops Manager DNS A Record

After you deploy the new Ops Manager VM, edit the Ops Manager DNS record in the EC2 dashboard to point to the IP address for the new VM.

To edit the Ops Manager DNS A record, do the following:

- Click **View Instances** to access the **Instances** page on the EC2 Dashboard.
- Select the VM that you created in the previous section.
- Locate the **IPv4 Public IP** value in the instance **Description** tab, and record this value for use in the next step.
- In your DNS provider, edit the **A** record for `pcf.YOUR-SYSTEM-DOMAIN` to point to the IP address recorded in the previous step.

Next Steps

After you complete this procedure, continue the upgrade instructions in [Upgrading Pivotal Cloud Foundry](#) topic.

Installing Pivotal Cloud Foundry on Azure

This topic describes how to install Pivotal Cloud Foundry (PCF) on Microsoft Azure.

It includes resource requirements, prerequisites, instructions for installing PCF on Azure, and additional resources.

Overview

You can install PCF on Azure, Azure Government Cloud, or Azure Germany. For more information about Azure regions, see [Azure regions](#) in the Microsoft Azure documentation.

You can install PCF on Azure with the Pivotal Application Service (PAS) runtime. There are resource requirements specific to both PAS and Azure. Ensure you meet the requirements for PAS and the requirements specific to Azure before installing PCF on Azure. For more information, see [Requirements](#).

Requirements

This section lists the following resource requirements for installing PCF on Azure:

- PAS resource requirements. See [PAS Resource Requirements](#).
- Azure-specific resource requirements. See [Azure Resource Requirements](#).

PAS Resource Requirements

The following are general resource requirements for deploying and managing a PCF deployment with Ops Manager and PAS:

- PAS requires sufficient IP allocation. The following lists the minimum required IP allocations:
 - One static IP address for either HAProxy or one of your Gorouters
 - One static IP address for each job in the Ops Manager tile. See the Ops Manager **Resource Config** pane for each tile for a full list.
 - One static IP address for each job listed below:
 - Consul
 - NATS
 - File Storage
 - MySQL Proxy
 - MySQL Server
 - Backup Restore Node
 - HAProxy
 - Router
 - MySQL Monitor
 - Diego Brain
 - TCP Router
 - One IP for each VM instance created by the service.
 - An additional IP address for each compilation worker. Use the following formula to determine the total IPs required:

$$\text{IPs needed} = \text{static IPs} + \text{VM instances} + \text{compilation workers}$$
 - Pivotal recommends that you allocate at least 36 dynamic IP addresses when deploying Ops Manager and PAS. BOSH requires additional dynamic IP addresses during installation to compile and deploy VMs, install PAS, and connect to services.
- Pivotal recommends using a network without DHCP for deploying PAS VMs.




Note: If you have DHCP, refer to the [Troubleshooting Guide](#) to avoid issues with your installation.

Azure Resource Requirements


The following are the minimum resource requirements for deploying a PCF deployment with Ops Manager and PAS on Azure:

- An OS disk of 120 GB for the Ops Manager VM.

 **Note:** Ops Manager v1.11 requires a Director VM with at least 8 GB memory.


- A minimum of the following VM instance limits in your Azure account. The number of VMs required depends on the number of tiles and availability zones you plan to deploy. The following VM guidelines apply to the PAS and Small Footprint PAS runtimes:
 - **PAS:** A new Azure deployment requires the following VMs for PAS and Ops Manager:

| VM Type | VM Count |
|---------|----------|
| F1s | 27 |
| F2s | 4 |
| F4s | 4 |
| DS11 v2 | 1 |
| DS12 v2 | 1 |

 **Note:** If you are deploying a test or sandbox PCF that does not require high availability, then you can scale down the number of VM instances in your deployment. For more information, see [Scaling PAS](#).

- **Small Footprint PAS:** A new Azure deployment requires the following VMs for Small Footprint PAS and Ops Manager:


| | VM Type | VM Count | Notes |
|----------------------------|---------|----------|---------------------------------|
| Small Footprint PAS | DS11 v2 | 1 | |
| | DS12 v2 | 2 | |
| | F2s | 0 | Add 1 to count if using HAProxy |
| | F1s | 5 | |
| Ops Manager | DS2 v2 | 1 | |
| | F4s | 4 | |

 **Note:** Some VM instance types are only supported in certain Azure regions. For more information, see [Products available by region](#) in the Azure documentation. To deploy PCF on an Azure region that does not support the above VM instance types, you must override the default VM sizes. For more information, see [Overriding defaults with custom disk types](#) in the Ops Manager API documentation. Changing the default VM sizes may increase the cost of your deployment.


Prerequisites

Before installing PCF on Azure, you must do the following:

- Install the Azure CLI v2.0. For instructions on how to install the Azure CLI for your operating system, see [Preparing to Deploy Ops Manager on Azure Manually](#).
- Configure sufficient IP allocation for PAS. For more information about IP allocation requirements, see [PAS Resource Requirements](#).
- Create an SSL certificate for your PCF domain.

 **Note:** To deploy PCF to a production environment, you must obtain a certificate from a certificate authority. Pivotal recommends using a self-signed certificate generated by Ops Manager for development and testing purposes only.

- Assign administrative rights to a domain for PCF. You must be able to add wildcard records to this domain.
- Create a wildcard DNS record that points to your router or load balancer. Alternatively, you can use a service such as xip.io. For example, `203.0.113.0.xip.io`. Then, create at least one wildcard TLS certificate that matches the DNS record you configured.

 **Note:** With a wildcard DNS record, every hostname in your domain resolves to the IP address of your router or load balancer. For example, if you create a DNS record `*.example.com` pointing to your router, every app deployed to the `example.com` domain resolves to the IP address of your router.

- Create one or more NTP servers, if the NTP servers are not already provided by your Azure project.
- Install the most recent version of the Cloud Foundry Command Line Interface (cf CLI). See [Cloud Foundry Command Line Interface](#) in GitHub.
- **(Optional)** Configure external storage. Pivotal recommends using external storage if possible. For more information about how file storage location affects platform performance and stability during upgrades, see [Configure File Storage](#).

- **(Optional)** Configure external databases. Pivotal recommends using external databases in production deployments for BOSH Director and PAS. An external database must be configured to use the UTC timezone.
- **(Optional)** Configure external user stores. When you deploy PCF, you can select a SAML user store for Ops Manager or a SAML or LDAP user store for PAS, to integrate existing user accounts.

Install PCF on Azure

You can install PCF on Azure either manually or using Terraform.

To install PCF on Azure, do one of the following:

- Install PCF on Azure manually. See [Installing PCF on Azure Manually](#).
- Install PCF on Azure using Terraform. See [Installing PCF on Azure Using Terraform](#).

Install PCF on Azure Government Cloud

To install PCF on Azure Government Cloud, see [Configuring BOSH Director on Azure Government Cloud](#).

Install PCF on Azure Germany

To install PCF in Azure Germany, see [Configuring BOSH Director on Azure Germany](#).

Additional Resources

The following are additional resources related to installing PCF on GCP:

- For information about troubleshooting the PCF on Azure install process, see [Troubleshooting PCF on Azure](#).
- For production-level deployment options for PCF on Azure, see [Reference Architecture for Pivotal Cloud Foundry on Azure](#).
- For information about how to manage IaaS users and credentials in Azure, see [Azure security documentation](#).
- For recommendations on how to create and scope Azure accounts for PCF, see [IaaS Permissions Guidelines](#).
- For information about deleting a PCF on Azure installation, see [Deleting a PCF on Azure Installation](#).
- For information about upgrading PCF on Azure, see [Upgrading BOSH Director on Azure](#).

Installing PCF on Azure Manually

This topic explains how to install Pivotal Cloud Foundry (PCF) on Microsoft Azure manually.

To install PCF on Azure manually, do the following:


1. Deploy Ops Manager. See [Deploying Ops Manager on Azure Manually](#).
2. Configure BOSH Director. See [Configuring BOSH Director on Azure Manually](#).
3. Deploy PAS. See [Deploying PAS on Azure](#).

Preparing to Deploy Ops Manager on Azure Manually



Page last updated:

This topic describes how to prepare Azure to deploy Ops Manager. You must deploy Ops Manager to deploy Pivotal Application Service (PAS) or Pivotal Container Service (PKS).

After you complete this procedure, follow the instructions in one of the following topics:

- [Deploying Ops Manager to Azure Using Terraform](#)
- [Launching a BOSH Director Instance with an ARM Template](#) 
- [Deploying Ops Manager on Azure Manually](#)

Step 1: Install and Configure the Azure CLI

1. Install the Azure CLI 2.0 by following the instructions for your operating system in the [Azure documentation](#) .
2. Set your cloud with the `--name` value corresponding to the Azure environment on which you are installing Ops Manager:
 - **Azure:** `AzureCloud` .
 - **Azure China:** `AzureChinaCloud` . If logging in to `AzureChinaCloud` fails with a `CERT_UNTRUSTED` [error](#) , use the latest version of node, 4.x or later.
 - **Azure Government Cloud:** `AzureUSGovernment` . Azure Government Cloud is only supported in Ops Manager v1.10 and later.
 - **Azure Germany:** `AzureGermanCloud` .

```
$ az cloud set --name AzureCloud
```



Note: For more information about installing Ops Manager in the China Region, see [Install in the China Region](#) in *Installing PCF in Airgapped Environments* in the Pivotal documentation.

3. Log in:

```
$ az login
```

Authenticate by navigating to the URL in the output, entering the provided code, and clicking your account.

Step 2: Set Your Default Subscription

1. To list your Azure subscriptions, run the following command:

```
$ az account list
[
  {
    "id": "12345678-1234-5678-1234-567891234567",
    "name": "Sample Subscription",
    "user": {
      "name": "Sample Account",
      "type": "user"
    },
    "tenantId": "11111111-1234-5678-1234-678912345678",
    "state": "Enabled",
    "isDefault": true,
    "registeredProviders": [],
    "environmentName": "AzureCloud"
  },
  {
    "id": "87654321-1234-5678-1234-678912345678",
    "name": "Sample Subscription1",
    "user": {
      "name": "Sample Account1",
      "type": "user"
    },
    "tenantId": "22222222-1234-5678-1234-678912345678",
    "state": "Enabled",
    "isDefault": false,
    "registeredProviders": [],
    "environmentName": "AzureCloud"
  }
]
```

- a. Identify your default subscription in the output of this command by locating the subscription listed that has `isDefault` set to `true`. To deploy Ops Manager to a different subscription, you must set the other subscription as the default. To set a new default subscription, run the following command:

```
$ az account set --subscription SUBSCRIPTION_ID
```

2. Record the value of the `id` set as the default. You use this value in future configuration steps.
3. Record the value of `tenantID` for your default subscription. This is your `TENANT_ID` for creating a service principal. If your `tenantID` value is not defined, you may be using a personal account to log in to your Azure subscription.

Step 3: Create an Azure Active Directory (AAD) Application

1. Run the following command to create an AAD application, replacing `PASSWORD` with a password of your choice. This is your `CLIENT_SECRET` for creating a service principal.

```
$ az ad app create --display-name "Service Principal for BOSH" \
--password "PASSWORD" --homepage "http://BOSHAzureCPI" \
--identifier-uris "http://BOSHAzureCPI"
```



Note: You can provide any string for the `homepage` and `identifier-uris` flags, but the value of `identifier-uris` must be unique within the organization associated with your Azure subscription. For the `homepage`, Pivotal recommends using `http://BOSHAzureCPI` as shown in the example above.

2. Record the value of `appId` from the output. This is your `APPLICATION_ID` for creating a service principal.

```
{
  "appId": "5c552e8f-b977-45f5-a50b-981cf17cb9d",
  "appPermissions": null,
  "availableToOtherTenants": false,
  "displayName": "Service Principal for BOSH",
  "homepage": "http://BOSHAzureCIP",
  "identifierUris": [
    "http://BOSHAzureCPI"
  ],
  "objectId": "f3884df4-7d1d-4894-a78c-c1fe75750436",
  "objectType": "Application",
  "replyUrls": []
}
```

Step 4: Create and Configure a Service Principal

1. To create a service principal, run `az ad sp create --id YOUR-APPLICATION-ID`, replacing `YOUR-APPLICATION-ID` with the `APPLICATION_ID` you recorded in the [previous step](#):

```
$ az ad sp create --id YOUR-APPLICATION-ID
{
  "appId": "5c552e8f-b977-45f5-a50b-981cfe17cb9d",
  "displayName": "Service Principal for BOSH",
  "objectId": "cc13c685-4c3b-461e-ae96-7a0563960b83",
  "objectType": "ServicePrincipal",
  "servicePrincipalNames": [
    "5c552e8f-b977-45f5-a50b-981cfe17cb9d",
    "http://BOSHAzureCPI"
  ]
}
```

2. You must have the Contributor role on your service principal to deploy Ops Manager to Azure. To assign the Contributor role on your service principal, run the following command:

```
$ az role assignment create --assignee "SERVICE-PRINCIPAL-NAME" \
--role "Contributor" --scope /subscriptions/SUBSCRIPTION-ID
```

- For `SERVICE-PRINCIPAL-NAME`, use any value of `Service Principal Names` from the output above, such as `YOUR-APPLICATION-ID`.
- For `SUBSCRIPTION-ID`, use the ID of the default subscription that you recorded in [Step 2](#).



Note: If you need to use multiple resource groups for your deployment on Azure, you can define custom roles for your Service Principal. These roles allow BOSH to deploy to pre-existing network resources outside of the resource group. For more information, see [Multiple Resource Group Deployment](#) in *Reference Architecture for Pivotal Cloud Foundry on Azure* in the Pivotal documentation.

For more information about Azure Role-Based Access Control, refer to the [RBAC: Built-in roles](#) topic in the Azure documentation.

3. Verify the assignment by running the following command:

```
$ az role assignment list --assignee "SERVICE-PRINCIPAL-NAME"
[
  {
    "id": "/subscriptions/995b7eed-77ef-45ff-a5c9-1a405ffb8243/providers/Microsoft.Authorization/roleAssignments/32e644cf-ba1a-4f43-bf7c-68b4583e463",
    "name": "32e644cf-ba1a-4f43-bf7c-68b4583e463",
    "properties": {
      "principalId": "cc13c685-4c3b-461e-ae96-7a0563960b83",
      "principalName": "http://BOSHAzureCPI",
      "roleDefinitionId": "/subscriptions/995b7eed-77ef-45ff-a5c9-1a405ffb8243/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c",
      "roleDefinitionName": "Contributor",
      "scope": "/subscriptions/995b7eed-77ef-45ff-a5c9-1a405ffb8243"
    },
    "type": "Microsoft.Authorization/roleAssignments"
  }
]
```

Step 5: Verify Your Service Principal

To verify your service principal, log in to your service principal with your `APPLICATION_ID`, `CLIENT_SECRET`, and `TENANT_ID`.

```
$ az login --username APPLICATION_ID --password CLIENT_SECRET \
--service-principal --tenant TENANT_ID
[
  {
    "cloudName": "AzureCloud",
    "id": "995b7eed-77ef-45ff-a5c9-1a405ffb8243",
    "isDefault": true,
    "name": "CF-Docs",
    "state": "Enabled",
    "tenantId": "29248f74-371f-4db2-9a50-c62a6877a0c1",
    "user": {
      "name": "5c552e8f-b977-45f5-a50b-981cfe17cb9d",
      "type": "servicePrincipal"
    }
  }
]
```

If you cannot log in, the service principal is invalid. Create a new service principal and try again.

Step 6: Perform Registrations

1. Register your subscription with Microsoft.Storage:

```
$ az provider register --namespace Microsoft.Storage
```

2. Register your subscription with Microsoft.Network:

```
$ az provider register --namespace Microsoft.Network
```

3. Register your subscription with Microsoft.Compute:

```
$ az provider register --namespace Microsoft.Compute
```

Next Steps

After you complete this topic, continue to one of the following topics:

- [Launching a BOSH Director Instance on Azure using Terraform](#): Perform the procedures in this topic to deploy BOSH Director using Terraform. Pivotal recommends using Terraform.
- [Launching a BOSH Director Instance with an ARM Template](#) [↗](#): Perform the procedures in this topic to deploy BOSH Director with an Azure Resource Manager (ARM) template.
- [Deploying Ops Manager on Azure Manually](#): Perform the procedures in this topic to deploy Ops Manager manually.

Deploying Ops Manager on Azure Manually

This topic describes how to deploy Ops Manager on Azure by using individual commands to create resources. Pivotal recommends this manual procedure for deploying to Azure China, Azure Germany, and Azure Government Cloud.

As an alternative to this procedure, you can use an Azure Resource Manager (ARM) template to create resources automatically. For information about using the ARM template, see the [Deploying BOSH and Ops Manager to Azure with ARM](#) topic.

Before you perform the procedures in this topic, you must have completed the procedures in [Preparing to Deploy Ops Manager on Azure Manually](#). After you complete the procedures in this topic, follow the instructions in [Configuring BOSH Director on Azure](#).

Note: If you are deploying BOSH and Ops Manager on Azure Stack, complete the procedures in [Install and configure CLI for use with Azure Stack](#) in the Microsoft documentation before following the procedures in this topic.

Note: The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

Step 1: Create Network Resources

To create network resources for your deployment, do the following:

1. Navigate to the Azure portal, click **Resource groups**, and click **Add** to create a new resource group for your deployment.
2. Enter a **Resource group name**, select your **Subscription**, and select a **Resource group location**. Click **Create**.
3. Export the name of your resource group as the environment variable `$RESOURCE_GROUP`.

```
$ export RESOURCE_GROUP="YOUR-RESOURCE-GROUP-NAME"
```

Note: If you are on a Windows machine, you can use `set` instead of `export`.

4. Export your location. For example, `westus`.

```
$ export LOCATION=westus
```

For a list of available locations, run `az account list-locations`.

5. Create a network security group named `pcf-nsg`.

```
$ az network nsg create --name pcf-nsg \
--resource-group $RESOURCE_GROUP \
--location $LOCATION
```

6. Add network security group rules to the `pcf-nsg` group to allow traffic to known ports from the public Internet.

```
$ az network nsg rule create --name ssh \
--nsg-name pcf-nsg --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 100 \
--destination-port-range '22'
```

```
$ az network nsg rule create --name http \
--nsg-name pcf-nsg --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 200 \
--destination-port-range '80'
```

```
$ az network nsg rule create --name https \
--nsg-name pcf-nsg --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 300 \
--destination-port-range '443'
```

```
$ az network nsg rule create --name diego-ssh \
--nsg-name pcf-nsg --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 400 \
--destination-port-range '2222'
```

- To block traffic from the public Internet, append `--source-address-prefixes AzureLoadBalancer` to allow traffic from only the Azure load balancer or `--source-address-prefixes VirtualNetwork` to only allow traffic from the virtual network.
- To allow traffic from both the Azure load balancer and the virtual network, create duplicates of each rule, one specifying `--source-address-prefixes AzureLoadBalancer` and one specifying `--source-address-prefixes VirtualNetwork`.

7. Create a network security group named `opsmgr-nsg`.

```
$ az network nsg create --name opsmgr-nsg \
--resource-group $RESOURCE_GROUP \
--location $LOCATION
```

8. Add a network security group rule to the `opsmgr-nsg` group to allow HTTP traffic to the Ops Manager VM.

```
$ az network nsg rule create --name http \
--nsg-name opsmgr-nsg --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 100 \
--destination-port-range 80
```

9. Add a network security group rule to the `opsmgr-nsg` group to allow HTTPS traffic to the Ops Manager VM.

```
$ az network nsg rule create --name https \
--nsg-name opsmgr-nsg --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 200 \
--destination-port-range 443
```

10. Add a network security group rule to the `opsmgr-nsg` group to allow SSH traffic to the Ops Manager VM.

```
$ az network nsg rule create --name ssh \
--nsg-name opsmgr-nsg --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 300 \
--destination-port-range 22
```

- To block traffic from the public Internet, append `--source-address-prefixes AzureLoadBalancer` to allow traffic from only the Azure load balancer or `--source-address-prefixes VirtualNetwork` to only allow traffic from the virtual network.
- To allow traffic from both the Azure load balancer and the virtual network, create duplicates of each rule, one specifying `--source-address-prefixes AzureLoadBalancer` and one specifying `--source-address-prefixes VirtualNetwork`.
- Optionally, if you want to use private IP ranges with Ops Manager and allow all internal traffic, you can create the Network Security Groups to allow all internal traffic.

```
$ az network nsg rule create --name internal-virtual-network \
--nsg-name internal-traffic --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 100 \
--destination-port-ranges '*' \
--source-address-prefixes VirtualNetwork
$ az network nsg rule create --name internal-from-lb \
--nsg-name internal-traffic --resource-group $RESOURCE_GROUP \
--protocol Tcp --priority 110 \
--destination-port-range *
--source-address-prefixes AzureLoadBalancer
```

11. Create a virtual network named `pcf-virtual-network`.

```
$ az network vnet create --name pcf-virtual-network \
--resource-group $RESOURCE_GROUP --location $LOCATION \
--address-prefixes 10.0.0/16
```

12. Add subnets to the network for Ops Manager, BOSH director, and the VMs for your runtime, and attach the Network Security Group.


```
$ az network vnet subnet create --name infrastructure \
--vnet-name pcf-virtual-network \
--resource-group $RESOURCE_GROUP \
--address-prefix 10.0.4.0/26 \
--network-security-group pcf-nsg
$ az network vnet subnet create --name pas \
--vnet-name pcf-virtual-network \
--resource-group $RESOURCE_GROUP \
--address-prefix 10.0.12.0/22 \
--network-security-group pcf-nsg
$ az network vnet subnet create --name services \
--vnet-name pcf-virtual-network \
--resource-group $RESOURCE_GROUP \
--address-prefix 10.0.8.0/22 \
--network-security-group pcf-nsg
```

Step 2: Create BOSH and Deployment Storage Accounts

PCF on Azure uses multiple general-purpose Azure storage accounts. The BOSH and Ops Manager VMs use one main BOSH account, and the other components share five or more deployment storage accounts.

To create storage accounts for BOSH and your deployment, do the following:

1. Choose a name for your BOSH storage account, and export it as the environment variable `STORAGE_NAME`. Storage account names must be globally unique across Azure, between 3 and 24 characters in length, and contain only lowercase letters and numbers.

```
$ export STORAGE_NAME="YOUR-BOSH-STORAGE-ACCOUNT-NAME"
```

2. Create a Standard storage account for BOSH with the following command. This account will be used for BOSH bookkeeping and running the Ops Manager VM itself, but does not have to be used for running any other VMs.

```
$ az storage account create --name $STORAGE_NAME \
--resource-group $RESOURCE_GROUP \
--sku Standard_LRS \
--location $LOCATION
```

 Note: `Standard_LRS` refers to a Standard Azure storage account. The BOSH Director requires table storage to store stemcell information. Azure Premium storage does not support table storage and cannot be used for the BOSH storage account.

If the command fails, ensure you have followed the rules for naming your storage account. Export another new storage account name if necessary.

3. Configure the Azure CLI to use the BOSH storage account as its default.

- a. Retrieve the connection string for the account.

```
$ az storage account show-connection-string \
--name $STORAGE NAME --resource-group $RESOURCE GROUP
```

The command returns output similar to the following:

```
{
  "connectionString": "DefaultEndpointsProtocol=https;EndpointSuffix=core.windows.net;AccountName=cfdocsboshstorage;AccountKey=EXAMPLEEaaaaabbbnrnc5igFxyWsgq016
```

- b. Record the full value of `connectionString` from the output above, starting with and including `DefaultEndpointsProtocol=`.
- c. Export the value of `connectionString` as the environment variable `$CONNECTION_STRING`.

```
$ export CONNECTION_STRING="YOUR-ACCOUNT-KEY-STRING"
```

4. Create three blob containers in the BOSH storage account, named `opsmanager`, `bosh`, and `stemcell`.

```
$ az storage container create --name opsmanager \
--connection-string $CONNECTION_STRING
$ az storage container create --name bosh \
--connection-string $CONNECTION_STRING
$ az storage container create --name stemcell --public-access blob \
--connection-string $CONNECTION_STRING
```

5. Create a table named `stemcells`.

```
$ az storage table create --name stemcells \
--connection-string $CONNECTION_STRING
```

6. Choose a set of unique names for five or more deployment storage accounts. As with the BOSH storage account above, the names must be unique, alphanumeric, lowercase, and 3-24 characters long. The account names must also be sequential or otherwise identical except for the last character. For example: `xyzdeploystorage1`, `xyzdeploystorage2`, `xyzdeploystorage3`, `xyzdeploystorage4`, and `xyzdeploystorage5`.

7. Decide which type of storage to use and run the corresponding command below.



Note: Pivotal recommends five Premium storage accounts, which provides a reasonable amount of initial storage capacity. You can use either Premium or Standard storage accounts, but they have very different scalability metrics. Pivotal recommends creating 1 Standard storage account for every 30 VMs, or 1 Premium storage account for every 150 VMs. You can increase the number of storage accounts later by provisioning more and following the naming sequence.

- To use Premium storage (recommended):

```
$ export STORAGE_TYPE="Premium_LRS"
```

- To use Standard storage:

```
$ export STORAGE_TYPE="Standard_LRS"
```

8. For each deployment storage account you create, do the following:

- a. Create the storage account with the following command, replacing `MY_DEPLOYMENT_STORAGE_X` with one of your deployment storage account names.

```
$ az storage account create --name MY_DEPLOYMENT_STORAGE_X \
--resource-group $RESOURCE_GROUP --sku $STORAGE_TYPE \
--kind Storage --location $LOCATION
```

If the command fails, try a different set of account names.

- b. Retrieve the connection string for the account.

```
$ az storage account show-connection-string \
--name MY_DEPLOYMENT_STORAGE_X --resource-group $RESOURCE_GROUP
```

The command returns output similar to the following:

```
{
  "connectionString": "DefaultEndpointsProtocol=https;EndpointSuffix=core.windows.net;AccountName=cfdoesdeploystorage1;AccountKey=EXAMPLEEaaaaaaQiSAmqj1OoesGh"
}
```

- c. Record the full value of `connectionString` from the output above, starting with and including `DefaultEndpointsProtocol=`.
- d. Create two blob containers named `bosh` and `stemcell` in the account.

```
$ az storage container create --name bosh \
--connection-string $CONNECTION_STRING
```

```
$ az storage container create --name stemcell \
--connection-string $CONNECTION_STRING
```

Step 3: Create Load Balancers

Your load balancer configuration depends on whether you want apps to be available from public IP addresses, private IP addresses, or both.

To create load balancers, do the following:

1. **Required:** PAS Load Balancer

- a. Create a load balancer named `pcf-lb`. A static IP address will be automatically created for Standard SKU load balancers unless specified otherwise with `--public-ip-address-allocation Dynamic`.

```
$ az network lb create --name pcf-lb \
--resource-group $RESOURCE_GROUP --location $LOCATION \
--backend-pool-name pcf-lb-be-pool --frontend-ip-name pcf-lb-fe-ip \
--public-ip-address pcf-lb-ip --public-ip-address-allocation Static \
--sku Standard
```



Note: If the Standard SKU is not available in Azure China, you can use the Basic SKU.

This back end pool is empty when you create it.

- b. Add a probe to the load balancer.

```
$ az network lb probe create --lb-name pcf-lb \
--name http8080 --resource-group $RESOURCE_GROUP \
--protocol Http --port 8080 --path \
```

- c. Add a load balancing rule for HTTP.

```
$ az network lb rule create --lb-name pcf-lb \
--name http --resource-group $RESOURCE_GROUP \
--protocol Tcp --frontend-port 80 \
--backend-port 80 --frontend-ip-name pcf-lb-fe-ip \
--backend-pool-name pcf-lb-be-pool \
--probe-name http8080
```

- d. Add a load balancing rule for HTTPS.

```
$ az network lb rule create --lb-name pcf-lb \
--name https --resource-group $RESOURCE_GROUP \
--protocol Tcp --frontend-port 443 \
--backend-port 443 --frontend-ip-name pcf-lb-fe-ip \
--backend-pool-name pcf-lb-be-pool \
--probe-name http8080
```

- e. (Optional) For private IPs, do the following:

- Create a load balancer named `pcf-lb`.

```
$ az network lb create --name pcf-lb \
--resource-group $RESOURCE_GROUP --location $LOCATION \
--backend-pool-name pcf-lb-be-pool --frontend-ip-name pcf-lb-fe-ip \
--private-ip-address 10.0.0.6 --sku Standard
```

- Add a probe to the load balancer.

```
$ az network lb probe create --lb-name pcf-lb \
--name http8080 --resource-group $RESOURCE_GROUP \
--protocol Http --port 8080
```

- Add a load balancing rule for HTTP.

```
$ az network lb rule create --lb-name pcf-lb \
--name http --resource-group $RESOURCE_GROUP \
--protocol Tcp --frontend-port 80 \
--backend-port 80 --frontend-ip-name pcf-lb-fe-ip \
--backend-pool-name pcf-lb-be-pool \
--probe-name http8080
```

- Add a load balancing rule for HTTPS.

```
$ az network lb rule create --lb-name pcf-lb \
--name https --resource-group $RESOURCE_GROUP \
--protocol Tcp --frontend-port 443 \
--backend-port 443 --frontend-ip-name pcf-lb-fe-ip \
--backend-pool-name pcf-lb-be-pool \
--probe-name http8080
```



Note: If the Standard SKU is not available in Azure China, you can use the Basic SKU.

This back end pool is empty when you create it.

- f. Navigate to your DNS provider and create an entry that points `*.YOUR-SUBDOMAIN` to the public IP address of your load balancer. For example, create an entry that points `azure.example.com` to `198.51.100.1`. You can retrieve it by running the following command:

```
az network public-ip show --name pcf-lb-ip --resource-group $RESOURCE_GROUP
```

2. Optional: Diego SSH Load Balancer

- a. Create a load balancer named `pcf-ssh-lb`.


```
$ az network lb create --name pcf-ssh-lb \
--resource-group $RESOURCE_GROUP --location $LOCATION \
--backend-pool-name pcf-ssh-lb-be-pool --frontend-ip-name pcf-ssh-lb-fe-ip \
--public-ip-address pcf-ssh-lb-ip --public-ip-address-allocation Static \
--sku Standard
```

 **Note:** If the Standard SKU is not available in Azure China, you can use the Basic SKU.

This back end pool is empty when you create it.

- b. (Optional) For private IPs, create a load balancer named `pcf-ssh-lb`.

```
$ az network lb create --name pcf-ssh-lb \
--resource-group $RESOURCE_GROUP --location $LOCATION \
--backend-pool-name pcf-ssh-lb-be-pool --frontend-ip-name pcf-ssh-lb-fe-ip \
--private-ip-address 10.0.0.7 \
--sku Standard
```

 **Note:** If the Standard SKU is not available in Azure China, you can change to use the Basic SKU.

This back end pool is empty when you create it.

- c. Add a probe to the load balancer.

```
$ az network lb probe create --lb-name pcf-ssh-lb \
--name tcp2222 --resource-group $RESOURCE_GROUP \
--protocol Tcp --port 2222
```

- d. Add a load balancing rule for SSH.

```
$ az network lb rule create --lb-name pcf-ssh-lb \
--name diego-ssh --resource-group $RESOURCE_GROUP \
--protocol Tcp --frontend-port 2222 \
--backend-port 2222 --frontend-ip-name pcf-ssh-lb-fe-ip \
--backend-pool-name pcf-ssh-lb-be-pool \
--probe-name tcp2222
```

- e. Navigate to your DNS provider, and create an entry that points `ssh.sys.YOUR-SUBDOMAIN` to the public IP address of your load balancer. For example, create an entry that points `azure.example.com` to `198.51.100.1`. You can retrieve it by running

```
az network public-ip show --name pcf-ssh-lb-ip --resource-group $RESOURCE_GROUP
```

Step 4: Boot Ops Manager


To boot Ops Manager, do the following:

1. Navigate to [Pivotal Network](#) and download the latest release of **Pivotal Cloud Foundry Ops Manager for Azure**.
2. View the downloaded PDF and locate the Ops Manager image URL appropriate for your region.
3. Export the Ops Manager image URL as an environment variable.

```
$ export OPS_MAN_IMAGE_URL="YOUR-OPS-MAN-IMAGE-URL"
```

4. Download the Ops Manager image. For compatibility when upgrading to future versions of Ops Manager, choose a unique name for the image that includes the Ops Manager version number. For example, replace `opsman-image-2.2.x` in the following examples with `opsman-image-2.2.1`.

- If you use unmanaged disks, perform the following steps:

 **Note:** Azure Stack requires unmanaged disks.

1. Download the Ops Manager image to your local machine. The image size is 10 GB.

```
$ wget $OPS_MAN_IMAGE_URL -O opsman-image-2.2.x.vhd
```

2. Upload the image to your storage account using the Azure CLI.

```
$ az storage blob upload --name opsman-image-2.2.x.vhd \
--connection-string $CONNECTION_STRING \
--container-name opsmanager \
--type page \
--file opsman-image-2.2.x.vhd
```

- o If you use managed disks, do the following:

1. Copy the Ops Manager image into your storage account using the Azure CLI.

```
$ az storage blob copy start --source-uri $OPS_MAN_IMAGE_URL \
--connection-string $CONNECTION_STRING \
--destination-container opsmanager \
--destination-blob opsman-image-2.2.x.vhd
```

2. Copying the image may take several minutes. Run the following command and examine the output under `"copy"`:

```
$ az storage blob show --name opsman-image-2.2.x.vhd \
--container-name opsmanager \
--connection-string $CONNECTION_STRING
...
"copy": {
  "completionTime": "2017-06-26T22:24:11+00:00",
  "id": "b9c8b272-a562-4574-baa6-f1a04afcefd1",
  "progress": "53687091712/53687091712",
  "source": "https://opsmanagerwestus.blob.core.windows.net/images/ops-manager-2.2.0.vhd",
  "status": "success",
  "statusDescription": null
},
```

3. Wait a few moments and re-run the command above if `status` is `pending`. When `status` reads `success`, continue to the next step.

5. Create a public IP address named `ops-manager-ip`.

```
$ az network public-ip create --name ops-manager-ip \
--resource-group $RESOURCE_GROUP --location $LOCATION \
--allocation-method Static
{
  "publicIp": {
    "dnsSettings": null,
    "etag": "W/4450ebc2-9e97-4b17-9ef2-44838339c661",
    "id": "/subscriptions/995b7eed-77cf-45ff-a5c9-1a405f1b8243/resourceGroups/cf-docs/providers/Microsoft.Network/publicIPAddresses/ops-manager-ip",
    "idleTimeoutInMinutes": 4,
    "ipAddress": "40.83.148.183",
    "ipConfiguration": null,
    "location": "westus",
    "name": "ops-manager-ip",
    "provisioningState": "Succeeded",
    "publicIpAddressVersion": "IPv4",
    "publicIpAllocationMethod": "Static",
    "resourceGroup": "cf-docs",
    "resourceGuid": "950d4831-1bec-42da-8a79-959becdea9dd",
    "tags": null,
    "type": "Microsoft.Network/publicIPAddresses"
  }
}
```

If you do not want to use a public IP for Ops Manager, skip this step.

6. Record the `ipAddress` from the output above. This is the public IP address of Ops Manager.
7. Create a network interface for Ops Manager.

```
$ az network nic create --vnet-name PCF \
--subnet infrastructure --network-security-group opsmgr-nsg \
--private-ip-address 10.0.4.4 \
--public-ip-address ops-manager-ip \
--resource-group $RESOURCE_GROUP \
--name opsman-nic --location $LOCATION
```

If you do not want use a public IP address for Ops Manager, remove the `--public-ip-address ops-manager-ip` flag and value.

8. Create a keypair on your local machine with the username `ubuntu`. For example, enter the following command:

```
$ ssh-keygen -t rsa -f opsman -C ubuntu
```

When prompted for a passphrase, press the `enter` key to provide an empty passphrase.

9. Create the Ops Manager VM.

- If you are using unmanaged disks, run the following command to create your Ops Manager VM, replacing `PATH-TO-PUBLIC-KEY` with the path to your public key `.pub` file:

```
$ az vm create --name opsman-2.2.x --resource-group $RESOURCE_GROUP \
--location $LOCATION \
--nics opsman-nic \
--image https://$STORAGE_NAME.my-azure-instance.com/opsmanager/opsman-image-2.2.x.vhd \
--os-disk-name opsman-2.2.x-osdisk \
--os-disk-size-gb 128 \
--os-type Linux \
--use-unmanaged-disk \
--storage-account $STORAGE_NAME \
--storage-container-name opsmanager \
--admin-username ubuntu \
--ssh-key-value PATH-TO-PUBLIC-KEY
```

Replace `my-azure-instance.com` with the URL of your Azure instance. Find the complete source URL in the Azure UI by viewing the **Blob properties** of the Ops Manager image you created earlier in this procedure.

- If you are using Azure managed disks, do the following:

1. Create a managed image from the Ops Manager VHD file:

```
$ az image create --resource-group $RESOURCE_GROUP \
--name opsman-image-2.2.x \
--source https://$STORAGE_NAME.blob.core.windows.net/opsmanager/image-2.2.x.vhd \
--location $LOCATION \
--os-type Linux
```


If you are using Azure China, Azure Government Cloud, or Azure Germany, replace `blob.core.windows.net` with the following:

- For Azure China, use `blob.core.chinacloudapi.cn`. See the [Azure documentation](#) for more information.
- For Azure Government Cloud, use `blob.core.usgovcloudapi.net`. See the [Azure documentation](#) for more information.
- For Azure Germany, use `blob.core.cloudapi.de`. See the [Azure documentation](#) for more information.

2. Create your Ops Manager VM, replacing `PATH-TO-PUBLIC-KEY` with the path to your public key `.pub` file.

```
$ az vm create --name opsman-2.2.x --resource-group $RESOURCE_GROUP \
--location $LOCATION \
--nics opsman-nic \
--image opsman-image-2.2.x \
--os-disk-size-gb 128 \
--os-disk-name opsman-2.2.x-osdisk \
--admin-username ubuntu \
--size Standard_DS2_v2 \
--storage-sku Standard_LRS \
--ssh-key-value PATH-TO-PUBLIC-KEY
```

10. If you plan to install more than one tile in this Ops Manager installation, do the following to increase the size of the Ops Manager VM disk. You can repeat this process and increase the disk again at a later time if necessary.

 **Note:** If you use Azure Stack, you must increase the Ops Manager VM disk size using the Azure Stack UI.

- a. Run the following command to stop the VM and detach the disk:

```
$ az vm deallocate --name opsman-2.2.x \
--resource-group $RESOURCE_GROUP
```

- b. Run the following command to resize the disk to 128 GB:

```
$ az disk update --size-gb 128 --name opsman-2.2.x-osdisk \  
--resource-group $RESOURCE_GROUP
```

- c. Run the following command to start the VM:

```
$ az vm start --name opsman-2.2.x --resource-group $RESOURCE_GROUP
```

Step 5: Complete BOSH Director Configuration

To finish configuring BOSH Director, do the following:

1. Navigate to your DNS provider, and create an entry that points a fully qualified domain name (FQDN) to the public IP address of Ops Manager. As a best practice, always use the FQDN to access Ops Manager.
2. Continue to [Configuring BOSH Director on Azure Manually](#).

Configuring BOSH Director on Azure Manually

Page last updated:

This topic describes how to configure the BOSH Director tile within Ops Manager on Azure after [Deploying Ops Manager on Azure Manually](#).

Prerequisites

See the following sections to prepare for configuring BOSH Director on Azure.

General Prerequisites

Before you perform the procedures in this topic, you must have completed the procedures in the following topics:

- [Preparing to Deploy Ops Manager on Azure Manually](#)
- [Deploying Ops Manager on Azure Manually](#)



Note: You can also perform the procedures in this topic using the Ops Manager API. For more information, see the [Using the Ops Manager API](#) topic.

Prerequisites for Azure Stack or Azure Government Cloud

If you are using Azure Stack or Azure Government Cloud, you must set custom VM types for a successful deployment. You can set custom VM types with the Ops Manager API. For more information, see [Using the Ops Manager API](#).

- **For Azure Stack:** The example below may not have up-to-date VM types. For a current list of supported Azure Stack VM types that you can include in your API call, see [Virtual Machine Sizes](#) from the Azure Stack documentation. Include at least one `Standard` VM type.

```
$ curl -k https://YOUR-OPS-MAN-FQDN/api/v0/vm_types -X
PUT -H "Authorization: bearer UAA-ACCESS-TOKEN"
"Content-Type: application/json" -d '{"vm_types":[
{"name":"Standard_DS1_v2","ram":3584,"cpu":1,"ephemeral_disk":51200},
{"name":"Standard_DS2_v2","ram":7168,"cpu":2,"ephemeral_disk":102400},
{"name":"Standard_DS3_v2","ram":14336,"cpu":4,"ephemeral_disk":204800},
{"name":"Standard_DS4_v2","ram":28672,"cpu":8,"ephemeral_disk":409600},
{"name":"Standard_DS5_v2","ram":57344,"cpu":8,"ephemeral_disk":819200},
{"name":"Standard_DS11_v2","ram":14336,"cpu":2,"ephemeral_disk":102400},
{"name":"Standard_DS12_v2","ram":28672,"cpu":4,"ephemeral_disk":204800},
{"name":"Standard_DS13_v2","ram":57344,"cpu":8,"ephemeral_disk":409600},
{"name":"Standard_DS14_v2","ram":114688,"cpu":16,"ephemeral_disk":819200}]}'
```

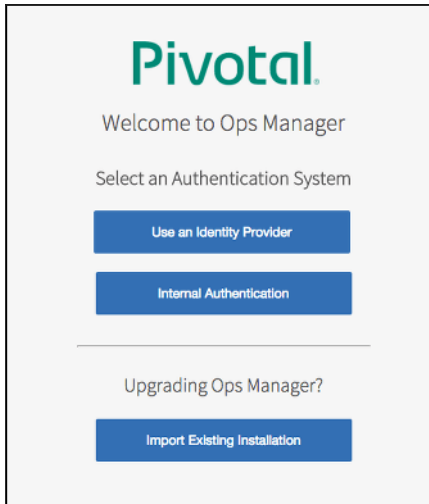
- **For Azure Government:** See the example `curl` command below for your list of VM types.

```
$ curl -k https://YOUR-OPS-MAN-FQDN/api/v0/vm_types -X
PUT -H "Authorization: bearer UAA-ACCESS-TOKEN"
"Content-Type: application/json" -d '{"vm_types":[
{"name": "Standard_D1_v2", "ram": 3584, "cpu": 1, "ephemeral_disk": 51200 },
{"name": "Standard_D2_v2", "ram": 7168, "cpu": 2, "ephemeral_disk": 102400 },
{"name": "Standard_D3_v2", "ram": 14336, "cpu": 4, "ephemeral_disk": 204800 },
{"name": "Standard_D4_v2", "ram": 28672, "cpu": 8, "ephemeral_disk": 409600 },
{"name": "Standard_D5_v2", "ram": 57344, "cpu": 8, "ephemeral_disk": 819200 },
{"name": "Standard_D11_v2", "ram": 14336, "cpu": 2, "ephemeral_disk": 102400 },
{"name": "Standard_D12_v2", "ram": 28672, "cpu": 4, "ephemeral_disk": 204800 },
{"name": "Standard_D13_v2", "ram": 57344, "cpu": 8, "ephemeral_disk": 409600 },
{"name": "Standard_D14_v2", "ram": 114688, "cpu": 16, "ephemeral_disk": 819200 },
{"name": "Standard_F1", "ram": 2048, "cpu": 1, "ephemeral_disk": 16384 },
{"name": "Standard_F2", "ram": 4096, "cpu": 2, "ephemeral_disk": 32768 },
{"name": "Standard_F4", "ram": 8192, "cpu": 4, "ephemeral_disk": 65536 },
{"name": "Standard_F8", "ram": 16384, "cpu": 8, "ephemeral_disk": 131072}]}'
```

To verify that you have successfully set your custom VM types, use the `GET /api/v0/vm_types` Ops Manager API endpoint.

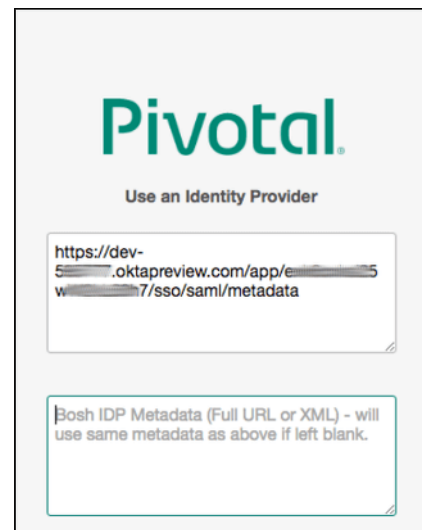
Step 1: Access Ops Manager

1. In a web browser, navigate to the fully qualified domain name (FQDN) of Ops Manager that you set up in either [Deploying BOSH and Ops Manager to Azure with ARM](#) or [Deploying Ops Manager on Azure Manually](#).
2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you use an Identity Provider, an external identity server maintains your user database.
 - [Internal Authentication](#): If you use Internal Authentication, Ops Manager maintains your user database.



Use an Identity Provider (IdP)

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.



2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.



Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a 500 error.




Note: These attributes are case-sensitive.

- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.
5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.
6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

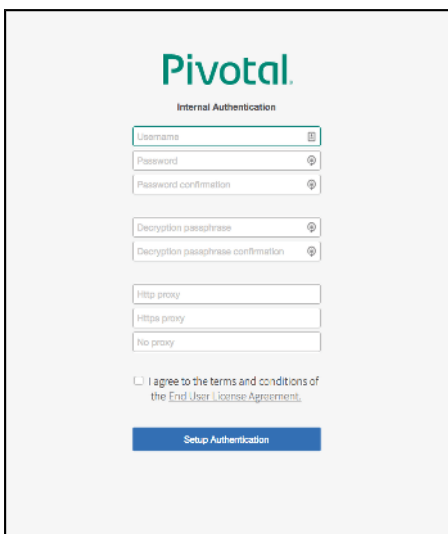
- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

 **Note:** To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

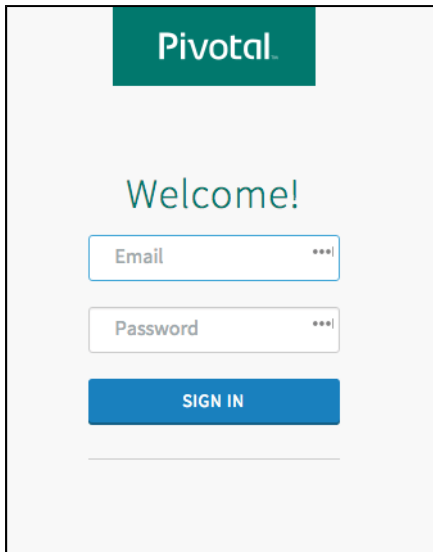
7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.
 - **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
 - **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
 - **Name ID:** Email Address
 - SAML authentication requests are always signed
8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.
 - **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
 - **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
 - **Name ID:** Email Address
 - SAML authentication requests are always signed
9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

Internal Authentication

1. When redirected to the **Internal Authentication** page, do the following:
 - Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
 - Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not recoverable.
 - If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in [Configuring Proxy Settings for the BOSH CPI](#).
 - Read the **End User License Agreement**, and select the checkbox to accept the terms.
 - Click **Setup Authentication**.



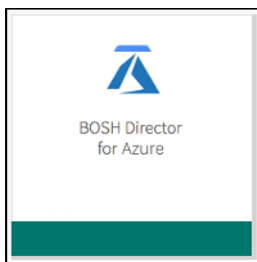
2. Log in to Ops Manager with the Admin username and password that you created in the previous step.



A login form with a light gray background. At the top left is a dark teal rectangle with the word "Pivotal" in white. Below it, the word "Welcome!" is centered in a teal font. Underneath are two input fields: "Email" and "Password", both with placeholder text and a small "xxx|" icon on the right. Below the fields is a blue button with the text "SIGN IN" in white. A thin horizontal line is at the bottom.

Step 2: Azure Config Page

1. Click the **BOSH Director** tile.



2. Select **Azure Config**.

Installation Dashboard
Ops Manager Director

Settings Status Credentials

Azure Config

Director Config

Create Networks

Assign Networks

Security

Syslog

Resource Config

Subscription ID*

Tenant ID*

Application ID*

Client Secret*

Resource Group Name*

BOSH Storage Account Name*

Cloud Storage Type

☒ Use Managed Disks

Storage Account Type

Premium_LRS

☐ Use Storage Accounts

Deployments Storage Account Name

Default Security Group*

SSH Public Key*

SSH Private Key*

Save

- Complete the following fields with information you obtained in [Preparing to Deploy Ops Manager on Azure Manually](#).
 - Subscription ID:** Enter the ID of your Azure subscription.
 - Tenant ID:** Enter your `TENANT_ID`.
 - Application ID:** Enter the `APPLICATION_ID` that you created in the [Create an AAD Application](#) step of *Preparing to Deploy Ops Manager on Azure Manually*.
 - Client Secret:** Enter your `CLIENT_SECRET`.
- Complete the following fields:
 - Resource Group Name:** Enter the name of your resource group, which you exported as the `$RESOURCE_GROUP` environment variable.
 - BOSH Storage Account Name:** Enter the name of your storage account, which you exported as the `$STORAGE_NAME` environment variable.
- For **Cloud Storage Type**, select one of the following options based on your Azure VM storage settings.

- **Use Managed Disks:** Select this option if you use Azure Managed Disks. See [Azure Managed Disks Overview](#) in the Microsoft documentation for more information. For **Storage Account Type**, select the storage option that corresponds with your Azure subscription. Select **Standard_LRS** for HDD-based storage or **Premium_LRS** for SSD-based storage.

- **Use Storage Accounts:** Select this option if you use storage accounts to store your Azure VMs. Enter the base storage name that you used to create your deployment storage accounts, prepended and appended with the wildcard character `*`. For example, if you created accounts named `xyzdeploymentstorage1`, `xyzdeploymentstorage2`, and `xyzdeploymentstorage3`, enter `*deploymentstorage*`. Ops Manager requires that you specify an asterisk at both the beginning and the end of the base storage account name.

Warning: You can update your deployment from using storage accounts to using managed disks. However, after you select **Use Managed Disks** and deploy Ops Manager, you cannot change your deployment back to use storage accounts.

6. (Optional) Enter your **Default Security Group**. For more information about Network Security Groups, see [Filter network traffic with network security groups](#) in Microsoft Azure's documentation.

Note: The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

7. For **SSH Public Key**, copy and paste the contents of your public key in the `opsman.pub` file. You created this file in either [Deploying BOSH and Ops Manager to Azure with ARM](#) topic or [Deploying Ops Manager on Azure Manually](#).
8. For **SSH Private Key**, copy and paste the contents of your private key in the `opsman` file.
9. For **Azure Environment**, select the Azure cloud you want to use. Pivotal recommends **Azure Commercial Cloud** for most Azure environments.

Note: If you selected Azure Stack or Azure Government Cloud as your Azure environment, you must set custom VM types. For more information, see [Prerequisites for Azure Stack or Azure Government Cloud](#) in *Configuring BOSH Director on Azure Manually*.

10. (Optional) If you selected `Azure Stack` for your **Azure Environment**, complete the following Azure Stack-only fields:
 - a. For **Domain**, enter the domain for your Azure Stack deployment. For example, `local.azurestack.external`.
 - b. Enter the **Tenant Management Resource Endpoint** from your AzureRM Environment Context. This URL changes with every ASDK installation.
 - c. Enter `AzureAD` for **Authentication**. If you want to use Azure China Cloud Active Directory for your authentication type, enter `AzureChinaCloudAD`.
 - d. Enter your **Azure Stack Endpoint Prefix**. For example, `management`.
 - e. Enter your **Azure Stack CA Certificate**. Azure Stack requires a custom CA certificate. Copy the certificate from your Azure Stack environment.
11. Click **Save**.

Step 3: Director Config Page

1. Select **Director Config**.

Director Config

NTP Servers (comma delimited)*

JMX Provider IP Address

Bosh HM Forwarder IP Address

☐ Enable VM Resurrector Plugin

☐ Enable Post Deploy Scripts

☐ Recreate all VMs


This will force BOSH to recreate all VMs on the next deploy. Persistent disk will be preserved

☐ Enable bosh deploy retries


This will attempt to re-deploy a failed deployment up to 5 times.

☐ Keep Unreachable Director VMs


- In the **NTP Servers (comma delimited)** field, enter a comma-separated list of valid NTP servers.

 **Note:** The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify the value of this field.

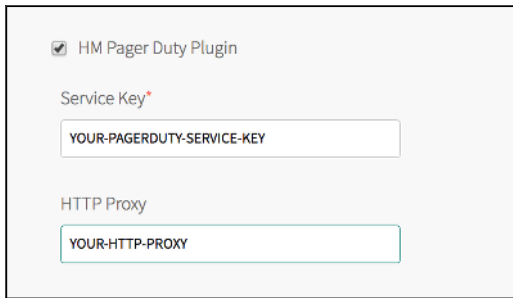
- Leave the **JMX Provider IP Address** field blank.

 **Note:** BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use PCF JMX Bridge for consuming them outside of the Firehose, you may receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank.

- Leave the **Bosh HM Forwarder IP Address** field blank.

 **Note:** BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use the BOSH HM Forwarder for consuming them, you may receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank.

- Select the **Enable VM Resurrector Plugin** checkbox to enable the Ops Manager Resurrector functionality and increase PAS availability.
- Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.
- Select **Recreate all VMs** to force BOSH to recreate all VMs on the next deploy. This process does not destroy any persistent disk data.
- Select **Enable bosh deploy retries** if you want Ops Manager to retry failed BOSH operations up to five times.
- (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS secure communications.
- Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.
- (Optional) Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.



☒ HM Pager Duty Plugin

Service Key*

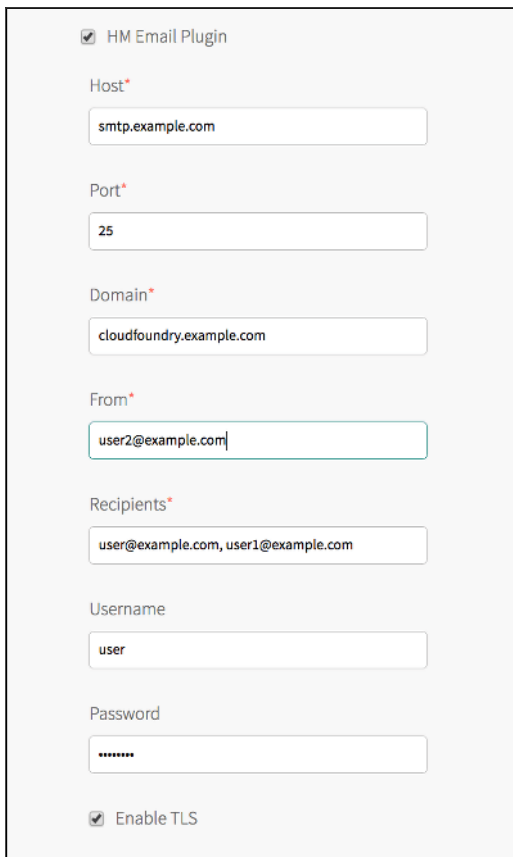
YOUR-PAGERDUTY-SERVICE-KEY

HTTP Proxy

YOUR-HTTP-PROXY

- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.

12. (Optional) Select **HM Email Plugin** to enable Health Monitor integration with email.



☒ HM Email Plugin

Host*

smtp.example.com

Port*

25

Domain*

cloudfoundry.example.com

From*

user2@example.com

Recipients*

user@example.com, user1@example.com

Username

user


Password

☒ Enable TLS

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma-separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter the password for your email server.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

13. For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

 **Note:** After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*


HSM Port Address*

Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**
 9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal

☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature

☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- o **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- o **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. Follow the procedures in [Sign up for Amazon S3](#) and [Creating a Bucket](#) in the AWS documentation. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.

- **GCS Blobstore:** Select this option to use an external GCS endpoint. To create a GCS bucket, you must have a GCS account. Follow the procedures in [Creating Storage Buckets](#) in the GCS documentation to create a GCS bucket. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Follow the steps in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually* to download a JSON file with a private key. Enter the contents of the JSON file into the field.

Database Location

☒ Internal

☐ External MySQL Database

Host*

Port*


Username*

Password*

Database*

15. For **Database Location**, Pivotal recommends that you keep **Internal** selected. In addition, if you selected **External MySQL Database**, you can fill out the following optional fields:

- **Enable TLS:** Selecting this checkbox enables TLS communication between the BOSH Director and the database.
- **TLS CA:** Enter the Certificate Authority for the TLS Certificate.
- **TLS Certificate:** Enter the client certificate for mutual TLS connections to the database.
- **TLS Private Key:** Enter the client private key for mutual TLS connections to the database.
- **Advanced DB Connection Options:** If you would like to provide additional options for the database, use this field to provide a JSON-formatted options string.

 **Note:** You must select **Enable TLS for Director Database** to configure the TLS-related fields.

16. (Optional) **Director Workers** sets the number of workers available to execute Director tasks. This field defaults to `5`.
17. (Optional) **Max Threads** sets the maximum number of threads that the BOSH Director can run simultaneously. Pivotal recommends that you leave the field blank to use the default value unless doing so results in rate limiting or errors on your IaaS.
18. (Optional) To add a custom URL for your BOSH Director, enter a valid hostname in **Director Hostname**. You can also use this field to configure [a](#)

[load balancer in front of your BOSH Director](#).

⚠ warning: In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, VMs become unavailable. This causes downtime. To restore VM availability, enable **Recreate All VMs** and redeploy. This issue is resolved in [Ops Manager v2.2.8](#) and later.

Director Workers

Max Threads

Director Hostname

19. (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.
20. (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.

⚡ Breaking Change: Do not disable BOSH DNS without consulting Pivotal Support.

21. (Optional) To set a custom banner that users see when logging in to the Director using SSH, enter text in the **Custom SSH Banner** field.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

22. (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1, hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.

💡 Note: Azure has limited space for identification tags. Pivotal recommends entering no more than five tags.

23. Click **Save**.

Step 4: Create Networks Page

In this procedure, you create three networks.


Create the Infrastructure Network

1. Select **Create Networks**.
2. Click **Add Network**.
3. Select **Enable ICMP checks** if you want to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.

4. For **Name**, enter the name of the network you want to create. For example, `infrastructure`.

5. Under **Subnets**, complete the following fields:

- **Azure Network Name:** Enter `pcf-virtual-network/pcf-infrastructure-subnet`. You can use either the `NETWORK-NAME/SUBNET-NAME` format or the `RESOURCE-GROUP/NETWORK-NAME/SUBNET-NAME` format. If you specify a resource group, it must exist under the same subscription ID you provided in the [Azure Config Page](#).

 **Note:** The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

- **CIDR:** Enter `10.0.4.0/26`.
- **Reserved IP Ranges:** Enter the first nine IP addresses of the subnet. For example, `10.0.4.1-10.0.4.9`.
- **DNS:** Enter `168.63.129.16`.
- **Gateway:** Enter the first IP address of the subnet. For example, `10.0.4.1`.

Create Networks

Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future.
Contact Pivotal support for help completing such a change.


Verification Settings

☐ Enable ICMP checks

Networks

[Add Network](#)

One or many IP ranges upon which your products will be deployed

▼ infrastructure 

Name*

infrastructure

Subnets

[Add Subnet](#)

Azure Network Name*

pcf-virtual-network/pcf-infrastructure-subn

CIDR*

10.0.4.0/26

Reserved IP Ranges

10.0.4.1-10.0.4.9


DNS*

168.63.129.16

Gateway*

10.0.4.1

6. Click **Save**.

 **Note:** After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

Create the Deployment Network

1. Click **Add Network**.
2. Select **Enable ICMP checks** if you want to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
3. For **Name**, enter the name of the network you want to create. For example, `pas`.
4. Under **Subnets**, complete the following fields:

- **Azure Network Name:** Enter `pcf-virtual-network/pcf-pas-subnet`. You can use either the `NETWORK-NAME/SUBNET-NAME` format or the `RESOURCE-GROUP/NETWORK-NAME/SUBNET-NAME` format. If you specify a resource group, it must exist under the same subscription ID you provided in the [Azure Config Page](#).

Note: The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

- **CIDR:** Enter `10.0.12.0/22`.
- **Reserved IP Ranges:** Enter the first nine IP addresses of the subnet. For example, `10.0.12.1-10.0.12.9`.
- **DNS:** Enter `168.63.129.16`.
- **Gateway:** Enter the first IP address of the subnet. For example, `10.0.12.1`.

The screenshot shows the 'Add Subnet' form in the Azure portal. The form is titled 'pas' and contains the following fields and values:

- Name:** pas
- Subnets:** (Section header)
- Azure Network Name:** pcf-virtual-network/pcf-pas-subnet
- CIDR:** 10.0.12.0/22
- Reserved IP Ranges:** 10.0.12.1-10.0.12.9
- DNS:** 168.63.129.16
- Gateway:** 10.0.12.1

An 'Add Subnet' button is located on the right side of the form.

5. Click **Save**.

Create the Services Network

1. Click **Add Network**.
2. Select **Enable ICMP checks** if you want to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
3. For **Name**, enter the name of the network you want to create. For example, `services`.
4. Under **Subnets**, complete the following fields:

- **Azure Network Name:** Enter `pcf-virtual-network/pcf-services-subnet`. You can use either the `NETWORK-NAME/SUBNET-NAME` format or the `RESOURCE-GROUP/NETWORK-NAME/SUBNET-NAME` format. If you specify a resource group, it must exist under the same subscription ID you provided in the [Azure Config Page](#).

Note: The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

- o **CIDR:** Enter `10.0.8.0/22`.
- o **Reserved IP Ranges:** Enter the first nine IP addresses of the subnet. For example, `10.0.8.1-10.0.8.9`.
- o **DNS:** Enter `168.63.129.16`.
- o **Gateway:** Enter the first IP address of the subnet. For example, `10.0.8.1`.

▼ services

Name*

services

Subnets

Add Subnet

Azure Network Name*

pcf-virtual-network/pcf-services-subnet

CIDR*

10.0.8.0/22

Reserved IP Ranges

10.0.8.1-10.0.8.9

DNS*

168.63.129.16

Gateway*

10.0.8.1

5. Click **Save**. If you do not have **Enable ICMP checks** selected, you may see red warnings which you can safely ignore.

Step 5: Assign Networks Page

1. Select **Assign Networks**.

Network Assignments

Network

infrastructure

Save

2. Under **Network**, select the `infrastructure` network that you created from the dropdown.
3. Click **Save**.

Step 6: Security Page

Security

Trusted Certificates

-----BEGIN CERTIFICATE-----
TH[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

These certificates enable BOSH-deployed components to trust a custom root certificate.

Generate VM passwords or use single password for all VMs

- ☒ Generate passwords
- ☐ Use default BOSH password

Save

1. Select **Security**.
2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:

```

-----BEGIN CERTIFICATE-----
ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678AB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BCDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABBB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----

```

 Note: If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#) for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 7: Syslog Page

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
 ☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save

- (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
- In the **Address** field, enter the IP address or DNS name for the remote server.
- In the **Port** field, enter the port number that the remote server listens on.
- In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
- (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
 - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
- Click **Save**.

Step 8: Resource Config Page


- Select **Resource Config**.


Resource Config


| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|------------------------|--------------|----------------------|---|----------------|--------------------------|
| Ops Manager Director | Automatic: 1 | Automatic: 50 GB | Automatic: Standard_DS2_v2 (cpu: 2, ram | | <input type="checkbox"/> |
| Master Compilation Job | Automatic: 4 | None | Automatic: Standard_F4s (cpu: 4, ram: 8 G | | <input type="checkbox"/> |

Save


2. Ensure that the **Internet Connected** checkboxes are deselected for all jobs.
3. Adjust any values as necessary for your deployment. Under the **Instances**, **Persistent Disk Type**, and **VM Type** fields, choose **Automatic** from the dropdown to allocate the recommended resources for the job. If the **Persistent Disk Type** field reads **None**, the job does not require persistent disk space.

 **Note:** Ops Manager requires a Director VM with at least 8 GB memory.

 **Note:** If you set a field to **Automatic** and the recommended resource allocation changes in a future version, Ops Manager automatically uses the updated recommended allocation.

 **Note:** If you install PAS for Windows, provision your **Master Compilation Job** with at least 100 GB of disk space.

4. (Optional) For **Load Balancers**, enter your Azure application gateway name for each associated job. To create an application gateway, follow the procedures in [Configure an application gateway for SSL offload by using Azure Resource Manager](#) from the Azure documentation. When you create the application gateway, associate the gateway's IP address with your system domain.

 **warning:** This feature is not recommended for production use. The Azure load balancer does not support an override port in the healthcheck configuration.

5. Click **Save**.

Step 9: (Optional) Add Custom VM Extensions

Use the Ops Manager API to add custom properties to your VMs such as associated security groups and load balancers. For more information, see [Managing Custom VM Extensions](#).

Step 10: Complete the BOSH Director Installation

1. Click **Apply Changes**. If a red ICMP error message appears and you have disabled ICMP, click **Ignore errors and start the install**.
2. BOSH Director installs. This may take a few moments. When the installation process successfully completes, the **Changes Applied** window appears.
3. Click the **Installation Dashboard** link to return to the Installation Dashboard.

Next Steps

- (Optional) When Ops Manager finishes deploying, deploy BOSH Add-ons to your system. For more information, see [Deploying BOSH Add-Ons](#).
- Install one or more PCF runtime environments to complete your installation. For more information, see [Installing Runtimes](#).

Deploying PAS on Azure

Page last updated:

This topic describes how to install and configure Pivotal Application Service (PAS) on Azure.

Before you perform the procedures in this topic, you must have completed the procedures in the following topics:

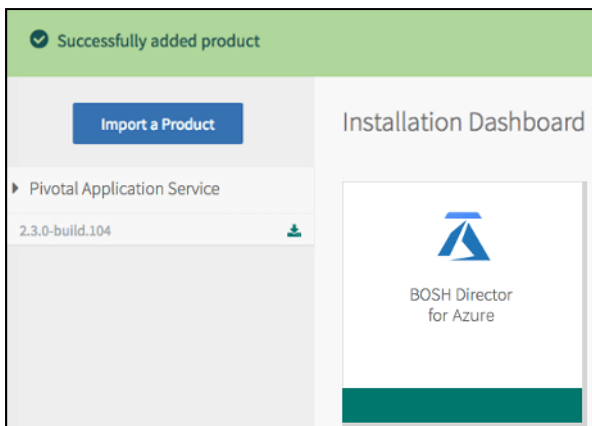
1. [Preparing to Deploy Ops Manager on Azure Manually](#)
2. [Deploying Ops Manager on Azure Manually](#)
3. [Configuring BOSH Director on Azure Manually](#)

Note: If you plan to [install the PCF IPsec add-on](#), you must do so before installing any other tiles. Pivotal recommends installing IPsec immediately after Ops Manager, and before installing the Pivotal Application Service (PAS) tile.

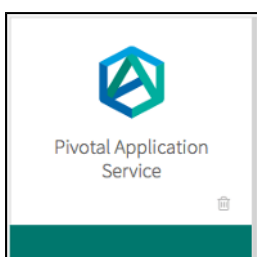
Note: The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

Step 1: Add PAS to Ops Manager

1. If you have not already downloaded PAS, log in to [Pivotal Network](#), and click on PAS.
2. From the **Releases** drop-down, select the release to install and choose one of the following:
 - a. Click PAS to download the PAS `.pivotal` file.
 - b. Click **PCF Small Footprint PAS** to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).
3. Navigate to the Ops Manager Installation Dashboard.
4. Click **Import a Product** and select the downloaded `.pivotal` file. For more information, refer to the [Adding and Deleting Products](#) topic.
5. Click the plus button next to the imported tile to add it to the Installation Dashboard.

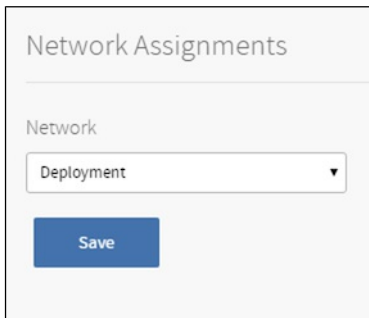


6. Click the PAS tile in the Installation Dashboard.



Step 2: Assign Networks

1. Select **Assign Networks**.
2. From the **Network** dropdown, select the network on which you want to run PAS.



Network Assignments

Network

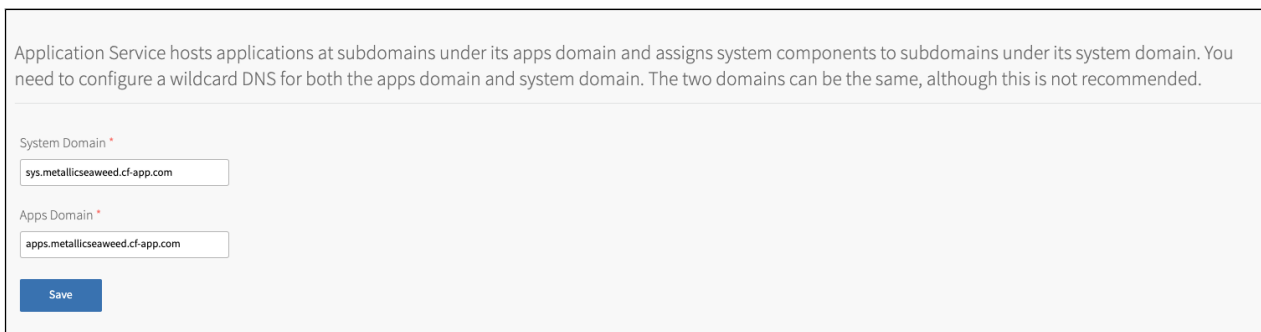
Deployment

Save

3. Click **Save**.

Step 3: Configure Domains

1. Select **Domains**.



Application Service hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain *

sys.metallicseaweed.cf-app.com

Apps Domain *

apps.metallicseaweed.cf-app.com

Save

2. Enter the system and application domains.
 - The **System Domain** defines your target when you push apps to PAS. For example, `system.example.com`.
 - The **Apps Domain** defines where PAS should serve your apps. For example, `apps.example.com`.

Note: Pivotal recommends that you use the same domain name but different subdomain names for your system and app domains. Doing so allows you to use a single wildcard certificate for the domain while preventing apps from creating routes that overlap with system routes.

3. Navigate to your DNS provider to create A records that point from your wildcard system and apps domains to the public IP address of your load balancer. For example, if the IP address of your load balancer is 198.51.100.1, then create an A record that points `*.system.example.com` to that address and another A record that points `*.apps.example.com` to that address.

Note: To retrieve the IP address of your load balancer, navigate to the Azure portal, click **All resources**, and click the **Public IP address** resource that ends with `pcf-lb-ip`.

4. Click **Save**.

Step 4: Configure Networking

1. Select **Networking**.
2. Leave the **Router IPs**, **SSH Proxy IPs**, **HAProxy IPs**, and **TCP Router IPs** fields blank. You do not need to complete these fields when deploying PCF to Azure.

Note: You specify load balancers in the **Resource Config** section of PAS later on in the installation process. See the [Configuring Resources](#) section.

3. Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate and Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.
 - a. Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

Certificates and Private Keys for HAProxy and Router Add

▼ example-cert 🗑️

Name *

example-cert A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

```
-----BEGIN CERTIFICATE-----
MIIE...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```

[Generate RSA Certificate](#)

▼ example-cert-2 🗑️

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager.

- b. If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see *Configure Front End* in [Preparing to Deploy Ops Manager on GCP Manually](#).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

4. (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Router** field, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

- ☐ TLSv1.0
- ☐ TLSv1.1
- ☒ TLSv1.2

- Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

- ☒ Log client IPs
- ☐ Disable logging of X-Forwarded-For header only
- ☐ Disable logging of both source IP and X-Forwarded-For header
- To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.

- Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.



Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

- ☒ TLS terminated for the first time at infrastructure load balancer
- ☐ TLS terminated for the first time at HAProxy
- ☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|---|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to | TLS terminated for | HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header. |

| | | |
|--|--|---|
| <ul style="list-style-type: none"> the instances of HAProxy, and HAProxy instance count is > 0 | the first time at HAProxy. |  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | TLS terminated for the first time at the Gorouter. | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |


For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).

- To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

- ☒ HAProxy does not request client certificates.
- ☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.


 **warning:** Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

- To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

 **warning:** Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client**


Certificate Validation in the Networking pane.

- In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.


 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:
`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384` If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable

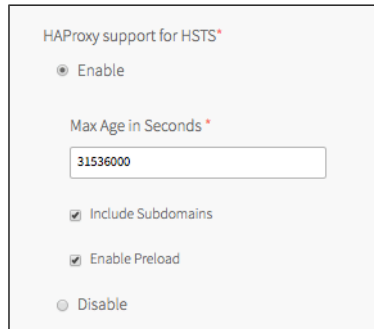
◦ Enable HAProxy forwarding of requests to Router over TLS

| If you want to: | Encrypt communication between HAProxy and the Gorouter |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

◦ Disable HAProxy forwarding of requests to Router over TLS

| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |

13. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field and complete



HAProxy support for HSTS*

☒ Enable

Max Age in Seconds*

31536000

☒ Include Subdomains


☒ Enable Preload

☐ Disable

the following optional configuration steps:

- (Optional) Enter a **Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
- (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
- (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from HAProxy.

- If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

- (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

- (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
- (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
- (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
- By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#)

- (Optional) By default, Gorouter support for the PROXY protocol is disabled. To enable the PROXY protocol, select **Enable support for PROXY protocol in CF Router**. When enabled, client-side load balancers that terminate TLS but do not support HTTP can pass along information from the originating client. Enabling this option may impact Gorouter performance. For more information about enabling the PROXY protocol in Gorouter, see the *HTTP Header Forwarding* sections in the [Securing Traffic in Cloud Foundry](#) topic.
- In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details.
 - If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
- (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is


Max Connections Per Backend *

500

23. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router *
☒ Enable
☐ Disable

24. (Optional) Increase the number of seconds in the **Router Timeout to Backends** field to accommodate larger uploads over connections with high latency. Set this value to less than or equal to the idle timeout value of the Azure load balancer, which defaults to 4 minutes.

 **Note:** If the router timeout value exceeds the Azure LB timeout, you may experience intermittent TCP resets. For more information about configuring Azure load balancer idle timeout, see the [Azure documentation](#).

25. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

26. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.

27. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

Load Balancer Healthy Threshold *

28. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP](#)

[headers](#) .

HTTP Headers to Log

29. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

30. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.


HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.


HAProxy Trusted CIDRs

31. The **Loggregator Port** defaults to if left blank. Leave this field blank.


Container Network Interface Plugin*

 Silk


32. For **Container Network Interface Plugin**, ensure **Silk** is selected and review the following fields:

 **Note:** The **External** option exists to support NSX-T integration for vSphere deployments.

- (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to . Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses .

 **warning:** The overlay network IP range must not conflict with any other IP addresses in your network.

- Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to .
- For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to .
- To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- By default, containers use the same DNS servers as the host. If you want to override the DNS servers to be used in containers, enter a comma-separated list of servers in **DNS Servers**.

 **Note:** If your deployment uses BOSH DNS, which is the default, you cannot use this field to override the DNS servers used in containers.

33. For **DNS Search Domains**, enter DNS search domains for your containers as a comma-separated list. DNS on your containers appends these names to its host names, to resolve them into full domain names.

DNS Search Domains

DNS search domains to be used in containers. A comma-separated list can be specified.

34. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is . You may

need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

35. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:

- a. Select **Enable TCP Routing**.
- b. For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. These are the same ports that you configured in the [Pre-Deployment Steps](#) of the *Enabling TCP Routing* topic.
 - To support multiple TCP routes, Pivotal recommends allocating multiple ports.
 - To allocate a list of ports rather than a range:
 1. Enter a single port in the **TCP Routing Ports** field.
 2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time
☒ **Enable TCP Routing**

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

1024-1123

- c. For Azure, you also need to specify the name of Azure load balancer in the LOAD BALANCER column of TCP Router job of the **Resource Config** screen. You configure this later on in PAS. See [Configuring Resources](#).

36. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) [↗](#) topic.

37. Click **Save**.

Step 5: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC

☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888


Docker Images Disk-Cleanup Scheduling on Cell VMs*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) *


10240


- The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.
- The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
- If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
- If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.


- To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting](#) in *HTTP Routing*.

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

 **Warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

7. You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
8. Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
9. Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
10. Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.

 **Note:** In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

11. (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs*

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

12. By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.

13. Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
14. You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is seconds and the maximum configurable timeout is seconds.
15. Click **Save**.

Step 6: Configure Application Developer Controls

1. Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *

Staging Timeout (Seconds) *

☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.
4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.

5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.

Note: If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of seconds you specify in this field.
9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 7: Review Application Security Group

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type ☐ in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 8: Configure UAA

1. Select **UAA**.
2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

3. Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN`.



Note: The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN`.

- If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
M
U
H
M
-----END CERTIFICATE-----

[Change](#)

SAML Service Provider Key Password

Secret

Password.

- (Optional) To override the default value, enter a custom SAML Entity ID in the **SAML Entity ID Override** field. By default, the SAML Entity ID is `http://login.YOUR-SYSTEM-DOMAIN` where `YOUR-SYSTEM-DOMAIN` is set in the **Domains > System Domain** field.
- For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
- (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line Interface (cf CLI) login access and refresh. Most deployments use the defaults.

Apps Manager Access Token Lifetime (in seconds) *

Apps Manager Refresh Token Lifetime (in seconds) *

Cloud Foundry CLI Access Token Lifetime (in seconds) *

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

Global Login Session Max Timeout (in seconds) *


Global Login Session Idle Timeout (in seconds) *

Customize Username Label (on login page) *

Customize Password Label (on login page) *

Proxy IPs Regular Expression *

8. (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:
 - **Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - **Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan
9. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
10. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Gorouter or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
11. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#) for help.

Internal Database Configuration


When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane. See the [Configure Internal Databases](#) section for details.

1. Select **Internal MySQL**.

Choose the location of your UAA database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use AWS RDS)

 **Note:** If you configure your system databases as external in the **Databases** pane, selecting Internal MySQL in the **UAA** pane has no effect.

2. Click **Save**.
3. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

1. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)

☒ External (preferred if, for example, you use AWS RDS)

Hostname *


TCP Port *

Username *


Password *

2. For **Hostname**, enter the hostname of the database server.
3. For **TCP Port**, enter the port of the database server.
4. For **User Account and Authentication database username**, specify a unique username that can access this specific database on the database server.
5. For **User Account and Authentication database password**, specify a password for the provided username.
6. Click **Save**.

Step 9: Configure CredHub

 **Note:** Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

1. Select **CredHub**.
2. Choose the location of your CredHub database. PAS includes this CredHub database for services to store their service instance credentials.

 **Note:** You cannot choose **Internal** for the CredHub database if you choose **External** for your System Databases. See [Configure System](#)

Databases below.

Configure the CredHub Server

Choose the location of your CredHub database *

- ☒ Internal MySQL (preferred for complete high-availability)
- ☐ External (preferred if, for example, you use Google Cloud SQL)

If you chose **External**, enter the following:

- **Hostname.** This is the IP address of your database server.
- **TCP Port.** This is the port of your database server, such as `3306`.
- **Username.** This is a unique username that can access your CredHub database on the database server.
- **Password.** This is the password for the provided username.
- **Database CA Certificate.** This certificate is used when encrypting traffic to and from the database.

3. Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys



Name *

Name of the encryption key.

Provider*

Key *

☐ Primary

- **Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- **Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- **Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- **Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.



Note: For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

4. (Optional) To configure CredHub to use an HSM, complete the following fields:

- **HSM Provider Partition.** This is the name of the HSM provider partition.
- **HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- **HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#) in the

Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

5. If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.

6. Click **Save**.

7. Select the **Resource Config** pane.

8. Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.

9. Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).

Step 10: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *


2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.

3. Click **Save**.

Step 11: Configure System Databases

You can configure PAS to use an internal MySQL database provided with PCF, or you can configure an external database provider for the databases required by PAS.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. Contact Pivotal Support for help. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration

If you want to use internal databases for your deployment, perform the following steps:

1. Select **Databases**.

2. Select one of the **Internal Databases** options:

- **Internal Databases - MySQL - Percona XtraDB Cluster** uses [Percona Server](#) with TLS encryption between server cluster nodes.
- **Internal Databases - MySQL - MariaDB Galera Cluster** uses [MariaDB](#) with cluster nodes communicating over plaintext.

⚠ warning: Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

3. Click **Save**.

Then proceed to [Step 12: \(Optional\) Configure Internal MySQL](#) to configure high availability for your internal MySQL databases.

External Database Configuration

⚠ warning: Protect whichever database you use in your deployment with a password.

To create your Pivotal Application Service (PAS) databases, follow the procedure below.

💡 Note: Exact configurations depend on your database provider. The following procedure uses AWS RDS as an example.

1. Add the `ubuntu` account key pair from your IaaS deployment to your local SSH profile so you can access the Ops Manager VM. For example, in AWS, you add a key pair created in AWS:

```
$ ssh-add aws-keypair.pem
```

2. SSH in to your Ops Manager using the Ops Manager FQDN and the username `ubuntu`:

```
$ ssh ubuntu@OPS-MANAGER-FQDN
```

3. Log in to your MySQL database instance using the appropriate hostname and user login values configured in your IaaS account. For example, to log in to your AWS RDS instance, run the following MySQL command:


```
$ mysql --host=RDSHOSTNAME --user=RDSUSERNAME --password=RDSPASSWORD
```

4. Run the following MySQL commands to create databases for the PAS components that require a relational database:


```
CREATE database ccd;
CREATE database notifications;
CREATE database autoscale;
CREATE database app_usage_service;
CREATE database routing;
CREATE database diego;
CREATE database account;
CREATE database nfsvolume;
CREATE database networkpolicyserver;
CREATE database silk;
CREATE database locket;
CREATE database uaa;
CREATE database credhub;
```

💡 Note: The command `CREATE database credhub;` is optional if you have no CredHub instances. By default, CredHub has `0` instances.

5. Type `exit` to quit the MySQL client, and `exit` again to close your connection to the Ops Manager VM.
6. In PAS, select **Databases**.
7. Select the **External Databases** option.


 **Note:** If you configure databases as external, you cannot configure an internal database in the **UAA** pane.

8. For **Hostname**, enter the hostname of the database server.
9. For **TCP Port**, enter the port of the database server.
10. Each component that requires a relational database has two corresponding fields: one for the database username and one for the database password. For each set of fields, specify a unique username that can access this specific database on the database server and a password for the provided username.

 **Note:** Ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.


11. Click **Save**.

Step 12: (Optional) Configure Internal MySQL

 **Note:** You only need to configure this section if you have selected one of the **Internal Databases - MySQL** options in the **Databases** section.

To use internal MySQL in High Availability configuration, you define a load balancer rule that lets PAS components send queries a single hostname backed by two redundant proxies. Each proxy then directs query traffic to three MySQL server nodes.

1. Allocate an internal load balancer rule to balance traffic between two static IP addresses. The static IP addresses cannot be within the range that that you have reserved for PAS.
The load balancer rule is separate from the software provided by Pivotal, and you need to define it within your infrastructure.
 - **Make your idle time out long enough to not interrupt long-running queries.** When queries take a long time, the load balancer can time out and interrupt the query.
For example, [AWS's Elastic Load Balancer](#) has a default idle timeout of 60 seconds, so queries that take longer than this duration sever the MySQL connection and return an error.
 - **Configure a healthcheck or monitor, using TCP against port 1936.** This defaults to TCP port `1936`, to maintain backwards compatibility with previous releases. This port is not configurable. Unauthenticated healthchecks against port 3306 may cause the service to become unavailable and require manual intervention to fix.
 - **Configure the load balancer to route traffic for TCP port 3306 to the IPs of all proxy instances on TCP port 3306.**
 - Record the hostname of the load balancer rule and the two static IP addresses.

 **warning:** You must configure a load balancer to achieve complete high availability.

2. From the PAS tile in Ops Manager, Select **Internal MySQL**.
3. In the **MySQL Proxy IPs** field, enter the static IP addresses used by the internal MySQL load balancer rule.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.


A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.

The automated backups functionality works with any S3-compatible file store that can receive your backup files.

MySQL Proxy IPs

MySQL Service Hostname

4. For **MySQL Service Hostname**, enter the IP address or hostname for your load balancer. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.
5. In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
6. In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.
7. (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
8. To prohibit the creation of command line history files on the MySQL nodes, disable the **Allow Command History** checkbox.
9. To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

10. For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the default value is 10 seconds.

Replication canary time period *

30

Replication canary read delay *

20

E-mail address (required) *

Fill in your desired email address

☒ Allow Command History

Cluster Probe Timeout

11. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.
12. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.
 - a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.

13. Enter values for the following fields:
 - **Load Balancer Healthy Threshold:** Specifies the amount of time, in seconds, to wait until declaring the MySQL Proxy instance started. This allows an external load balancer time to register the instance as healthy.
 - **Load Balancer Unhealthy Threshold:** Specifies the amount of time, in seconds, that the MySQL Proxy continues to accept connections before shutting down. During this period, the Healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.
14. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.
15. Click **Save**.

For more information on how to monitor the node health of your MySQL Proxy instances, see [Using the MySQL Proxy](#).

Step 13: Configure File Storage

To minimize system downtime, Pivotal recommends using highly resilient and redundant *external* filestores for your Pivotal Application Service (PAS) file storage.

When configuring file storage for the Cloud Controller in PAS, you can select one of the following:

- Internal WebDAV filestore
- External S3-compatible or Ceph-compatible filestore
- External Google Cloud Storage with Access Key and Secret Key
- External Google Cloud Storage with Service Account
- External Azure Cloud Storage

For production-level PCF deployments on Azure, the recommended selection is Azure Storage. For more information about production-level PCF deployments on Azure, see the [Reference Architecture for Pivotal Cloud Foundry on Azure](#).

For more factors to consider when selecting file storage, see [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#).

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External Azure Storage

To use external Azure file storage for your Pivotal Application Service (PAS) filestore, perform the following steps:

1. Select the **External AzureStorage** option.

Configure your Cloud Controller's filesystem*

☐ Internal WebDAV (provided by Elastic Runtime)
 ☐ External S3-Compatible File Store (if you want to use a service like S3 or Ceph)
 ☐ External Google Cloud Storage
 ☒ External Azure Storage

Account Name *

pcfstorageaccount

Access Key *

.....

Buildpacks Container Name *

pcfbuildpacks

Droplets Container Name *

pcfdroplets

Packages Container Name *

pcfpackages

Resources Container Name *

pcfresources

2. To create a new storage account and storage containers for the PAS filestore, perform the following steps.
 - In the Azure Portal, navigate to the **Storage accounts** tab.
 - Click on the plus icon to add a new storage account.
 - In the **Name** field, enter a unique name (all lowercase, 3 to 24 alphanumeric characters) for the storage account.
 - For the **Deployment model**, select **Resource manager**.
 - For **Account kind**, select **General purpose**.

- For **Performance**, select **Standard**.
 - From the **Replication** dropdown, select **Locally-redundant storage (LRS)**.
 - For **Storage service encryption**, select **Disabled**.
 - From the **Subscription** dropdown, select the subscription where you want to deploy PCF resources.
 - For **Resource group**, select **Use existing** and enter the name of the resource group where you deployed PAS.
 - From **Location** the dropdown, select the **Location** where you are deploying PCF.
 - Click **Create**.
 - After the storage account is created, select the new storage account from the dashboard.
 - Navigate to the **Blob Service** section of the storage account, and then click on **Containers** to create one or more containers in this storage account for buildpacks, droplets, resources, and packages.
 - For each container that you create, set the **Access type** to **Private**.
3. In PAS, enter the name of the storage account you created for **Account Name**.
 4. In the **Secret Key** field, enter one of the access keys provided for the storage account. To obtain a value for this fields, visit the Azure Portal, navigate to the **Storage accounts** tab and click on **Access keys**.
 5. For the **Buildpacks Container Name**, enter the container name for storing your app buildpacks.
 6. For **Droplets Container Name**, enter the container name for your app droplet storage. Pivotal recommends that you use a unique container name, but you can use the same container name as the previous step.
 7. For **Resources Container Name**, enter the container name for resources. Pivotal recommends that you use a unique container name, but you can use the same container name as the previous step.
 8. For **Packages Container Name**, enter the container name for packages. Pivotal recommends that you use a unique container name, but you can use the same container name as the previous step.
 9. Click **Save**.


 **Note:** To enable backup and restore of your PAS tile that uses S3 compatible blobstore, see [Enable External Blobstore Backups](#).

Other IaaS Storage Options

[Google Cloud Storage](#) and [External S3-Compatible File Storage](#) are also available as file storage options but are not recommended for typical PCF on Azure installations.

Step 14: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

 **Note:** The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

- ☒ No
☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging


☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration

Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.

 **Note:** The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.



Note: Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 15: (Optional) Customize Apps Manager

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑️
- ▶ Docs 🗑️
- ▶ Tools 🗑️

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

4. Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
5. Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
6. Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
7. Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
8. The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
9. The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 16: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret

Save

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

Note: If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 17: (Optional) Configure App Autoscaler

To use App Autoscaler, you must create an instance of the service and bind it to an app. To create an instance of App Autoscaler and bind it to an app, see [Set Up App Autoscaler](#) in the *Scaling an Application Using App Autoscaler* topic.

- Click **App Autoscaler**.

Configure the App Autoscaler

Autoscaler Instance Count (min: 1) *

Autoscaler API Instance Count (min: 1) *

Metric Collection Interval (min: 60, max: 3600) (min: 60, max: 3600) *

Scaling Interval (min: 15, max: 120) (min: 15, max: 120) *

☐ Verbose Logging

☐ Disable API Connection Pooling

☒ Enable Notifications

Save

- Review the following settings:

- Autoscaler Instance Count:** How many instances of the App Autoscaler service you want to deploy. The default value is `3`. For high availability, set this number to `3` or higher. You should set the instance count to an odd number to avoid split-brain scenarios during leadership elections. Larger environments may require more instances than the default number.
- Autoscaler API Instance Count:** How many instances of the App Autoscaler API you want to deploy. The default value is `1`. Larger environments may require more instances than the default number.
- Metric Collection Interval:** How many seconds of data collection you want App Autoscaler to evaluate when making scaling decisions. The minimum interval is 60 seconds, and the maximum interval is 3600 seconds. The default value is `120`. Increase this number if the metrics you use in your scaling rules are emitted less frequently than the existing Metric Collection Interval.
- Scaling Interval:** How frequently App Autoscaler evaluates an app for scaling. The minimum interval is 15 seconds, and the maximum interval is 120 seconds. The default value is `35`.
- Verbose Logging** (checkbox): Enables verbose logging for App Autoscaler. Verbose logging is disabled by default. Select this checkbox to see more detailed logs. Verbose logs show specific reasons why App Autoscaler scaled the app, including information about minimum and maximum instance limits, App Autoscaler's status. For more information about App Autoscaler logs, see [App Autoscaler Events and Notifications](#).
- Disable API Connection Pooling:** API connection pooling increases performance by reducing the cost associated with establishing new connections. If you do not want to keep connections open for reuse, select this option.

3. Click **Save**.

Step 18: Configure Cloud Controller

1. Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
 ☒ Disable

Save

2. Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

3. CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

4. Click **Save**.

Step 19: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

1. Select **Smoke Tests**.
2. If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

- ☐ Temporary space within the system organization (This is deleted after smoke tests finish.)
- ☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.

Step 20: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

Note: Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.

Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.

Whitelist for non-RFC-1918 Private Networks *

allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.

CF CLI Connection Timeout

15

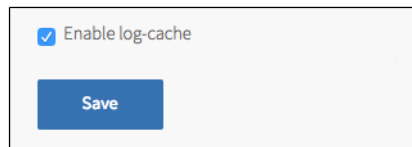
2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PASTopic*.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

⚠ warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 21: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

💡 Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.

- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

💡 Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.


- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.
- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

Step 22: Configure Resources


1. Select **Resource Config**.

| Resource Config | | | | |
|---------------------|--------------|----------------------|---|---------------|
| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCER |
| Consul | Automatic: 3 | Automatic: 1 GB | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| NATS | Automatic: | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| etcd | Automatic: 3 | Automatic: 1 GB | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| File Storage | Automatic: 1 | Automatic: 100 GB | Automatic: Standard_F2s (cpu: 2, ram: 4 GB, disk: 3 | |
| MySQL Proxy | Automatic: | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| MySQL Server | Automatic: 3 | Automatic: 100 GB | Automatic: Standard_DS11_v2 (cpu: 2, ram: 14 GB, | |
| Backup Prepare Node | 0 | Automatic: 200 GB | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| UAA | Automatic: 2 | None | Automatic: Standard_F2s (cpu: 2, ram: 4 GB, disk: 3 | |
| Cloud Controller | Automatic: 2 | Automatic: 1 GB | Automatic: Standard_F2s (cpu: 2, ram: 4 GB, disk: 3 | |
| HAProxy | Automatic: 1 | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| Router | Automatic: 3 | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |

2. Ensure a **Standard** VM type is selected for the **Router** VM. The PAS deployment fails if you select a **Basic** VM type.
3. Retrieve the name(s) of your external ALB by navigating to the Azure portal, clicking **All resources**, and locating your **Load balancer** resource.


 **Note:** The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource. `az network lb list`

4. Locate the **Router** job in the **Resource Config** pane and enter the name of your external ALB in the field under **Load Balancers**.
5. Retrieve the name of your Diego SSH Load Balancer by navigating to the Azure portal, clicking **All resources**, and locating your **Load balancer** resource.
6. Locate the **Diego Brain** job in the **Resource Config** pane and enter the name of the Diego SSH Load Balancer in the field under **Load Balancers**.
7. Ensure that the **Internet Connected** checkboxes are deselected for all jobs.
8. Scale the number of instances as appropriate for your deployment.

 **Note:** For a high availability deployment of PCF on Azure, Pivotal recommends scaling the number of each PAS job to a minimum of three (3) instances. Using three or more instances for each job creates a sufficient number of availability sets and fault domains for your deployment. For more information, see [Reference Architecture for Pivotal Cloud Foundry on Azure](#).

Step 23: (Optional) Scale Down and Disable Resources

 **Note:** The **Resource Config** pane has fewer VMs if you are installing the [Small Footprint Runtime](#).

 **Note:** The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to **3** instances and scale the **Control** VM to **2** instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by using the dropdowns under **Instances** for each job.

By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding system-provided resources in Ops Manager to reduce costs and administrative overhead.

Complete the following procedures to disable specific VMs in Ops Manager:

1. Click **Resource Config**.

2. If you configured PAS to use an external S3-compatible filestore, enter in **Instances** in the **File Storage** field.
3. If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:
 - **MySQL Proxy:** Enter in **Instances**.
 - **MySQL Server:** Enter in **Instances**.
 - **MySQL Monitor:** Enter in **Instances**.
4. If you disabled TCP routing, enter **Instances** in the **TCP Router** field.
5. Click **Save**.

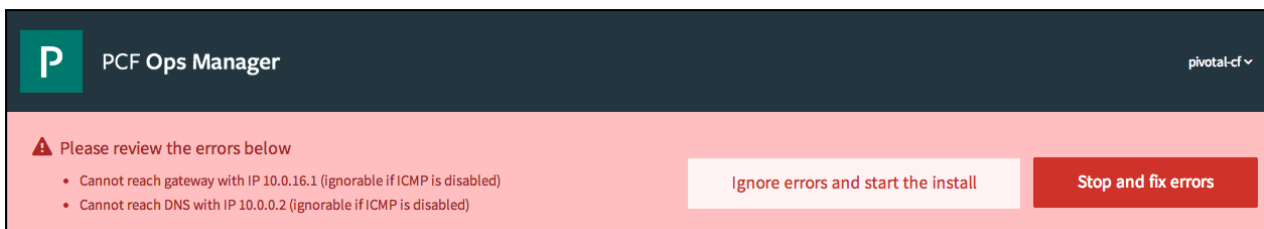
Step 24: Download Stemcell

This step is only required if your Ops Manager does not already have the stemcell version required by PAS. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

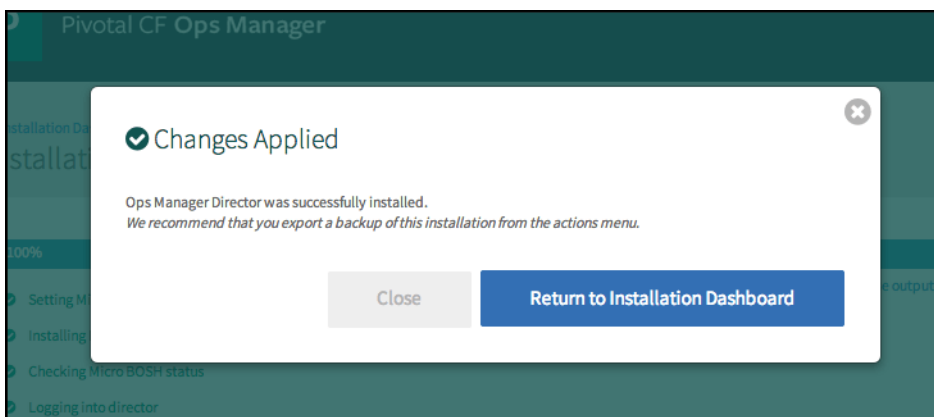
1. Open the [Stemcell product page](#) in the Pivotal Network. *Note, you may have to log in.*
2. Download the appropriate stemcell version targeted for your IaaS.
3. Navigate to **Stemcell Library** in the **Installation Dashboard**.
4. Click **Import Stemcell** to import the downloaded stemcell file.
5. When prompted, enable the Ops Manager product checkbox to stage your stemcell.
6. Click **Apply Stemcell to Products**.

Step 25: Complete the PAS Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.



The install process generally requires a minimum of 90 minutes to complete. The image shows the Changes Applied window that displays when the installation process successfully completes.



Installing PCF on Azure Using Terraform

This topic explains how to install Pivotal Cloud Foundry (PCF) on Microsoft Azure using Terraform.

To install PCF on Azure using Terraform, do the following:

1. Deploy Ops Manager. See [Deploying Ops Manager on Azure Using Terraform](#).
2. Configure BOSH Director on Azure Using Terraform. See [Configuring BOSH Director on Azure Using Terraform](#).
3. Deploy PAS. See [Deploying PAS on Azure Using Terraform](#).

Deploying Ops Manager on Azure Using Terraform

Page last updated:

This guide describes the preparation steps required to install Ops Manager on Azure using Terraform templates.

The Azure Terraform templates describe a set of Azure resources and properties. For more information about how Terraform creates resources in Azure, see the [Azure Provider](#) topic on the Terraform site.

You may also find it helpful to review different deployment options in the [Reference Architecture for Pivotal Cloud Foundry on Azure](#).

Prerequisites

In addition to fulfilling the prerequisites listed in the [Installing Pivotal Cloud Foundry on Azure](#) topic, ensure you have the following:

- The [Terraform CLI](#)
- In your Azure project, ensure you have completed the steps in [Preparing to Deploy Ops Manager on Azure Using Terraform](#) to create a service principal.

Step 1: Download Templates and Edit Variables File

Before you can run Terraform commands to provision infrastructure resources, you must download the Azure Terraform Templates and create a Terraform template variables file as described below:

1. On [Pivotal Network](#), navigate to the Pivotal Application Service (PAS) release.
2. Download the Azure Terraform ZIP file.
3. Extract the contents of the ZIP file.
4. Move the extracted folder to the `workspace` directory on your local machine.
5. On the command line, navigate to the directory. For example:

```
$ cd ~/workspace/pivotal-cf-terraforming-azure
```

6. Navigate to the `terraforming-pas` or `terraforming-pks` directory that contains the Terraform files for your runtime.
7. In the runtime directory, create a text file named `terraform.tfvars`.
8. Open the `terraform.tfvars` file and add the following:

```
subscription_id = "YOUR-SUBSCRIPTION-ID"
tenant_id       = "YOUR-TENANT-ID"
client_id       = "YOUR-CLIENT-ID"
client_secret   = "YOUR-CLIENT-SECRET"

env_name        = "YOUR-ENVIRONMENT-NAME"
env_short_name  = "YOUR-ENVIRONMENT-SHORTNAME"
location        = "YOUR-AZURE-LOCATION"
ops_manager_image_uri = "YOUR-OPS-MAN-IMAGE-URI"
dns_suffix      = "YOUR-DNS-SUFFIX"
vm_admin_username = "YOUR-ADMIN-USERNAME"
```

9. Edit the values in the file according to the table below.

| Value to replace | Guidance |
|-----------------------------------|--|
| <code>YOUR-SUBSCRIPTION-ID</code> | Enter the subscription ID of your Azure service principal. Terraform uses this ID when creating resources. |
| <code>YOUR-TENANT-ID</code> | Enter the tenant ID of your Azure service principal. Terraform uses this ID when creating resources. |
| <code>YOUR-CLIENT-ID</code> | Enter the client ID of your Azure service principal. Terraform uses this ID when creating |

| | |
|---|--|
| <code>YOUR-CLIENT-SECRET</code> | resources. Enter your Azure service client secret. Terraform requires this secret to create resources. |
| <code>YOUR-ENVIRONMENT-NAME</code> | Enter a name to use to identify resources in Azure. Terraform prepends the names of the resources it creates with this environment name. This environment variable is also used to name the Azure resource group created for the deployment. Example: <code>mypcf</code> . |
| <code>YOUR-ENVIRONMENT-SHORTNAME</code> | Enter a name to use when creating storage accounts in Azure. Must be a-z only and no longer than 10 characters. Example: <code>myazure</code> . |
| <code>YOUR-AZURE-LOCATION</code> | Enter the name of the Azure location in which you want Terraform to create resources. Example: <code>Central US</code> . |
| <code>YOUR-OPS-MAN-IMAGE-URI</code> | Enter the URL for the Ops Manager Azure image you want to boot. You can find this code in the PDF included with the Ops Manager release on Pivotal Network . |
| <code>YOUR-DNS-SUFFIX</code> | Enter a domain name to use as part of the system domain for your deployment. Terraform creates DNS records in Azure using <code>YOUR-ENVIRONMENT-NAME</code> and <code>YOUR-DNS-SUFFIX</code> . For example, if you enter <code>example.com</code> for your DNS suffix and have <code>pcf</code> as your environment name, Terraform creates DNS records at <code>pcf.example.com</code> . |
| <code>YOUR-ADMIN-USERNAME</code> | Enter the admin username you want to use for your Ops Manager deployment. |

Step 2: (Optional) Add Variables for Isolation Segment

Complete this section if you plan to deploy the Isolation Segment tile.

 **Note:** You can see the configurable options by opening the `variables.tf` file and looking for variables with default values.

Add the following variable to your `terraform.tfvars` file. This causes Terraform to create an additional HTTP load balancer and DNS record to use for the Isolation Segment tile.

```
isolation_segment = "true"
```

Step 3: Create Azure Resources with Terraform

Follow these steps to use the Terraform CLI to create resources on Azure:

1. From the directory that contains the Terraform files, run `terraform init` to initialize the directory based on the information you specified in the `terraform.tfvars` file.

```
$ terraform init
```

2. Run the following command to create the execution plan for Terraform.

```
$ terraform plan -out=plan
```

3. Run the following command to execute the plan from the previous step. It may take several minutes for Terraform to create all the resources in Azure.

```
$ terraform apply plan
```

Step 4: Create DNS Record

1. In a browser, navigate to the DNS provider for the DNS suffix you entered in your `terraform.tfvars` file.
2. Create a new NS (Name server) record for your system domain. Your system domain is `YOUR-ENVIRONMENT-NAME.YOUR-DNS-SUFFIX`.
3. In this record, enter the name servers included in `env_dns_zone_name_servers` from your Terraform output.

Next Steps

Proceed to the next step in the deployment, [Configuring BOSH Director on Azure Using Terraform](#).

Configuring BOSH Director on Azure Using Terraform

Page last updated:

This topic describes how to configure the BOSH Director tile within Ops Manager on Azure after [Deploying Ops Manager to Azure Using Terraform](#).

Note: You can also perform the procedures in this topic using the Ops Manager API. For more information, see the [Using the Ops Manager API](#) topic.

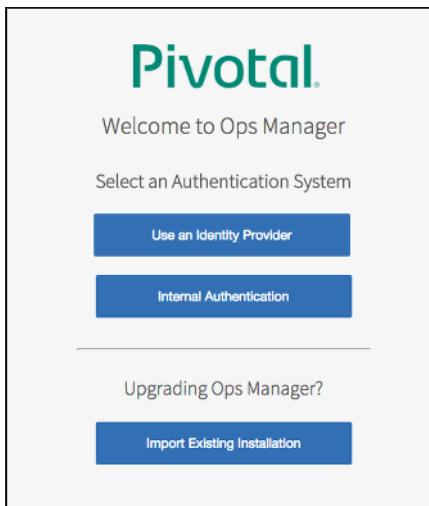
Prerequisite

To complete the procedures in this topic, you must have access to the output from when you ran `terraform apply` to create resources for this deployment. You can view this output at any time by running `terraform output`. You use the values in your Terraform output to configure the BOSH Director tile.

Step 1: Access Ops Manager

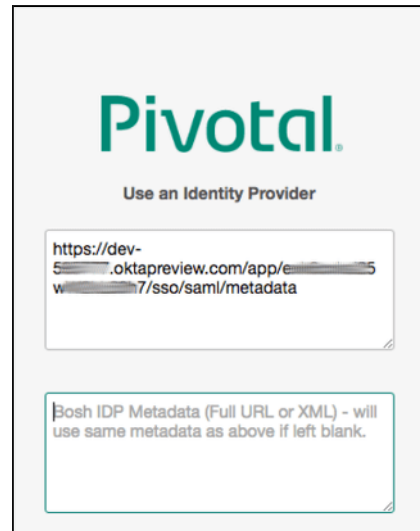
Note: For security, Ops Manager v1.7 and later require that you log in using a fully qualified domain name.

1. In a web browser, navigate to the fully qualified domain name (FQDN) of the BOSH Director. Use the `ops_manager_dns` value from running `terraform output`.
2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you use an Identity Provider, an external identity server maintains your user database.
 - [Internal Authentication](#): If you use Internal Authentication, Ops Manager maintains your user database.



Use an Identity Provider (IdP)

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.



2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.

Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a `500` error.

Note: These attributes are case-sensitive.

- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.

5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.

6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

Note: To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.

- **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
- **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
- **Name ID:** Email Address
- SAML authentication requests are always signed

8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.

- **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
- **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
- **Name ID:** Email Address
- SAML authentication requests are always signed

9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

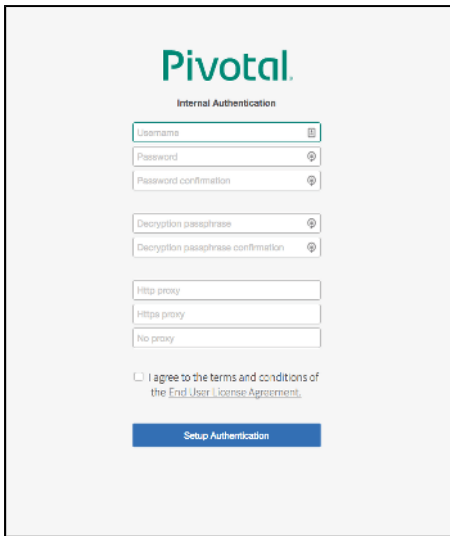
Internal Authentication

1. When redirected to the **Internal Authentication** page, do the following:

- Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
- Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not

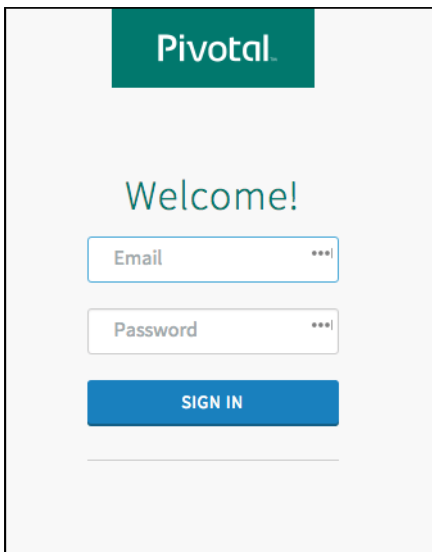
recoverable if lost.

- If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in the [Configuring Proxy Settings for the BOSH CPI](#) topic.
- Read the **End User License Agreement**, and select the checkbox to accept the terms.
- Click **Setup Authentication**.



The image shows the 'Internal Authentication' setup page in Pivotal. It features the Pivotal logo at the top. Below the logo, the title 'Internal Authentication' is centered. The form contains several input fields: 'Username', 'Password', 'Password confirmation', 'Decryption passphrase', and 'Decryption passphrase confirmation'. Each of these fields has a small icon to its right. Below these fields are three radio button options for 'Http proxy': 'Http proxy', 'Https proxy', and 'No proxy'. At the bottom of the form, there is a checkbox labeled 'I agree to the terms and conditions of the End User License Agreement'. A blue button labeled 'Setup Authentication' is positioned at the bottom center of the form.

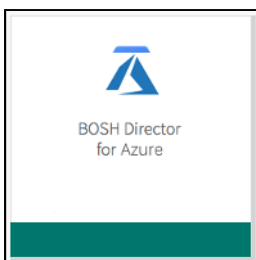
2. Log in to Ops Manager with the Admin username and password that you created in the previous step.



The image shows the 'Welcome!' login page in Pivotal. It features the Pivotal logo at the top. Below the logo, the title 'Welcome!' is centered. The form contains two input fields: 'Email' and 'Password'. Each field has a small icon to its right. A blue button labeled 'SIGN IN' is positioned below the 'Password' field. A horizontal line is located at the bottom of the form.

Step 2: Azure Config Page

1. Click the **BOSH Director** tile.



2. Select **Azure Config**.

Installation Dashboard

Ops Manager Director

Settings Status Credentials

Azure Config

- ☐ Azure Config
- ☐ Director Config
- ☐ Create Networks
- ☐ Assign Networks
- ☒ Security
- ☒ Syslog
- ☒ Resource Config

Azure Config

Subscription ID*

Tenant ID*

Application ID*

Client Secret*

Resource Group Name*

BOSH Storage Account Name*

Cloud Storage Type

☒ Use Managed Disks

Storage Account Type

Premium_LRS

☐ Use Storage Accounts

Deployments Storage Account Name

Default Security Group*

SSH Public Key*

SSH Private Key*

Save

- Complete the following fields with information you obtained in the [Preparing to Deploy Ops Manager on Azure Using Terraform](#) topic.
 - Subscription ID:** Enter the ID of your Azure subscription.
 - Tenant ID:** Enter your `TENANT_ID`.
 - Application ID:** Enter the `APPLICATION_ID` that you created in the [Create an AAD Application](#) step of the *Preparing to Deploy Ops Manager on Azure Using Terraform* topic.
 - Client Secret:** Enter your `CLIENT_SECRET`.
- Complete the following fields:
 - Resource Group Name:** Enter the name of your resource group, which is exported from Terraform as the output `pcf_resource_group_name`.
 - BOSH Storage Account Name:** Enter the name of your storage account, which is exported from Terraform as the output `bosh_root_storage_account`.
- For **Cloud Storage Type**, select **Use Managed Disks**. For **Storage Account Type**, select **Premium_LRS** which corresponds to SSD-based storage.

See [Azure Managed Disks Overview](#) in the Microsoft documentation for more information.

Cloud Storage Type

☒ Use Managed Disks

Storage Account Type

Premium_LRS Storage Account Type to use with managed disks

☐ Use Storage Accounts

Warning: You can update your deployment from using storage accounts to using managed disks. However, after you select **Use Managed Disks** and deploy Ops Manager, you cannot change your deployment back to use storage accounts.

- For **Default Security Group**, enter the `bosh_deployed_vms_security_group_name` output from Terraform.
- For **SSH Public Key**, enter the `ops_manager_ssh_public_key` output from Terraform.
- For **SSH Private Key**, enter the `ops_manager_ssh_private_key` output from Terraform.
- For **Azure Environment**, select **Azure Commercial Cloud**.
- Click **Save**.

Step 3: Director Config Page

- Select **Director Config** to open the **Director Config** page.

Director Config

NTP Servers (comma delimited)*

time.nist.gov

JMX Provider IP Address

Bosh HM Forwarder IP Address

☐ Enable VM Resurrector Plugin

☐ Enable Post Deploy Scripts

☐ Recreate all VMs

This will force BOSH to recreate all VMs on the next deploy. Persistent disk will be preserved

☐ Enable bosh deploy retries

This will attempt to re-deploy a failed deployment up to 5 times.

☐ Keep Unreachable Director VMs

- In the **NTP Servers (comma delimited)** field, enter a comma-separated list of valid NTP servers.

Note: The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify the value of this field.

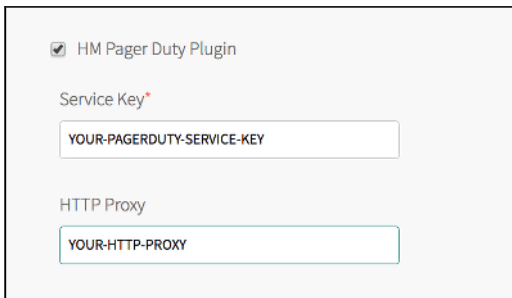
- Leave the **JMX Provider IP Address** field blank.

Note: BOSH-reported system metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use PCF JMX Bridge for consuming them outside of the Firehose, you may receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank.

4. Leave the **Bosh HM Forwarder IP Address** field blank.

Note: BOSH-reported system metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use the BOSH HM Forwarder for consuming them, you may receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank.

5. Select the **Enable VM Resurrector Plugin** checkbox to enable the Ops Manager Resurrector functionality and increase Pivotal Application Service (PAS) availability.
6. Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.
7. Select **Recreate all VMs** to force BOSH to recreate all VMs on the next deploy. This process does not destroy any persistent disk data.
8. Select **Enable bosh deploy retries** if you want Ops Manager to retry failed BOSH operations up to five times.
9. (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS secure communications.
10. Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.
11. Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.



☒ HM Pager Duty Plugin

Service Key*

YOUR-PAGERDUTY-SERVICE-KEY

HTTP Proxy

YOUR-HTTP-PROXY

- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.

12. Select **HM Email Plugin** to enable Health Monitor integration with email.

☒ HM Email Plugin

Host*

Port*

Domain*

From*

Recipients*

Username


Password

☒ Enable TLS

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma-separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter the password for your email server.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

- For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

 **Note:** After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*


HSM Port Address*

Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**
 9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal
☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature
☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- o **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- o **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. Follow the procedures in [Sign up for Amazon S3](#) and [Creating a Bucket](#) in the AWS documentation. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.


- **GCS Blobstore:** Select this option to use an external GCS endpoint. To create a GCS bucket, you must have a GCS account. Follow the procedures in [Creating Storage Buckets](#) in the GCS documentation to create a GCS bucket. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Follow the steps in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually* to download a JSON file with a private key. Enter the contents of the JSON file into the field.

15. For **Database Location**, select **Internal**.

16. (Optional) **Director Workers** sets the number of workers available to execute Director tasks. This field defaults to `5`.

17. (Optional) **Max Threads** sets the maximum number of threads that the BOSH Director can run simultaneously. Pivotal recommends that you leave the field blank to use the default value, unless doing so results in rate limiting or errors on your IaaS.

18. (Optional) To add a custom URL for your BOSH Director, enter a valid hostname in **Director Hostname**. You can also use this field to configure a load balancer in front of your BOSH Director. For more information, see [How to set up a load balancer in front of BOSH Director](#) in the Pivotal Knowledge Base.

 **Warning:** In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, VMs become unavailable. This causes downtime. To restore VM availability, enable **Recreate All VMs** and redeploy. This issue is resolved in [Ops Manager v2.2.8](#) and later.

19. (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.

20. (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.


 **Breaking Change:** Do not disable BOSH DNS without consulting Pivotal Support.

21. (Optional) To set a custom banner that users see when logging in to the Director using SSH, enter text in the **Custom SSH Banner** field.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

22. (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1, hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.


 **Note:** Azure has limited space for identification tags. Pivotal recommends entering no more than five tags.

23. Click **Save**.

Step 4: Create Networks Page

Select **Create Networks** and follow the procedures in this section to add the network configuration you created for your VPC.

Create the Infrastructure Network

1. Click **Add Network**.
 2. (Optional) Select **Enable ICMP checks** to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
 3. For **Name**, enter the name of the network you want to create. For example, `infrastructure`.
 4. Under **Subnets**, complete the following fields:
 - **Azure Network Name:** Enter `NETWORK-NAME/SUBNET-NAME`, where `NETWORK-NAME` is the `network_name` output from Terraform and `SUBNET-NAME` is the `infrastructure_subnet_name` output from Terraform.
-  **Note:** The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.
- **CIDR:** Enter the CIDR listed under `infrastructure_subnet_cidrs` output from Terraform. For example, `10.0.8.0/26`.
 - **Reserved IP Ranges:** Enter the first nine IP addresses of the subnet. For example, `10.0.8.1-10.0.8.9`.
 - **DNS:** Enter `168.63.129.16`.
 - **Gateway:** Enter the first IP address of the subnet. For example, `10.0.8.1`.

Create Networks


Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future.
Contact Pivotal support for help completing such a change.

Verification Settings


☐ Enable ICMP checks

Networks

One or many IP ranges upon which your products will be deployed

▼ infrastructure 

Name*

Subnets 


Azure Network Name*

CIDR*


Reserved IP Ranges

DNS*

Gateway*



5. Click **Save**.

 **Note:** After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

Create the PAS Network

- Click **Add Network**.
- (Optional) Select **Enable ICMP checks** to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
- For **Name**, enter the name of the network you want to create. For example, `pas`.
- Under **Subnets**, complete the following fields:
 - Azure Network Name:** Enter `NETWORK-NAME/SUBNET-NAME`, where `NETWORK-NAME` is the `network_name` output from Terraform and `SUBNET-NAME` is the `pas_subnet_name` output from Terraform.
 - CIDR:** Enter the CIDR listed under `pas_subnet_cidrs` output from Terraform. For example, `10.0.0.0/22`.
 - Reserved IP Ranges:** Enter the first nine IP addresses of the subnet. For example, `10.0.0.1-10.0.0.9`.
 - DNS:** Enter `168.63.129.16`.
 - Gateway:** Enter the first IP address of the subnet. For example, `10.0.0.1`.

▼ pas

Name*

pas

Subnets Add Subnet

Azure Network Name*

pcf-virtual-network/pcf-pas-subnet

CIDR*

10.0.12.0/22

Reserved IP Ranges

10.0.12.1-10.0.12.9

DNS*

168.63.129.16

Gateway*

10.0.12.1

5. Click **Save**.

Create the Services Network

1. (Optional) Select **Enable ICMP checks** to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
2. For **Name**, enter the name of the network you want to create. For example, `services`.
3. Under **Subnets**, complete the following fields:
 - **Azure Network Name:** Enter `NETWORK-NAME/SUBNET-NAME`, where `NETWORK-NAME` is the `network_name` output from Terraform and `SUBNET-NAME` is the `services_subnet_name` output from Terraform.
 - **CIDR:** Enter the CIDR listed under `services_subnet_cidrs` output from Terraform. For example, `10.0.4.0/22`.
 - **Reserved IP Ranges:** Enter the first nine IP addresses of the subnet. For example, `10.0.4.1-10.0.4.9`.
 - **DNS:** Enter `168.63.129.16`.
 - **Gateway:** Enter the first IP address of the subnet. For example, `10.0.4.1`.

▼ services

Name*

services

Subnets

Add Subnet

Azure Network Name*

pcf-virtual-network/pcf-services-subnet

CIDR*

10.0.8.0/22

Reserved IP Ranges

10.0.8.1-10.0.8.9

DNS*

168.63.129.16

Gateway*

10.0.8.1

4. Click **Save**. If you do not have **Enable ICMP checks** selected, you may see red warnings which you can safely ignore.

Step 5: Assign Networks Page

1. Select **Assign Networks**.

Network Assignments

Network

infrastructure

Save

2. Use the dropdown to select the `infrastructure` network for your BOSH Director.
3. Click **Save**.

Step 6: Security Page

[illegible]

1. Select **Security**.
2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:

```

-----BEGIN CERTIFICATE-----
ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678AB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BCDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABBB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----

```

 Note: If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#) for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 7: Syslog Page

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
 ☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save

- (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
- In the **Address** field, enter the IP address or DNS name for the remote server.
- In the **Port** field, enter the port number that the remote server listens on.
- In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
- (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
 - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
- Click **Save**.

Step 8: Resource Config Page


- Select **Resource Config**.


Resource Config


| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|------------------------|--------------|----------------------|---|----------------|--------------------------|
| Ops Manager Director | Automatic: 1 | Automatic: 50 GB | Automatic: Standard_DS2_v2 (cpu: 2, ram | | <input type="checkbox"/> |
| Master Compilation Job | Automatic: 4 | None | Automatic: Standard_F4s (cpu: 4, ram: 8 G | | <input type="checkbox"/> |

Save

- Adjust any values as necessary for your deployment. Under the **Instances**, **Persistent Disk Type**, and **VM Type** fields, choose **Automatic** from the dropdown to allocate the recommended resources for the job. If the **Persistent Disk Type** field reads **None**, the job does not require persistent disk space.

 **Note:** Pivotal recommends provisioning a BOSH Director VM with at least 8 GB memory.

 **Note:** If you set a field to **Automatic** and the recommended resource allocation changes in a future version, Ops Manager automatically uses the new recommended allocation.

 **Note:** If you install PAS for Windows, provision your **Master Compilation Job** with at least 100 GB of disk space.


- (Optional) For **Load Balancers**, enter your Azure application gateway name for each associated job. To create an application gateway, follow the procedures in [Create an application gateway with SSL termination using Azure PowerShell](#) from the Azure documentation. When you create the application gateway, associate the gateway's IP with your system domain.
- Click **Save**.

Step 9: (Optional) Add Custom VM Extensions


Use the Ops Manager API to add custom properties to your VMs such as associated security groups and load balancers. For more information, see [Managing Custom VM Extensions](#).

Step 10: Complete the BOSH Director Installation

- Click the **Installation Dashboard** link to return to the Installation Dashboard.
- Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.


PCF Ops Manager

pivotal-cf

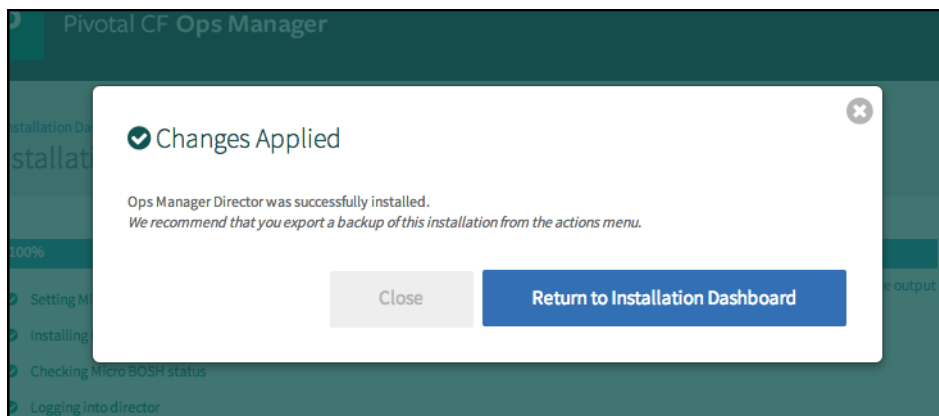
 Please review the errors below

- Cannot reach gateway with IP 10.0.16.1 (ignorable if ICMP is disabled)
- Cannot reach DNS with IP 10.0.0.2 (ignorable if ICMP is disabled)

Ignore errors and start the install

Stop and fix errors

- BOSH Director installs. This may take a few moments. When the installation process successfully completes, the **Changes Applied** window appears.



Next Steps

After you complete this procedure, follow the procedures in [Deploying PAS on Azure Using Terraform](#).

Deploying PAS on Azure Using Terraform

Page last updated:

This topic describes how to install and configure Pivotal Application Service (PAS) on Azure.

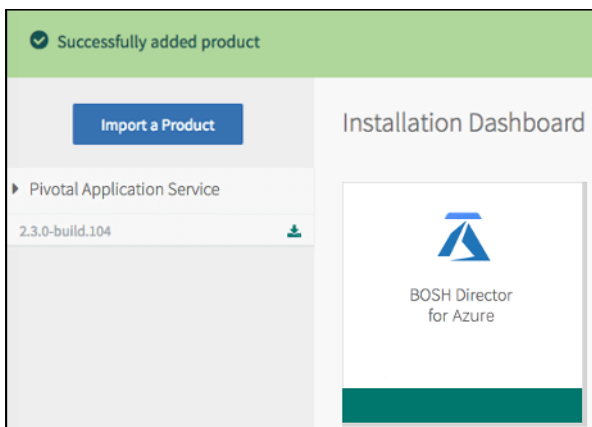
Before you perform the procedures in this topic, you must have completed the procedures in [Deploying Ops Manager to Azure Using Terraform](#), the [Launching a BOSH Director Instance on Azure Using Terraform](#) topic, and the [Configuring BOSH Director on Azure Using Terraform](#) topic.

Note: If you plan to [install the PCF IPsec add-on](#), you must do so before installing any other tiles. Pivotal recommends installing IPsec immediately after Ops Manager, and before installing the Pivotal Application Service (PAS) tile.

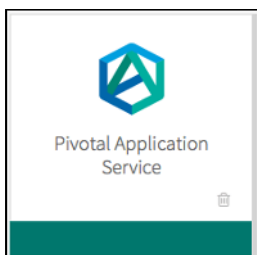
Note: The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

Step 1: Add PAS to Ops Manager

1. If you have not already downloaded PAS, log in to [Pivotal Network](#), and click on PAS.
2. From the **Releases** drop-down, select the release to install and choose one of the following:
 - a. Click PAS to download the PAS `.pivotal` file.
 - b. Click **PCF Small Footprint PAS** to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).
3. Navigate to the Ops Manager Installation Dashboard.
4. Click **Import a Product** and select the downloaded `.pivotal` file. For more information, refer to the [Adding and Deleting Products](#) topic.
5. Click the plus button next to the imported tile to add it to the Installation Dashboard.

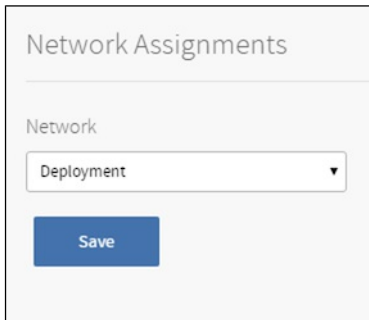


6. Click the PAS tile in the Installation Dashboard.



Step 2: Assign Networks

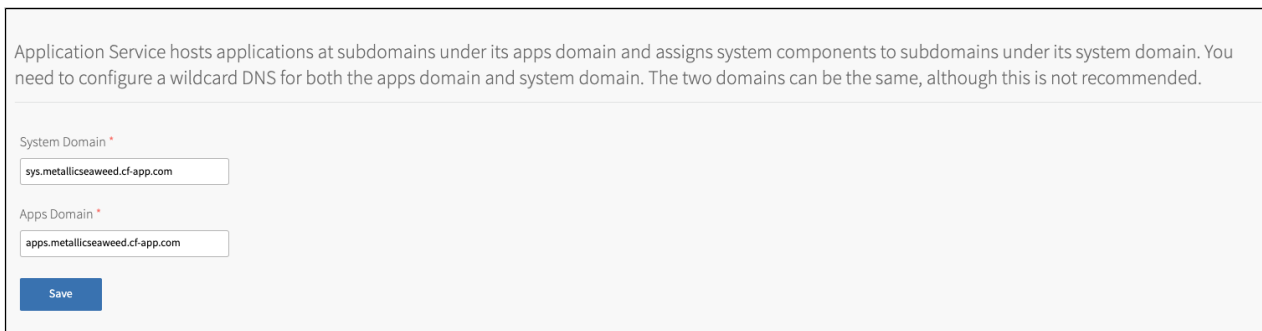
1. Select **Assign Networks**.
2. From the **Network** dropdown, select the network on which you want to run PAS.




3. Click **Save**.

Step 3: Configure Domains

1. Select **Domains**.




2. Enter the system and application domains.
 - For **System Domain**, enter the value of `sys_domain` from the Terraform output. This defines your target when you push apps to PAS.
 - For **Apps Domain**, enter the value of `apps_domain` from the Terraform output. This defines where PAS should serve your apps.

 **Note:** You configured a wildcard DNS record for these domains in an earlier step.

3. Click **Save**.

Step 4: Configure Networking

1. Select **Networking**.
2. Leave the **Router IPs**, **SSH Proxy IPs**, **HAProxy IPs**, and **TCP Router IPs** fields blank. You do not need to complete these fields when deploying PCF to Azure.

 **Note:** You specify load balancers in the **Resource Config** section of PAS later on in the installation process. See the [Configuring Resources](#) section.

3. Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate and Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.
 - a. Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

Certificates and Private Keys for HAProxy and Router

Add

▼ example-cert

Name *

example-cert

A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

Generate RSA Certificate

▼ example-cert-2

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager.

- b. If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see *Configure Front End* in [Preparing to Deploy Ops Manager on GCP Manually](#).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

4. (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Router** field, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

- ☐ TLSv1.0
- ☐ TLSv1.1
- ☒ TLSv1.2

- Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

- ☒ Log client IPs
- ☐ Disable logging of X-Forwarded-For header only
- ☐ Disable logging of both source IP and X-Forwarded-For header
- To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.

- Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.



Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

- ☒ TLS terminated for the first time at infrastructure load balancer
- ☐ TLS terminated for the first time at HAProxy
- ☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|---|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to | TLS terminated for | HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header. |

| | | |
|--|--|---|
| the instances of HAProxy, and o HAProxy instance count is > 0 | the first time at HAProxy. |  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |
| o The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | TLS terminated for the first time at the Gorouter. | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |


For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).

8. To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

- ☒ HAProxy does not request client certificates.
- ☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- o **HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- o **HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.


 **warning:** Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

9. To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- o **Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- o **Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- o **Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

 **warning:** Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client**


Certificate Validation in the Networking pane.

- In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.


 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:
`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384` If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable


◦ Enable HAProxy forwarding of requests to Router over TLS

| If you want to: | Encrypt communication between HAProxy and the Gorouter |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

◦ Disable HAProxy forwarding of requests to Router over TLS

| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |

13. If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

14. (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

15. (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
16. (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
17. (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
18. By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#)

19. In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details.
 - a. If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
20. (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

0

500

21. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router *

- ☒ Enable
- ☐ Disable

22. (Optional) Increase the number of seconds in the **Router Timeout to Backends** field to accommodate larger uploads over connections with high latency. Set this value to less than or equal to the idle timeout value of the Azure load balancer, which defaults to 4 minutes.




Note: If the router timeout value exceeds the Azure LB timeout, you may experience intermittent TCP resets. For more information about configuring Azure load balancer idle timeout, see the [Azure documentation](#).

23. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

24. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
25. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

Load Balancer Healthy Threshold *

26. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

27. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

28. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.


HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.

HAProxy Trusted CIDRs

29. The **Loggregator Port** defaults to `443` if left blank. Leave this field blank.


Container Network Interface Plugin *

 Silk


30. For **Container Network Interface Plugin**, ensure **Silk** is selected and review the following fields:

 **Note:** The **External** option exists to support NSX-T integration for vSphere deployments.

- a. (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to `1454`. Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- b. (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses `10.255.0.0/16`.

 **warning:** The overlay network IP range must not conflict with any other IP addresses in your network.

- c. Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- d. For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to `1`.
- e. For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to `100`.
- f. To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- g. By default, containers use the same DNS servers as the host. If you want to override the DNS servers to be used in containers, enter a comma-separated list of servers in **DNS Servers**.

 **Note:** If your deployment uses BOSH DNS, which is the default, you cannot use this field to override the DNS servers used in containers.

- h. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is `120`. You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

31. For **DNS Search Domains**, enter DNS search domains for your containers as a comma-separated list. DNS on your containers appends these names to its host names, to resolve them into full domain names.

DNS Search Domains

DNS search domains to be used in containers. A comma-separated list can be specified.

32. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is `120`. You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

33. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:

- a. Select **Enable TCP Routing**.
- b. For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. These are the same ports that you configured in the [Pre-Deployment Steps](#) of the *Enabling TCP Routing* topic.

- To support multiple TCP routes, Pivotal recommends allocating multiple ports.
- To allocate a list of ports rather than a range:

1. Enter a single port in the **TCP Routing Ports** field.
2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time
 ☒ **Enable TCP Routing**

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

- c. For Azure, you also need to specify the name of Azure load balancer in the LOAD BALANCER column of TCP Router job of the **Resource Config** screen. You configure this later on in PAS. See [Configuring Resources](#).

34. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) topic.

35. Click **Save**.

Step 5: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC
- ☐ Router uses TLS to verify application identity


Private Docker Insecure Registry Whitelist

Docker Images Disk-Cleanup Scheduling on Cell VMs*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached


Threshold of Disk-Used (MB) (min: 1) *

- The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.
- The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
- If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
- If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.

- To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting](#) in *HTTP Routing*.

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

Warning: You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

- You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
- Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
- Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
- Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.

Note: In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

- (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs *

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

12. By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.
13. Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
14. You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is seconds and the maximum configurable timeout is seconds.
15. Click **Save**.

Step 6: Configure Application Developer Controls

1. Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *

Staging Timeout (Seconds) *


☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.

4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.
5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.

 **Note:** If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of seconds you specify in this field.
9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 7: Review Application Security Group

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type ☐ in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 8: Configure UAA

1. Select **UAA**.
2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

- Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN`.



Note: The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN`.

- If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
M
U
H
M
-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----

[Change](#)

SAML Service Provider Key Password

Secret

Password.

- (Optional) To override the default value, enter a custom SAML Entity ID in the **SAML Entity ID Override** field. By default, the SAML Entity ID is `http://login.YOUR-SYSTEM-DOMAIN` where `YOUR-SYSTEM-DOMAIN` is set in the **Domains > System Domain** field.
- For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
- (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line Interface (cf CLI) login access and refresh. Most deployments use the defaults.

Apps Manager Access Token Lifetime (in seconds) *

Apps Manager Refresh Token Lifetime (in seconds) *

Cloud Foundry CLI Access Token Lifetime (in seconds) *

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

Global Login Session Max Timeout (in seconds) *


Global Login Session Idle Timeout (in seconds) *

Customize Username Label (on login page) *

Customize Password Label (on login page) *

Proxy IPs Regular Expression *

8. (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:
 - **Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - **Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan
9. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
10. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Gorouter or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
11. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#) for help.


Internal Database Configuration

When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane. See the [Configure Internal Databases](#) section for details.

1. Select **Internal MySQL**.

Choose the location of your UAA database *

☒ Internal MySQL (preferred for complete high-availability)
☐ External (preferred if, for example, you use AWS RDS)

 **Note:** If you configure your system databases as external in the **Databases** pane, selecting Internal MySQL in the **UAA** pane has no effect.

2. Click **Save**.
3. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

1. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)
☒ External (preferred if, for example, you use AWS RDS)

Hostname *

TCP Port *


Username *

Password *


Secret

2. For **Hostname**, enter the hostname of the database server.
3. For **TCP Port**, enter the port of the database server.
4. For **User Account and Authentication database username**, specify a unique username that can access this specific database on the database server.
5. For **User Account and Authentication database password**, specify a password for the provided username.
6. Click **Save**.

Step 9: Configure CredHub

 **Note:** Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

1. Select **CredHub**.
2. Choose the location of your CredHub database. PAS includes this CredHub database for services to store their service instance credentials.

 **Note:** You cannot choose **Internal** for the CredHub database if you choose **External** for your System Databases. See [Configure System](#)

Databases below.

Configure the CredHub Server

Choose the location of your CredHub database *

- ☒ Internal MySQL (preferred for complete high-availability)
- ☐ External (preferred if, for example, you use Google Cloud SQL)

If you chose **External**, enter the following:

- **Hostname.** This is the IP address of your database server.
- **TCP Port.** This is the port of your database server, such as `3306`.
- **Username.** This is a unique username that can access your CredHub database on the database server.
- **Password.** This is the password for the provided username.
- **Database CA Certificate.** This certificate is used when encrypting traffic to and from the database.

3. Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys



Name *

Name of the encryption key.

Provider*

Key *

☐ Primary

- **Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- **Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- **Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- **Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.



Note: For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

4. (Optional) To configure CredHub to use an HSM, complete the following fields:

- **HSM Provider Partition.** This is the name of the HSM provider partition.
- **HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- **HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#) in the

Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

5. If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.

6. Click **Save**.

7. Select the **Resource Config** pane.

8. Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.

9. Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).

Step 10: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *


2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.

3. Click **Save**.

Step 11: Configure System Databases

You can configure PAS to use an internal MySQL database provided with PCF, or you can configure an external database provider for the databases required by PAS.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. Contact Pivotal Support for help. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration

If you want to use internal databases for your deployment, perform the following steps:

1. Select **Databases**.

2. Select one of the **Internal Databases** options:

- Internal Databases - MySQL - Percona XtraDB Cluster uses [Percona Server](#) with TLS encryption between server cluster nodes.
- Internal Databases - MySQL - MariaDB Galera Cluster uses [MariaDB](#) with cluster nodes communicating over plaintext.

⚠ warning: Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

3. Click **Save**.

Then proceed to [Step 12: \(Optional\) Configure Internal MySQL](#) to configure high availability and automatic backups for your internal MySQL databases.

External Database Configuration

⚠ warning: Protect whichever database you use in your deployment with a password.

To create your Pivotal Application Service (PAS) databases, follow the procedure below.

💡 Note: Exact configurations depend on your database provider. The following procedure uses AWS RDS as an example.

- Add the `ubuntu` account key pair from your IaaS deployment to your local SSH profile so you can access the Ops Manager VM. For example, in AWS, you add a key pair created in AWS:

```
$ ssh-add aws-keypair.pem
```

- SSH in to your Ops Manager using the Ops Manager FQDN and the username `ubuntu`:

```
$ ssh ubuntu@OPS-MANAGER-FQDN
```

- Log in to your MySQL database instance using the appropriate hostname and user login values configured in your IaaS account. For example, to log in to your AWS RDS instance, run the following MySQL command:


```
$ mysql --host=RDSHOSTNAME --user=RDSUSERNAME --password=RDSPASSWORD
```

- Run the following MySQL commands to create databases for the PAS components that require a relational database:


```
CREATE database ccd;
CREATE database notifications;
CREATE database autoscale;
CREATE database app_usage_service;
CREATE database routing;
CREATE database diego;
CREATE database account;
CREATE database nfsvolume;
CREATE database networkpolicyserver;
CREATE database silk;
CREATE database locket;
CREATE database uaa;
CREATE database credhub;
```

💡 Note: The command `CREATE database credhub;` is optional if you have no CredHub instances. By default, CredHub has `0` instances.

5. Type `exit` to quit the MySQL client, and `exit` again to close your connection to the Ops Manager VM.
6. In PAS, select **Databases**.
7. Select the **External Databases** option.


 **Note:** If you configure databases as external, you cannot configure an internal database in the **UAA** pane.

8. For **Hostname**, enter the hostname of the database server.
9. For **TCP Port**, enter the port of the database server.
10. Each component that requires a relational database has two corresponding fields: one for the database username and one for the database password. For each set of fields, specify a unique username that can access this specific database on the database server and a password for the provided username.

 **Note:** Ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.


11. Click **Save**.

Step 12: (Optional) Configure Internal MySQL

 **Note:** You only need to configure this section if you have selected one of the **Internal Databases - MySQL** options in the **Databases** section.

To use internal MySQL in High Availability configuration, you define a load balancer rule that lets PAS components send queries a single hostname backed by two redundant proxies. Each proxy then directs query traffic to three MySQL server nodes.

1. Allocate an internal load balancer rule to balance traffic between two static IP addresses. The static IP addresses cannot be within the range that that you have reserved for PAS.
The load balancer rule is separate from the software provided by Pivotal, and you need to define it within your infrastructure.
 - **Make your idle time out long enough to not interrupt long-running queries.** When queries take a long time, the load balancer can time out and interrupt the query.
For example, [AWS's Elastic Load Balancer](#) has a default idle timeout of 60 seconds, so queries that take longer than this duration sever the MySQL connection and return an error.
 - **Configure a healthcheck or monitor, using TCP against port 1936.** This defaults to TCP port `1936`, to maintain backwards compatibility with previous releases. This port is not configurable. Unauthenticated healthchecks against port 3306 may cause the service to become unavailable and require manual intervention to fix.
 - **Configure the load balancer to route traffic for TCP port 3306 to the IPs of all proxy instances on TCP port 3306.**
 - Record the hostname of the load balancer rule and the two static IP addresses.

 **warning:** You must configure a load balancer to achieve complete high availability.

2. From the PAS tile in Ops Manager, Select **Internal MySQL**.
3. In the **MySQL Proxy IPs** field, enter the static IP addresses used by the internal MySQL load balancer rule.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.


A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.

The automated backups functionality works with any S3-compatible file store that can receive your backup files.

MySQL Proxy IPs

MySQL Service Hostname

4. For **MySQL Service Hostname**, enter the IP address or hostname for your load balancer. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.
5. In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
6. In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.
7. (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
8. To prohibit the creation of command line history files on the MySQL nodes, disable the **Allow Command History** checkbox.
9. To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

10. For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the default value is 10 seconds.

Replication canary time period *

30

Replication canary read delay *

20

E-mail address (required) *

Fill in your desired email address

☒ Allow Command History

Cluster Probe Timeout

11. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.
12. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.
 - a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.

13. Enter values for the following fields:
 - **Load Balancer Healthy Threshold:** Specifies the amount of time, in seconds, to wait until declaring the MySQL Proxy instance started. This allows an external load balancer time to register the instance as healthy.
 - **Load Balancer Unhealthy Threshold:** Specifies the amount of time, in seconds, that the MySQL Proxy continues to accept connections before shutting down. During this period, the Healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.
14. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.
15. Click **Save**.

For more information on how to monitor the node health of your MySQL Proxy instances, see [Using the MySQL Proxy](#).

Step 13: Configure File Storage

To minimize system downtime, Pivotal recommends using highly resilient and redundant *external* filestores for your Pivotal Application Service (PAS) file storage.

When configuring file storage for the Cloud Controller in PAS, you can select one of the following:

- Internal WebDAV filestore
- External S3-compatible or Ceph-compatible filestore
- External Google Cloud Storage with Access Key and Secret Key
- External Google Cloud Storage with Service Account
- External Azure Cloud Storage

For production-level PCF deployments on Azure, the recommended selection is Azure Storage. For more information about production-level PCF deployments on Azure, see the [Reference Architecture for Pivotal Cloud Foundry on Azure](#).

For more factors to consider when selecting file storage, see [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#).

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External Azure Storage

To use external Azure file storage for your Pivotal Application Service (PAS) filestore, perform the following steps:

1. Select the **External AzureStorage** option.

Configure your Cloud Controller's filesystem*

☐ Internal WebDAV (provided by Elastic Runtime)
 ☐ External S3-Compatible File Store (if you want to use a service like S3 or Ceph)
 ☐ External Google Cloud Storage
 ☒ External Azure Storage

Account Name *

pcfstorageaccount

Access Key *

.....

Buildpacks Container Name *

pcfbuildpacks

Droplets Container Name *

pcfdroplets

Packages Container Name *

pcfpackages

Resources Container Name *

pcfresources

2. To create a new storage account and storage containers for the PAS filestore, perform the following steps.
 - In the Azure Portal, navigate to the **Storage accounts** tab.
 - Click on the plus icon to add a new storage account.
 - In the **Name** field, enter a unique name (all lowercase, 3 to 24 alphanumeric characters) for the storage account.
 - For the **Deployment model**, select **Resource manager**.
 - For **Account kind**, select **General purpose**.

- For **Performance**, select **Standard**.
 - From the **Replication** dropdown, select **Locally-redundant storage (LRS)**.
 - For **Storage service encryption**, select **Disabled**.
 - From the **Subscription** dropdown, select the subscription where you want to deploy PCF resources.
 - For **Resource group**, select **Use existing** and enter the name of the resource group where you deployed PAS.
 - From **Location** the dropdown, select the **Location** where you are deploying PCF.
 - Click **Create**.
 - After the storage account is created, select the new storage account from the dashboard.
 - Navigate to the **Blob Service** section of the storage account, and then click on **Containers** to create one or more containers in this storage account for buildpacks, droplets, resources, and packages.
 - For each container that you create, set the **Access type** to **Private**.
3. In PAS, enter the name of the storage account you created for **Account Name**.
 4. In the **Secret Key** field, enter one of the access keys provided for the storage account. To obtain a value for this fields, visit the Azure Portal, navigate to the **Storage accounts** tab and click on **Access keys**.
 5. For the **Buildpacks Container Name**, enter the container name for storing your app buildpacks.
 6. For **Droplets Container Name**, enter the container name for your app droplet storage. Pivotal recommends that you use a unique container name, but you can use the same container name as the previous step.
 7. For **Resources Container Name**, enter the container name for resources. Pivotal recommends that you use a unique container name, but you can use the same container name as the previous step.
 8. For **Packages Container Name**, enter the container name for packages. Pivotal recommends that you use a unique container name, but you can use the same container name as the previous step.
 9. Click **Save**.


 **Note:** To enable backup and restore of your PAS tile that uses S3 compatible blobstore, see [Enable External Blobstore Backups](#).

Other IaaS Storage Options

[Google Cloud Storage](#) and [External S3-Compatible File Storage](#) are also available as file storage options but are not recommended for typical PCF on Azure installations.

Step 14: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

 **Note:** The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

- ☒ No
☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging


☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration

Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.

 **Note:** The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.



Note: Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 15: (Optional) Customize Apps Manager

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

Add

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑️
- ▶ Docs 🗑️
- ▶ Tools 🗑️

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

4. Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
5. Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
6. Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
7. Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
8. The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
9. The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 16: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret


Save

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

 **Note:** If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 17: Configure Cloud Controller

- Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
☒ Disable

Save

- Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

- CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

- Click **Save**.

Step 18: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

- Select **Smoke Tests**.
- If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify

where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

☐ Temporary space within the system organization (This is deleted after smoke tests finish.)

☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.


Step 19: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

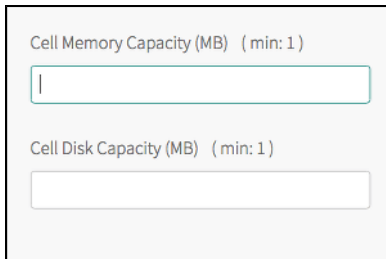
If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

 **Note:** Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.

To enable overcommit, do the following:


1. Select **Advanced Features**.



Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

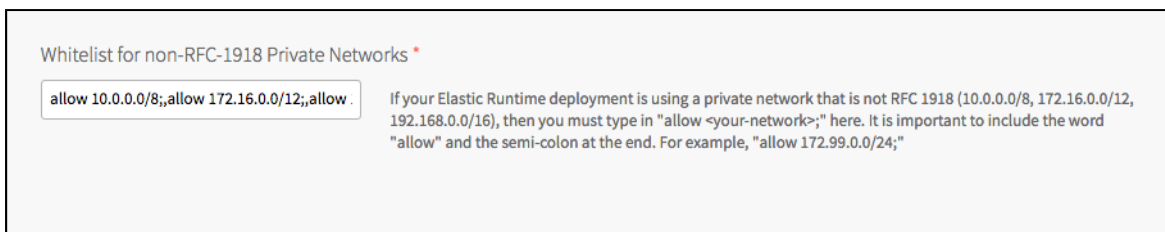
Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.



Whitelist for non-RFC-1918 Private Networks *

`allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .`

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

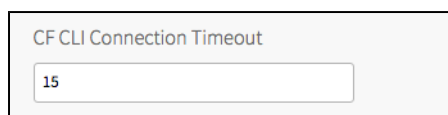
CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.



CF CLI Connection Timeout

2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.

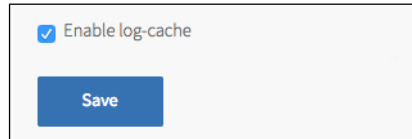
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PAS* topic.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

Warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 20: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.

- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.

- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.

- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

Step 21: Configure Resources

1. Select **Resource Config**.

| Resource Config | | | | |
|---------------------|--------------|----------------------|---|---------------|
| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCER |
| Consul | Automatic: 3 | Automatic: 1 GB | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| NATS | Automatic: | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| etcd | Automatic: 3 | Automatic: 1 GB | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| File Storage | Automatic: 1 | Automatic: 100 GB | Automatic: Standard_F2s (cpu: 2, ram: 4 GB, disk: 3 | |
| MySQL Proxy | Automatic: | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| MySQL Server | Automatic: 3 | Automatic: 100 GB | Automatic: Standard_DS11_v2 (cpu: 2, ram: 14 GB, | |
| Backup Prepare Node | 0 | Automatic: 200 GB | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| UAA | Automatic: 2 | None | Automatic: Standard_F2s (cpu: 2, ram: 4 GB, disk: 3 | |
| Cloud Controller | Automatic: 2 | Automatic: 1 GB | Automatic: Standard_F2s (cpu: 2, ram: 4 GB, disk: 3 | |
| HAProxy | Automatic: 1 | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |
| Router | Automatic: 3 | None | Automatic: Standard_F1s (cpu: 1, ram: 2 GB, disk: 1 | |

- Ensure a **Standard** VM type is selected for the **Router** VM. The PAS deployment fails if you select a **Basic** VM type.
- Enter the value of `web_lb_name` from your Terraform output in the **Resource Config** pane under **Load Balancers** for the **Router** job.
 - Enter the value of `diego_ssh_lb_name` from your Terraform output in the **Resource Config** pane under **Load Balancers** for the **Diego Brain** job.
 - Ensure that the **Internet Connected** checkboxes are deselected for all jobs.
 - Scale the number of instances as appropriate for your deployment.

Note: For a high availability deployment of PCF on Azure, Pivotal recommends scaling the number of each PAS job to a minimum of three (3) instances. Using three or more instances for each job creates a sufficient number of availability sets and fault domains for your deployment. For more information, see [Reference Architecture for Pivotal Cloud Foundry on Azure](#).

Step 22: (Optional) Scale Down and Disable Resources

Note: The **Resource Config** pane has fewer VMs if you are installing the [Small Footprint Runtime](#).

Note: The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to **3** instances and scale the **Control** VM to **2** instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by using the dropdowns under **Instances** for each job.

By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding system-provided resources in Ops Manager to reduce costs and administrative overhead.

Complete the following procedures to disable specific VMs in Ops Manager:

1. Click **Resource Config**.
2. If you configured PAS to use an external S3-compatible filestore, enter in **Instances** in the **File Storage** field.
3. If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:
 - **MySQL Proxy**: Enter in **Instances**.
 - **MySQL Server**: Enter in **Instances**.
 - **MySQL Monitor**: Enter in **Instances**.
4. If you disabled TCP routing, enter **Instances** in the **TCP Router** field.
5. Click **Save**.

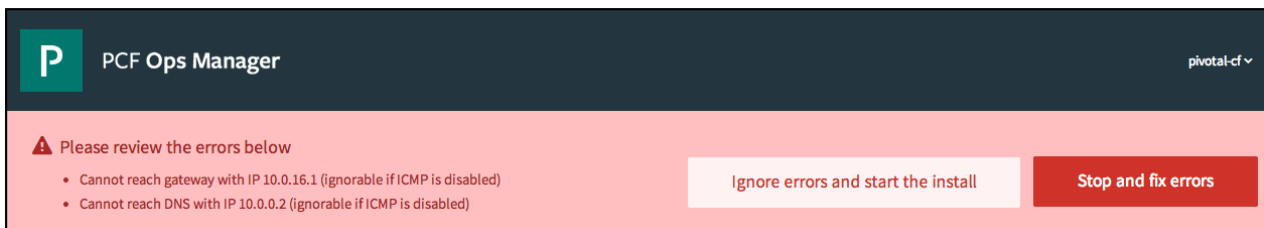
Step 23: Download Stemcell

This step is only required if your Ops Manager does not already have the stemcell version required by PAS. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

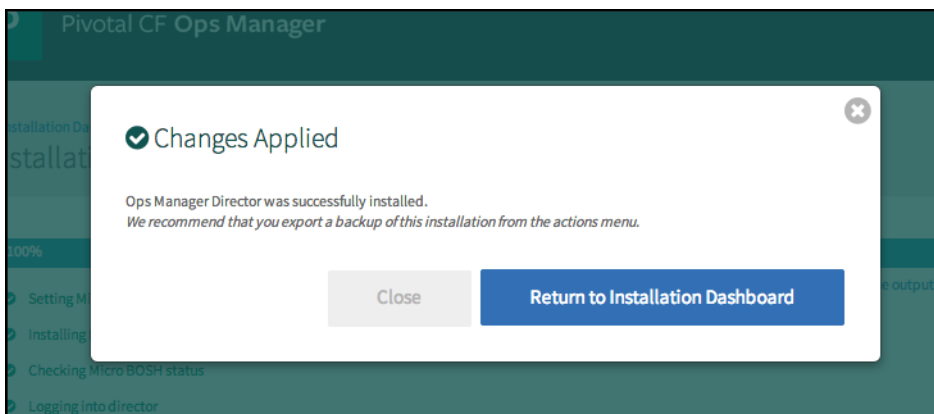
1. Open the [Stemcell product page](#) in the Pivotal Network. *Note, you may have to log in.*
2. Download the appropriate stemcell version targeted for your IaaS.
3. Navigate to **Stemcell Library** in the **Installation Dashboard**.
4. Click **Import Stemcell** to import the downloaded stemcell file.
5. When prompted, enable the Ops Manager product checkbox to stage your stemcell.
6. Click **Apply Stemcell to Products**.

Step 24: Complete the PAS Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.



The install process generally requires a minimum of 90 minutes to complete. The image shows the Changes Applied window that displays when the installation process successfully completes.



Troubleshooting PCF on Azure

Page last updated:

This topic describes how to troubleshoot known issues when deploying or running Pivotal Cloud Foundry (PCF) on Azure.

Installation Issues

Cannot Copy the Ops Manager Image

Symptom

Cannot copy the Ops Manager image into your storage account as part of *Step 4: Boot Ops Manager* in [Deploying Ops Manager on Azure Manually](#).

Explanation

You have an outdated version of the Azure CLI. You need the Azure CLI version 2.0.0 or greater. Run `az --version` from the command line to display your current Azure CLI version.

Solution

Install the Azure CLI 2.0 by following the instructions for your operating system in the [Azure documentation](#).

Deployment Fails at “create-env”

Symptom

After clicking **Apply Changes** to install Ops Manager and PAS, the deployment fails at `create-env` with an error message similar to the following:

```
Command 'deploy' failed:
Deploying:
Creating instance 'bosh/0':
Waiting until instance is ready:
Starting SSH tunnel:
Parsing private key file '/tmp/bosh_ec2_private_key.pem':
asn1: structure error: tags don't match (16 vs {class:3 tag:28 length:127
isCompound:false}) {optional:false explicit:false application:false
defaultValue:<nil> tag:<nil> stringType:0 timeType:0 set:false omitEmpty:false} pkcs1PrivateKey @2
===== 2016-09-29 16:28:22 UTC Finished "bosh create-env"
/var/tempest/workspaces/default/deployments/bosh.yml";
Duration: 328s; Exit Status: 1
Exited with 1.
```

Explanation

You provided a passphrase when creating your key pair in *Step 4: Boot Ops Manager* of [Deploying Ops Manager on Azure Manually](#).

Solution

Create a new key pair with no passphrase and redo the installation. See *Step 4: Boot Ops Manager* in [Deploying Ops Manager on Azure Manually](#).

Insufficient External Database Permissions

Upgrade issues can be caused when the external database user used for the network policy DB is given insufficient permissions. To avoid this upgrade issue, ensure that the networkpolicyserver database user has the

ALL
PRIVILEGES

permission.

Operation Issues

Slow Performance or Timeouts

Symptom

Developers suffer from slow performance or timeouts when pushing or managing apps, and end users suffer from slow performance or timeouts when accessing apps

Explanation

The Azure Load Balancer (ALB) disconnects active TCP connections lying idle for over four minutes.

Solution

To mitigate slow performance or timeouts, the default value of the **Router Timeout to Backends (in seconds)** field is set to 900 seconds. This default value is set high to mitigate performance issues but operators should tune this parameter to fit their infrastructure.

To edit the **Router Timeout to Backends (in seconds)** field:

1. Select the Pivotal Application Service (PAS) tile that is located within your **Installation Dashboard**.
2. Select the **Networking** tab.
3. Enter your desired time, in seconds, within the **Router Timeout to Backends (in seconds)** field.

Router Timeout to Backends (in seconds) (min: 1) *

Timeout for connections from Router (and HAProxy, if you use it) to applications and system components. Increase this to accommodate larger uploads over connections with high latency.

4. Click **Save**.

Service Instance Creation Times Out

Symptom

You are unable to provision a service instance of a Java or Go service. `cf create-service` fails with error

Failure provisioning service instance... Timed out after 8 minutes...

or similar.

Explanation

HTTP libraries for Java and Go, running with default settings, prune idle (for 240 seconds) connections from their connection pool without sending a TCP reset message back to the client service broker. This removes the ability of the broker to provision new service instances.

Solution

In the PAS tile **Configure Networking** pane, set **Frontend Idle Timeout** to 240 seconds or less, so that Cloud Foundry regenerates the front-end connection before it times out.

See the Knowledge Base article [Azure Networking Connection Idle for more than Four minutes](#) [↗](#) for details.

Deleting a PCF on Azure Installation

Page last updated:

When you deploy [Pivotal Cloud Foundry](#) (PCF) to Azure, you provision a set of resources. This topic describes how to delete the resources associated with a PCF deployment.

The fastest way to remove resources is to delete the resource group, or resource groups, associated with your PCF on Azure installation.

Delete the Resource Group

Perform the following steps to delete a resource group:

1. Navigate to the [Azure Portal](#).
2. Within your subscription, select **Resource Groups**.
3. Click on the resource group you wish to delete.
4. In the details pane for the resource group, click on the trash can icon. Review the information in the confirmation screen before proceeding.
5. To confirm deletion, type in the resource group name and click **Delete**.

For more information about managing resource groups in Azure, see the [Azure documentation](#).


Upgrading BOSH Director on Azure

This topic describes how to upgrade BOSH Director for Pivotal Cloud Foundry (PCF) on Azure.

Complete the tasks in this topic as part of the Ops Manager upgrade process. For more information, see [Upgrading Pivotal Cloud Foundry](#).

Overview

In this procedure, you create an Ops Manager VM instance to host the upgraded version of Ops Manager. Then, to complete the Ops Manager upgrade, you export your existing Ops Manager installation onto this new VM.

 **Note:** The Azure portal sometimes displays the names of resources with incorrect capitalization. Always use the Azure CLI to retrieve the correctly capitalized name of a resource.

To create an Ops Manager VM instance, do the following:

1. Export environment variables. See [Export Environment Variables](#).
2. Copy the Ops Manager image into your storage account. See [Copy the Ops Manager Image](#).
3. Configure the Ops Manager IP Address. See [Configure Ops Manager IP Address](#).
4. Create Ops Manager VM instance. See [Create Ops Manager VM Instance](#).

Prerequisites

To complete the Ops Manager upgrade, you must have your Ops Manager decryption passphrase. You defined this decryption passphrase during the initial installation of Ops Manager.

Export Environment Variables

Export the `connectionString` variable for your Azure account and assign it to a new environment variable. You use the `connectionString` environment variable when you copy the Ops Manager image in the following procedure.

To export environment variables, do the following:

1. Install the Azure CLI 2.0 by following the instructions for your operating system in the [Azure documentation](#).
2. Set your cloud:

```
$ az cloud set --name AzureCloud
```

If you deployed PCF in an environment other than Azure Cloud, consult the following list:

- For Azure China, replace `AzureCloud` with `AzureChinaCloud`. If logging in to `AzureChinaCloud` fails with a `CERT_UNTRUSTED` error, use the latest version of node, 4.x or later.
- For Azure Government Cloud, replace `AzureCloud` with `AzureUSGovernment`.
- For Azure Germany, replace `AzureCloud` with `AzureGermanCloud`.

3. Log in:

```
$ az login
```

Authenticate by navigating to the URL in the output, entering the provided code, and clicking your account.

4. Ensure that the following environment variables are set to the names of the resources you created when deploying Ops Manager as part of the procedures in [Deploying Ops Manager on Azure Manually](#).
 - `$RESOURCE_GROUP`: This should be set to the name of your resource group. Run `az group list` to list the resource groups for your subscription.

- `$LOCATION` : This should be set to your location, such as `westus` . For a list of available locations, run `az account list-locations` .
- `$STORAGE_NAME` : This should be set to your BOSH storage account name. Run `az storage account list` to list your storage accounts.

5. Retrieve the connection string for the account.

```
$ az storage account show-connection-string \
--name $STORAGE_NAME --resource-group $RESOURCE_GROUP
```

The command returns output similar to the following:

```
{
  "connectionString": "DefaultEndpointsProtocol=https;EndpointSuffix=core.windows.net;AccountName=cfdocsboshstorage;AccountKey=EXAMPLExXXXXXXXXXXXXLprnc5igFyYWsgq0"
}
```

6. From the `data:` field in the output above, record the full value of `connectionString` from the output above, starting with and including `DefaultEndpointsProtocol=` .
7. Export the value of `connectionString` as the environment variable `$AZURE_STORAGE_CONNECTION_STRING` .

```
$ export AZURE_STORAGE_CONNECTION_STRING="YOUR-ACCOUNT-KEY-STRING"
```

Copy the Ops Manager Image

Copy the Ops Manager image into your storage account. You use the Ops Manager image to create the VM that hosts that the new version of Ops Manager.

To copy the Ops Manager image into your storage account, do the following:

1. Navigate to [Pivotal Network](#) and download the release of **Pivotal Cloud Foundry Ops Manager for Azure** you want to upgrade to.
2. View the downloaded PDF and locate the Ops Manager image URL appropriate for your region.
3. Export the Ops Manager image URL as an environment variable.

```
$ export OPS_MAN_IMAGE_URL="YOUR-OPS-MAN-IMAGE-URL"
```

This command overrides the old Ops Manager image URL with the new Ops Manager image URL.

4. Copy the Ops Manager image into your storage account. For compatibility when upgrading to future versions of Ops Manager, choose a unique name for the image that includes the Ops Manager version number. For example, replace `opsman-image-version` in the following examples with `opsman-image-2.0.1` .

```
$ az storage blob copy start --source-uri $OPS_MAN_IMAGE_URL \
--connection-string $AZURE_STORAGE_CONNECTION_STRING \
--destination-container opsmanager \
--destination-blob opsman-image-version.vhd
```

5. Copying the image may take several minutes. Run the following command and examine the output under `"copy"` :

```
$ az storage blob show --name opsman-image-version.vhd \
--container-name opsmanager \
--account-name $STORAGE_NAME
...
"copy": {
  "completionTime": "2017-06-26T22:24:11+00:00",
  "id": "b9c8b272-a562-4574-baa6-fla04afcefd",
  "progress": "53687091712/53687091712",
  "source": "https://opsmanagerwestus.blob.core.windows.net/images/ops-manager-2.0.x.vhd",
  "status": "success",
  "statusDescription": null
},
```

When `status` reads `success` , continue to the next step.

Configure Ops Manager IP Address

Remove the old Ops Manager VM and record the IP address for the Ops Manager network interface. You use this IP address when creating the new Ops Manager VM that hosts the upgraded version of Ops Manager.

To configure the Ops Manager IP address, do one of the following:

- [Reuse the existing dynamic public IP address.](#)
- [Use a new dynamic public IP address.](#)

Reuse Existing Dynamic Public IP Address

To reuse an existing dynamic public IP address, do the following:

1. List your VMs and record the name of your Ops Manager VM:

```
$ az vm list
```

2. Delete your old Ops Manager VM:

```
$ az vm delete --name YOUR-OPS-MAN-VM --resource-group $RESOURCE_GROUP
```

3. List your network interfaces and record the name of the Ops Manager network interface:

```
$ az resource list --resource-group $RESOURCE_GROUP \
--resource-type Microsoft.Network/networkInterfaces
```

Use a New Dynamic Public IP Address

To use a new dynamic public IP address, do the following:

1. Create a new public IP address named `ops-manager-ip-new`.

```
$ az network public-ip create --name ops-manager-ip-new \
--resource-group $RESOURCE_GROUP --location $LOCATION \
--allocation-method Static
{
  "publicIp": {
    "dnsSettings": null,
    "etag": "W/\"4450ebe2-9e97-4b17-9ef2-44838339c661\"",
    "id": "/subscriptions/995b7eed-77cf-45ff-a5c9-1a405ffb8243/resourceGroups/cf-docs/providers/Microsoft.Network/publicIPAddresses/ops-manager-ip-new",
    "idleTimeoutInMinutes": 4,
    "ipAddress": "40.83.148.183",
    "ipConfiguration": null,
    "location": "westus",
    "name": "ops-manager-ip-new",
    "provisioningState": "Succeeded",
    "publicIpAddressVersion": "IPv4",
    "publicIpAllocationMethod": "Static",
    "resourceGroup": "cf-docs",
    "resourceGuid": "950d4831-1bec-42da-8a79-959beddea9dd",
    "tags": null,
    "type": "Microsoft.Network/publicIPAddresses"
  }
}
```

2. Record the value for `ipAddress` from the output above. This is the public IP address of Ops Manager.

3. Create a network interface for Ops Manager.

```
$ az network nic create --vnet-name pcf-net \
--subnet pcf --network-security-group opsmgr-nsg \
--private-ip-address 10.0.0.5 \
--public-ip-address ops-manager-ip-new \
--resource-group $RESOURCE_GROUP \
--name ops-manager-nic-new --location $LOCATION
```

4. Shut down your old Ops Manager VM, if it still exists:

```
$ az vm deallocate --name ops-manager --resource-group $RESOURCE_GROUP
```

If your Ops Manager VM is not named `ops-manager`, provide the correct name. To list all VMs in your account, use `az vm list`.

5. Update your DNS record to point to your new public IP address of Ops Manager.

Create Ops Manager VM Instance

Create an Ops Manager VM instance to host the new version of Ops Manager.

To create an Ops Manager VM instance, do the following:

1. To use the key pair from your previous Ops Manager, locate the path to the file on your local machine. To create a new key pair, enter the following command:

```
$ ssh-keygen -t rsa -f opsman -C ubuntu
```

When prompted for a passphrase, press the `enter` key to provide an empty passphrase.

2. Create the Ops Manager VM.

- If you are using unmanaged disks, run the following command to create your Ops Manager VM, replacing `PATH-TO-PUBLIC-KEY` with the path to your public key .pub file, and replacing `opsman-image-version` with the version of Ops Manager you are deploying, for example

```
opsman-image-2.0.1 :
```

```
$ az vm create --name opsman-version --resource-group $RESOURCE_GROUP \
--location $LOCATION \
--nics opsman-nic \
--image https://$STORAGE_NAME.my-azure-instance.com/opsmanager/opsman-image-version.vhd \
--os-disk-name opsman-version-osdisk \
--os-disk-size-gb 128 \
--os-type Linux \
--use-unmanaged-disk \
--storage-account $STORAGENAME \
--storage-container-name opsmanager \
--admin-username ubuntu \
--ssh-key-value PATH-TO-PUBLIC-KEY
```

Replace `my-azure-instance.com` with the URL of your Azure instance. Find the complete source URL in the Azure UI by viewing the **Blob properties** of the Ops Manager image you created earlier in this procedure.

- If you are using Azure managed disks, perform the following steps, replacing `opsman-image-version` with the version of Ops Manager you are deploying, for example `opsman-image-2.0.1` .:

1. Create a managed image from the Ops Manager VHD file:

```
$ az image create --resource-group $RESOURCE_GROUP \
--name opsman-image-version \
--source https://$STORAGE_NAME.blob.core.windows.net/opsmanager/opsman-image-version.vhd \
--location $LOCATION \
--os-type Linux
```


If you are using Azure China, Azure Government Cloud, or Azure Germany, replace `blob.core.windows.net` with the following:

- For Azure China, use `blob.core.chinacloudapi.cn`. See the [Azure documentation](#) for more information.
- For Azure Government Cloud, use `blob.core.usgovcloudapi.net`. See the [Azure documentation](#) for more information.
- For Azure Germany, use `blob.core.cloudapi.de`. See the [Azure documentation](#) for more information.

2. Create your Ops Manager VM, replacing `PATH-TO-PUBLIC-KEY` with the path to your public key `.pub` file, and replacing `opsman-version` and `opsman-image-version` with the version of Ops Manager you are deploying, for example `opsman-2.0.1`, `opsman-2.0.1-osdisk`, and `opsman-image-2.0.1`.

```
$ az vm create --name opsman-version --resource-group $RESOURCE_GROUP \
--location $LOCATION \
--nics opsman-nic \
--image opsman-image-version \
--os-disk-name opsman-version-osdisk \
--admin-username ubuntu \
--size Standard_DS2_v2 \
--storage-sku Standard_LRS \
--ssh-key-value PATH-TO-PUBLIC-KEY
```

3. If you have deployed more than one tile in this Ops Manager installation, perform the following steps to increase the size of the Ops Manager VM disk. You can repeat this process and increase the disk again at a later time if necessary.

 **Note:** If you use Azure Stack, you must increase the Ops Manager VM disk size using the Azure Stack UI.

- a. Run the following command to stop the VM and detach the disk, replacing `opsman-version` with the version of Ops Manager you are deploying, for example `opsman-2.0.1`:

```
$ az vm deallocate --name opsman-version \
--resource-group $RESOURCE_GROUP
```

- b. Run the following command to resize the disk to 128 GB, replacing `opsman-version` with the version of Ops Manager you are deploying, for example `opsman-2.0.1`:

```
$ az disk update --size-gb 128 --name opsman-version-osdisk \
--resource-group $RESOURCE_GROUP
```

- c. Run the following command to start the VM, replacing `opsman-version` with the version of Ops Manager you are deploying, for example `opsman-2.0.1`:

```
$ az vm start --name opsman-version --resource-group $RESOURCE_GROUP
```

Next Steps

After you complete this procedure, continue the upgrade instructions in [Upgrading Pivotal Cloud Foundry](#) topic.

Installing Pivotal Cloud Foundry on GCP

Page last updated:

This topic describes how to install [Pivotal Cloud Foundry](#) (PCF) on Google Cloud Platform (GCP).

It includes resource requirements, prerequisites, instructions for installing PCF on GCP, and additional resources.

Overview

You can install PCF on GCP with either the Pivotal Application Service (PAS) or Pivotal Container Service (PKS) runtime. There are resource requirements specific to each runtime. Ensure you meet the requirements for your runtime and the requirements specific to GCP before installing PCF on GCP.

Requirements

This section lists the following resource requirements for installing PCF on GCP:

- General PCF resource requirements. See [PCF Resource Requirements](#).
- GCP-specific resource requirements. See [GCP Resource Requirements](#).

PCF Resource Requirements

This section lists PCF resource requirements for installing PCF on GCP. It includes general PCF resource requirements for both the PAS and PKS runtimes.

View one of the following, depending on your PCF runtime:


- PAS-specific PCF resource requirements. See [PAS Resource Requirements](#).
- PKS-specific PCF resource requirements. See [PKS Resource Requirements](#).

PAS Resource Requirements

The following are general resource requirements for deploying and managing a PCF deployment with Ops Manager and PAS:

- PAS requires sufficient IP allocation. The following lists the minimum required IP allocations:
 - One static IP address for either HAProxy or one of your Gorouters
 - One static IP address for each job in the Ops Manager tile. See the Ops Manager **Resource Config** pane for each tile for a full list.
 - One static IP address for each job listed below:
 - Consul
 - NATS
 - File Storage
 - MySQL Proxy
 - MySQL Server
 - Backup Restore Node
 - HAProxy
 - Router
 - MySQL Monitor
 - Diego Brain
 - TCP Router
 - One IP for each VM instance created by the service.
 - An additional IP address for each compilation worker. Use the following formula to determine the total IPs required:

$$\text{IPs needed} = \text{static IPs} + \text{VM instances} + \text{compilation workers}$$
 - Pivotal recommends that you allocate at least 36 dynamic IP addresses when deploying Ops Manager and PAS. BOSH requires additional dynamic IP addresses during installation to compile and deploy VMs, install PAS, and connect to services.
- Pivotal recommends using a network without DHCP for deploying PAS VMs.

 **Note:** If you have DHCP, refer to the [Troubleshooting Guide](#) to avoid issues with your installation.

PKS Resource Requirements


For PKS-specific resource requirements, see [GCP Prerequisites and Resource Requirements](#).

GCP Resource Requirements

The following are GCP-specific resource requirements for installing PCF on GCP:

- Installing PCF on GCP requires a minimum of the following VM instance limits in your GCP account. The number of VMs required depends on the number of tiles and availability zones you plan to deploy. The following VM guidelines apply to the PAS and Small Footprint PAS runtimes:
 - PAS:** At a minimum, a new GCP deployment requires the following `custom` VMs for PAS and Ops Manager:

| VM Count | vCPU Count per VM | RAM (GB) |
|----------|-------------------|----------|
| 30 | 1 | 1 |
| 3 | 1 | 2 |
| 4 | 2 | 4 |
| 3 | 2 | 8 |
| 3 | 4 | 16 |

 **Note:** If you are deploying a test or sandbox PCF that does not require high availability, then you can scale down the number of VM instances in your deployment. For more information, see [Scaling PAS](#).

- Small Footprint PAS:** At a minimum, a new GCP deployment requires the following VMs to run Small Footprint PAS:

| | VM Type | VM Count | vCPU Count per VM | RAM (GB) | Notes |
|---------------------|-------------|----------|-------------------|----------|------------------------------------|
| Small Footprint PAS | micro | 12 | 1 | 1 | Add 1 to VM count if using HAProxy |
| | small | 3 | 1 | 2 | |
| | xlarge.disk | 1 | 4 | 16 | |
| | xlarge | 1 | 4 | 16 | |
| | medium.mem | 1 | 1 | 6 | |
| | large.disk | 1 | 2 | 8 | |
| Ops Manager | large.disk | 1 | 2 | 8 | |
| | large.cpu | 4 | 4 | 4 | |


- PKS:** See [GCP Prerequisites and Resource Requirements](#).
- (PAS-only) Your GCP project must have sufficient quota to deploy all the VMs needed to install PCF with PAS. For a list of suggested quotas, see [Recommended GCP Quotas](#).

Prerequisites


To install PCF on GCP, you must do the following:

- Install the Google Cloud SDK on your machine and authenticate it to your GCP account. To download the Google Cloud SDK, see [Google Cloud SDK](#).
- Increase or remove the VM instance limits in your GCP account. For VM instance requirements, see [GCP Resource Requirements](#).
- Update your GCP account with the following required permissions:
 - The following permissions are required to create firewalls, networks, load balancers, and other resources:
 - Compute Engine > Compute Instances Admin (beta)
 - Compute Engine > Compute Network Admin
 - Compute Engine > Compute Security Admin

- To use Google Cloud Storage (GCS) for Cloud Controller file storage, the following permission is required to create buckets:
 - **Storage > Storage Admin**
- To use Cloud DNS, the following permission is required to add and modify DNS entries:
 - **Project > Editor**
- Create an SSL certificate for your PCF domain.

 **Note:** To deploy PCF to a production environment, you must obtain a certificate from a certificate authority. Pivotal recommends using a self-signed certificate generated by Ops Manager for development and testing purposes only.

- Assign administrative rights to a domain for PCF. You need to be able to add wildcard records to this domain.
- Create a wildcard DNS record that points to your router or load balancer. Alternatively, you can use a service such as xip.io. For example, `203.0.113.0.xip.io`. Then, create at least one wildcard TLS certificate that matches the DNS record you configured.

 **Note:** With a wildcard DNS record, every hostname in your domain resolves to the IP address of your router or load balancer. For example, if you create a DNS record `*.example.com` pointing to your router, every app deployed to the `example.com` domain resolves to the IP address of your router.

- Create one or more NTP servers, if the NTP servers are not already provided by your GCP project.
- Install the most recent version of one of the following CLIs, depending on your PCF runtime:
 - **PAS:** The Cloud Foundry Command Line Interface (cf CLI). See [Cloud Foundry Command Line Interface](#) in GitHub.
 - **PKS:** The PKS CLI. See [Installing the PKS CLI](#).
- **(PAS-only)** Request a quota increase for your GCP project. For GCP quota requirements, see [GCP Resource Requirements](#). To request an increase, see [Quotas](#) in the GCP console.
- **(PAS-only)** Configure sufficient IP allocation. For more information about IP allocation requirements, see [PAS Resource Requirements](#).
- **(Optional) (PAS-only)** Configure external storage. Pivotal recommends using external storage if possible. For more information about how file storage location affects platform performance and stability during upgrades, see [Configure File Storage](#).
- **(Optional) (PAS and Ops Manager-only)** Configure external databases. Pivotal recommends using external databases in production deployments for BOSH Director and PAS. An external database must be configured to use the UTC timezone.
- **(Optional) (PAS and Ops Manager-only)** Configure external user stores. When you deploy PCF, you can select a SAML user store for Ops Manager or a SAML or LDAP user store for PAS, to integrate existing user accounts.

Install PCF on GCP

You can install PCF on GCP either manually or using Terraform.

To install PCF on GCP, do one of the following:

- Install PCF on GCP manually. See [Installing PCF on GCP Manually](#).
- Install PCF on GCP using Terraform. See [Install PCF on GCP Using Terraform](#).

Additional Resources

The following are additional resources related to installing PCF on GCP:

- For general authentication guidelines for GCP, see [GCP authentication documentation](#).
- For more information about troubleshooting the PCF on GCP infrastructure, see [Troubleshooting PCF on GCP](#).
- For production-level deployment options for PCF on GCP, see [Reference Architecture for Pivotal Cloud Foundry on GCP](#).
- For general certificate requirements for deploying PCF, see [Certificate Requirements](#).

Recommended GCP Quotas

Page last updated:

Default quotas on a new GCP subscription do not have enough quota for a typical production-level PCF deployment.

The following table lists recommended resource quotas for a single PCF deployment.

| Metric | Resource | Suggested Minimum Quota |
|-----------------------------------|----------|-------------------------|
| CPUs | Regional | 150 [*] |
| Firewall rules | Global | 15 |
| Forwarding rules | Global | 15 |
| Backend services | Global | 5 |
| Health checks | Global | 5 |
| Images | Global | 10 |
| Static IP addresses ^{**} | Regional | 5 |
| In-use IP addresses | Global | 5 |
| In-use IP addresses ^{**} | Regional | 5 |
| Networks | Global | 5 |
| Subnetworks | Global | 5 |
| Routes | Global | 20 |
| Target pools | Global | 5 |
| Target HTTP proxies | Global | 5 |
| Target HTTPS proxies | Global | 5 |
| Persistent Disk Standard (GB) | Regional | 15,000 |

^{*} Assuming a deployment with 100 app instances.

^{**} Assuming a SNAT topology.

To view production-level deployment options for PCF on GCP, see the [Reference Architecture for Pivotal Cloud Foundry on GCP](#).

For instructions on how to set up GCP resources required to deploy PCF, see [Preparing to Deploy Ops Manager on GCP Manually](#).

Installing PCF on GCP Manually

This topic explains how to install PCF on GCP manually.

Overview

You can install PCF on GCP with either the Pivotal Application Service (PAS) or Pivotal Container Service (PKS) runtime.

To install PCF on GCP manually, do one of the following:

- Install with PAS. See [Install Manually with PAS](#).
- Install with PKS. See [Install Manually with PKS](#).

Install Manually with PAS

To install manually with PAS, do the following:

1. Prepare to deploy Ops Manager. See [Preparing to Deploy Ops Manager on GCP Manually](#).
2. Deploy Ops Manager. See [Deploying Ops Manager on GCP Manually](#).
3. Configure BOSH Director. See [Configuring BOSH Director on GCP Manually](#).
4. (Optional). Configure a shared VPC. See [\(Optional\) Configuring a Shared VPC on GCP](#).
5. Configure PAS. See [Deploying PAS on GCP](#).

Install Manually with PKS

To install manually with PKS, do the following:

1. Prepare to deploy Ops Manager. See [Preparing to Deploy Ops Manager on GCP Manually](#).
2. Deploy Ops Manager. See [Deploying Ops Manager on GCP Manually](#).
3. Configure BOSH Director. See [Configuring BOSH Director on GCP Manually](#).
4. (Optional). Configure a shared VPC. See [\(Optional\) Configuring a Shared VPC on GCP](#).
5. Configure PKS. See [Installing PKS on GCP](#).

Preparing to Deploy Ops Manager on GCP Manually

Page last updated:

This topic describes the preparation steps required to install Ops Manager for Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP).

Prerequisites

Before you prepare your Ops Manager installation, do the following depending on the runtime you intend to deploy:

- If you are deploying Pivotal Application Service (PAS), see [PCF on GCP Requirements](#).
- If you are deploying Pivotal Container Service (PKS), see [GCP Prerequisites and Resource Requirements](#).

Configuration and Components

This section outlines high-level infrastructure options for PCF on GCP. A PCF deployment includes Ops Manager and your chosen runtime. For example, both Ops Manager with PAS and Ops Manager with PKS are PCF deployments. For more information, review the deployment options and recommendations in [Reference Architecture for Pivotal Cloud Foundry on GCP](#).

When deploying PCF on GCP, Pivotal recommends using the following GCP components:

- [Google Cloud SQL](#) for external database services
- [NAT Gateway Instances](#) to limit the number of VMs with public IP addresses
- [Google Cloud Storage](#) for external file storage

For more information, review the different deployment options and recommendations in [Reference Architecture for Pivotal Cloud Foundry on GCP](#).

Step 1: Set up an IAM Service Account

1. From the GCP console, select **IAM & Admin**, then **Service accounts**.

2. Click **Create Service Account**:

- **Service account name:** Enter a name. For example, `bosh`.
- **Role:** Select the following roles:
 - **Service Accounts > Service Account User**
 - **Service Accounts > Service Account Token Creator**
 - **Compute Engine > Compute Instance Admin (v1)**
 - **Compute Engine > Compute Network Admin**
 - **Compute Engine > Compute Storage Admin**
 - **Storage > Storage Admin**



Note: You must scroll down in the pop-up windows to select all required roles.

The **Service Account User** role is only required if you plan to use **The Ops Manager VM Service Account** to deploy Ops Manager. For more information about **The Ops Manager VM Service Account**, see [Step 2: Google Cloud Platform Config in Configuring BOSH Director on GCP](#).

- **Service account ID:** The field automatically generates a unique ID based on the username.
- **Furnish a new private key:** Select this checkbox and JSON as the **Key type**.

Create service account

Service account name ?
bosh

Service account ID
bosh-48 @cf-sf-onboarding-env-3.iam.g...

☒ **Furnish a new private key**
Downloads a file that contains the private key. Store the file in a secure location. The private key can't be recovered if lost.

Key type
☒ **JSON**
Recommended
☐ **P12**
For backward compatibility with code using the P12 format

☐ **Enable G Suite Domain-wide Delegation**
Allows this service account to be authorized to access all resources in the domain without manual authorization on their part. [Learn more](#)

Role ?
Compute Instance Admin (v1)

Selected

- ✓ Compute Instance Admin (v1)
- ✓ Compute Network Admin
- ✓ Compute Storage Admin
- ✓ Service Account Token Creator
- ✓ Service Account User
- ✓ Storage Admin

Project

- App Engine
- BigQuery
- Billing
- Cloud IAP
- Cloud KMS
- Cloud SQL
- Cloud Security Scanner

3. Click **Create**. Your browser automatically downloads a JSON file with a private key for this account. Save this file in a secure location.

Step 2: Enable Google Cloud APIs

Ops Manager manages GCP resources using the Google Compute Engine and Cloud Resource Manager APIs. To enable these APIs, do the following:

1. Log in to the Google Developers Console at <https://console.developers.google.com>.
2. In the console, navigate to the GCP project where you want to install Ops Manager.
3. Select **API Manager > Library**.
4. Under **Google Cloud APIs**, select **Compute Engine API**.
5. On the **Google Compute Engine API** page, click **Enable**.
6. In the search field, enter `Google Cloud Resource Manager API`.
7. On the **Google Cloud Resource Manager API** page, click **Enable**.
8. To verify that the APIs have been enabled, do the following:
 - a. Log in to GCP using the IAM service account you created in [Set up an IAM Service Account](#):

```
$ gcloud auth activate-service-account --key-file JSON_KEY_FILENAME
```

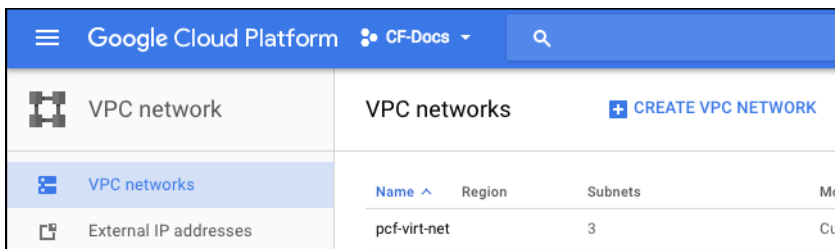
- b. List your projects:

```
$ gcloud projects list
PROJECT_ID      NAME      PROJECT_NUMBER
my-project-id   my-project-name   #####
```

This command lists the projects where you enabled Google Cloud APIs.

Step 3: Create a GCP Network with Subnets

1. Log in to the [GCP console](#).
2. Navigate to the GCP project where you want to install Ops Manager.
3. Select **VPC network**, then **CREATE VPC NETWORK**.



4. In the **Name** field, enter a name of your choice for the VPC network. This name helps you identify resources for this deployment in the GCP console. Network names must be lowercase. For example, `pcf-virt-net`.

[←](#)
Create a VPC network

Name

- a. Under **Subnets**, complete the form as follows to create an infrastructure subnet for Ops Manager and NAT instances:

| | |
|-------------------------|--|
| Name | <p><code>pcf-infrastructure-subnet-GCP-REGION</code></p> <p>Example: <code>pcf-infrastructure-subnet-us-west1</code></p> |
| Region | <p>A region that supports three availability zones. For help selecting the correct region for your deployment, see the Google documentation about regions and zones.</p> |
| IP address range | <p>A CIDR ending in <code>/26</code></p> <p>Example: <code>192.168.101.0/26</code></p> |

See the following image for an example:

New subnet

Name ?

pcf-subnet-infrastructure-us-west1

Add a description

Region ?

us-west1

IP address range ?

192.168.101.0/26

Create secondary IP range

Private Google access ?


☐ On
 ☒ Off

Flow logs

☐ On
 ☒ Off

Done

Cancel

 **Note:** For deployments that do not use external IP addresses, enable **Private Google access** to allow your runtime to make API calls to Google services.

- b. Click **Add subnet** to add a second subnet for the BOSH Director and components specific to your runtime. Complete the form as follows:

| | |
|------------------|---|
| Name | pcf-RUNTIME-subnet-GCP-REGION Example: pcf-pas-subnet-us-west1 |
| Region | The same region you selected for the infrastructure subnet |
| IP address range | A CIDR ending in /22 Example: 192.168.16.0/22 |

- c. Click **Add subnet** to add a third **Subnet** with the following details:

| | |
|--------|---|
| Name | pcf-services-subnet-GCP-REGION Example: pcf-services-subnet-us-west1 |
| Region | The same region you selected for the previous subnets |
| | |

| | |
|---|--|
| IP address range | A CIDR in <input type="text" value="/22"/> |
| Example: <input type="text" value="192.168.20.0/22"/> | |

See the following image for an example:

| VPC networks + CREATE VPC NETWORK REFRESH | | | | | | | |
|---|----------|------------------------------------|--------|---------------------|---------------|----------------|------------------------|
| Name ^ | Region | Subnets | Mode | IP addresses ranges | Gateways | Firewall Rules | Global dynamic routing |
| pcf-virt-network | | 3 | Custom | | | 0 | Off |
| | us-west1 | pcf-subnet-ert-us-west1 | | 192.168.16.0/22 | 192.168.16.1 | | |
| | us-west1 | pcf-subnet-infrastructure-us-west1 | | 192.168.101.0/26 | 192.168.101.1 | | |
| | us-west1 | pcf-subnet-services-us-west1 | | 192.168.20.0/22 | 192.168.20.1 | | |

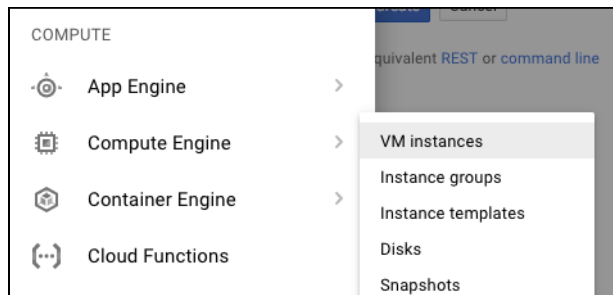
- Under **Dynamic routing mode**, leave **Regional** selected.
- Click **Create**.

Step 4: Create NAT Instances

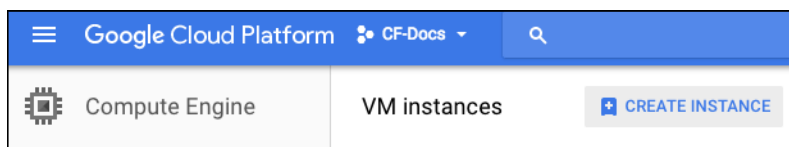
Use NAT instances when you want to expose only a minimal number of public IP addresses.

Creating NAT instances permits internet access from cluster VMs. You might, for example, need this internet access for pulling Docker images or enabling internet access for your workloads.

For more information, see [Reference Architecture for Pivotal Cloud Foundry on GCP](#) and [GCP documentation](#).



- In the console, navigate to **Compute Engine** > **VM instances**.



- Click **CREATE INSTANCE**.

- Complete the following fields:

- Name:** Enter . This is the first, or primary, of three NAT instances you need. If you use a single AZ, you need only one NAT instance.
- Zone:** Select the first zone from your region. Example: For region , select zone .
- Machine type:** Select .
- Boot disk:** Click **Change** and select .

Create an instance

Name [?]
pcf-nat-gateway-pri

Zone [?]
us-west1-a

Machine type
4 vCPUs 15 GB memory [Customize](#)

Boot disk [?]
New 10 GB standard persistent disk
Image
Ubuntu 14.04 LTS [Change](#)

4. Expand the additional configuration fields by clicking **Management, disks, networking, SSH keys**.

Firewall [?]
Add tags and firewall rules to allow specific network traffic from the Internet

☐ Allow HTTP traffic
☐ Allow HTTPS traffic

Management, disks, networking, SSH keys

- a. In the **Startup script** field under **Automation**, enter the following text:

```
#!/bin/bash
sudo sysctl -w net.ipv4.ip_forward=1
sudo sh -c 'echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf'
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Automation

Startup script (Optional)
You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine. [Learn more](#)

```
#!/bin/bash
sudo sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
```

Management Disks **Networking** SSH Keys

Network tags [?] (Optional)
nat-traverse x pcf-nat-instance x

5. Click **Networking** to open additional network configuration fields:

- In the **Network tags** field, add the following: `nat-traverse` and `pcf-nat-instance`.
- Click on the **Networking** tab and the pencil icon to edit the **Network interface**.
- For **Network**, select `pcf-virt-net`. You created this network in [Step 1: Create a GCP Network with Subnets](#).
- For **Subnetwork**, select `pcf-infrastructure-subnet-GCP-REGION`.
- For **Primary internal IP**, select `Ephemeral (Custom)`. Enter an IP address, for example, `192.168.101.2`, in the **Custom ephemeral IP address** field. The IP address must meet the following requirements:
 - The IP address must exist in the CIDR range you set for the `pcf-infrastructure-subnet-GCP-REGION` subnet.
 - The IP address must exist in a reserved IP range set later in BOSH Director. The reserved range is typically the first `.1` through `.9` addresses in the CIDR range you set for the `pcf-infrastructure-subnet-GCP-REGION` subnet.
 - The IP address cannot be the same as the Gateway IP address set later in Ops Manager. The Gateway IP address is typically the first `.1` address in the CIDR range you set for the `pcf-infrastructure-subnet-GCP-REGION` subnet.
- For **External IP**, select `Ephemeral`.

Note: If you select a static external IP address for the NAT instance, then you can use the static IP to further secure access to your CloudSQL instances.

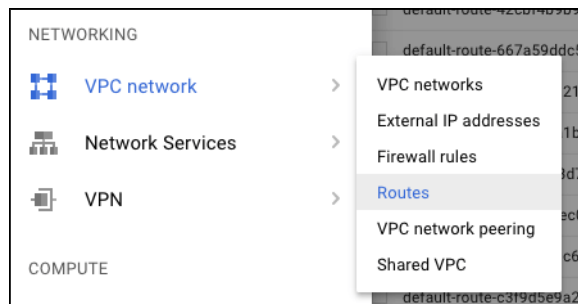
- g. Set **IP forwarding** to **On**.
- h. Click **Done**.

6. Click **Create** to finish creating the NAT instance.

7. Repeat steps 2-6 to create two additional NAT instances with the names and zones specified in the table below. The rest of the configuration remains the same.

| | | |
|------------|-------------|---|
| Instance 2 | Name | pcf-nat-gateway-sec |
| | Zone | Select the second zone from your region. Example: For region <code>us-west1</code> , select zone <code>us-west1-b</code> . |
| | Internal IP | Select Custom and enter an IP address in the Internal IP address field. Example: <code>192.168.101.3</code> . As described above, this address must in the CIDR range you set for the <code>pcf-infrastructure-subnet-GCP-REGION</code> subnet, must exist in a reserved IP range set later in BOSH Director, and cannot be the same as the Gateway IP address set later in Ops Manager. |
| Instance 3 | Name | pcf-nat-gateway-ter |
| | Zone | Select the third zone from your region. Example: For region <code>us-west1</code> , select zone <code>us-west1-c</code> . |
| | Internal IP | Select Custom and enter an IP address in the Internal IP address field. Example: <code>192.168.101.4</code> . As described above, this address must in the CIDR range you set for the <code>pcf-infrastructure-subnet-GCP-REGION</code> subnet, must exist in a reserved IP range set later in BOSH Director, and cannot be the same as the Gateway IP address set later in Ops Manager. |

Create Routes for NAT Instances



1. In the GCP console, navigate to **VPC Networks > Routes**.

2. Click **CREATE ROUTE**.

3. Complete the form as follows:

- o **Name:** `pcf-nat-pri`
- o **Network:** `pcf-virt-net`
- o **Destination IP range:** `0.0.0.0/0`
- o **Priority:** `800`
- o **Instance tags:** `pcf`
- o **Next hop:** `Specify an instance`
- o **Next hop instance:** `pcf-nat-gateway-pri`

4. Click **Create** to finish creating the route.

5. Repeat steps 2-4 to create two additional routes with the names and next hop instances specified in the table below. The rest of the configuration remains the same.

| | |
|---------|---|
| Route 2 | Name: <code>pcf-nat-sec</code> Next hop instance: <code>pcf-nat-gateway-sec</code> |
| Route 3 | Name: <code>pcf-nat-ter</code> Next hop instance: <code>pcf-nat-gateway-ter</code> |


Step 5: Create Firewall Rules for the Network

GCP lets you assign tags to VM instances and create firewall rules that apply to VMs based on their tags. For more information about tags, see [Labeling Resources](#) in the Google Cloud documentation. This step assigns tags and firewall rules to Ops Manager components and VMs that handle incoming traffic.

1. In the **Networking** > **VPC network** pane, select **Firewall rules**.
2. Apply the firewall rules in the following table:

| Firewall Rules | |
|-------------------|---|
| Rule 1 | <p>This rule allows SSH from public networks.</p> <p>Name: <code>pcf-allow-ssh</code></p> <p>Network: <code>pcf-virt-net</code></p> <p>Allowed protocols and ports: <code>tcp:22</code></p> <p>Source filter: IP ranges</p> <p>Source IP ranges: <code>0.0.0.0/0</code></p> <p>Target tags: <code>allow-ssh</code></p> |
| Rule 2 | <p>This rule allows HTTP from public networks.</p> <p>Name: <code>pcf-allow-http</code></p> <p>Network: <code>pcf-virt-net</code></p> <p>Allowed protocols and ports: <code>tcp:80</code></p> <p>Source filter: IP ranges</p> <p>Source IP ranges: <code>0.0.0.0/0</code></p> <p>Target tags: <code>allow-http</code>, <code>router</code></p> |
| Rule 3 | <p>This rule allows HTTPS from public networks.</p> <p>Name: <code>pcf-allow-https</code></p> <p>Network: <code>pcf-virt-net</code></p> <p>Allowed protocols and ports: <code>tcp:443</code></p> <p>Source filter: IP ranges</p> <p>Source IP ranges: <code>0.0.0.0/0</code></p> <p>Target tags: <code>allow-https</code>, <code>router</code></p> |
| Rule 4 | <p>This rule allows Gorouter health checks.</p> <p>Name: <code>pcf-allow-http-8080</code></p> <p>Network: <code>pcf-virt-net</code></p> <p>Allowed protocols and ports: <code>tcp:8080</code></p> <p>Source filter: IP ranges</p> <p>Source IP Ranges: <code>0.0.0.0/0</code></p> <p>Target tags: <code>router</code></p> |
| Rule 5 | <p>This rule allows communication between BOSH-deployed jobs.</p> <p>Name: <code>pcf-allow-pas-all</code></p> <p>Network: <code>pcf-virt-net</code></p> <p>Allowed protocols and ports: <code>tcp;udp;icmp</code></p> <p>Source filter: Source tags</p> <p>Target tags: <code>pcf</code>, <code>pcf-opsman</code>, <code>nat-traverse</code></p> <p>Source tags: <code>pcf</code>, <code>pcf-opsman</code>, <code>nat-traverse</code></p> |
| Rule 6 (Optional) | <p>This rule allows access to the TCP router.</p> <p>Name: <code>pcf-allow-cf-tcp</code></p> <p>Network: <code>pcf-virt-net</code></p> <p>Source filter: IP ranges</p> <p>Source IP ranges: <code>0.0.0.0/0</code></p> <p>Allowed protocols and ports: <code>tcp:1024-65535</code></p> <p>Target tags: <code>pcf-cf-tcp</code></p> |
| | <p>This rule allows access to the SSH proxy.</p> <p>Name: <code>pcf-allow-ssh-proxy</code></p> |

| | |
|-------------------|--|
| Rule 7 (Optional) | Network: <code>pcf-virt-net</code> Source filter: IP ranges Source IP ranges: <code>0.0.0.0/0</code> Allowed protocols and ports: <code>tcp:2222</code> Target tags: <code>pcf-ssh-proxy</code> , <code>diego-brain</code> |
|-------------------|--|

 **Note:** If you want your firewall rules to only permit traffic within your private network, modify the **Source IP Ranges** from the table accordingly.

3. If you are only using your GCP project to deploy Ops Manager, then you can delete the following default firewall rules:

- `default-allow-http`
- `default-allow-https`
- `default-allow-icmp`
- `default-allow-internal`
- `default-allow-rdp`
- `default-allow-ssh`


If you are deploying **PKS only**, continue to [Next Steps](#).

If you are deploying **PAS or other runtimes**, proceed to the following step.

Step 6: Create Database Instance and Databases

Create Database Instance

1. From the GCP console, select **SQL** and click **CREATE INSTANCE**.
2. Ensure **MySQL** is selected and click **Next**.
3. Under **MySQL**, select instance type **Second Generation**.
4. Click **Configure MySQL** under your choice for instance type: Development, Staging, or Production.
5. Configure the instance as follows:
 - **Instance ID:** `pcf-pas-sql`
 - **Root password:** Set a password for the root user.
 - **Region:** Select the region you specified when creating networks.
 - **Zone:** Any.
 - **Configure machine type and storage:**
 - Click **Change** and then select **db-n1-standard-2**.
 - Ensure that **Enable automatic storage increases** is selected. This allows DB storage to grow automatically when space is required.
 - **Enable auto backups and high availability:** Make the following selections:
 - Leave **Automate backups** and **Enable binary logging** selected.
 - Under **High availability**, select the **Create failover replica** checkbox.
 - **Authorize Networks:** Click **Add network** and create a network named `all` that allows traffic from `0.0.0.0/0`.

 **Note:** If you assigned static IP addresses to your NAT instances, you can instead limit access to the database instances by specifying the NAT IP addresses.

6. Click **Create**.

Create Databases


1. From the **Instances** page, select the database instance you just created.
2. Select the **Databases** tab.

3. Click **Create database** to create the following databases:

- o account
- o app_usage_service
- o autoscale
- o cddb
- o console
- o diego
- o locket
- o networkpolicyserver
- o nfsvolume
- o notifications
- o routing
- o silk
- o uaa
- o credhub

4. Select the **USERS** tab.

5. Click **Create user account** to create a unique username and password for each database you created above. For **Host name**, select **Allow any host**. You must create a total of fourteen user accounts.

 **Note:** Ensure that the networkpolicyserver database user has the **ALL PRIVILEGES** permission.

Step 7: Create Storage Buckets

1. From the GCP Console, select **Storage** > **Browser**.

2. Using **CREATE BUCKET**, create buckets with the following names. For **Default storage class**, select **Multi-Regional**:

- o pcf-buildpacks
- o pcf-droplets
- o pcf-packages
- o pcf-resources

Step 8: Create HTTP Load Balancer

Create Instance Group

1. Navigate to **Compute Engine** > **Instance groups**.

2. Click **CREATE INSTANCE GROUP**.

3. Complete the form as follows:

- o For **Name**, enter **pcf-http-lb**
- o For **Location**, select **Single-zone**.
- o For **Zone**, select the first zone from your region.
Example: For region **us-west1**, select zone **us-west1-a**.
- o Under **Group type**, select **Unmanaged instance group**.
- o For **Network**, select **pcf-virt-net**.
- o For **Subnetwork**, select the **pcf-pas-subnet-my-gcp-region** subnet that you created previously.
- o Click **Create**.

4. Create a second instance group with the following details:

- o **Name:** **pcf-http-lb**
- o **Location:** **Single-zone**
- o **Zone:** Select the second zone from your region.

Example: For region `us-west1`, select zone `us-west1-b`.

- **Group type:** Select **Unmanaged instance group**.
- **Network:** Select `pcf-virt-net`.
- **Subnetwork:** Select the `pcf-pas-subnet-my-gcp-region` subnet that you created previously.

5. Create a third instance group with the following details:

- **Name:** `pcf-http-lb`
- **Location:** **Single-zone**
- **Zone:** Select the third zone from your region.
Example: For region `us-west1`, select zone `us-west1-c`.
- **Group type:** Select **Unmanaged instance group**.
- **Network:** Select `pcf-virt-net`.
- **Subnetwork:** Select the `pcf-pas-subnet-my-gcp-region` subnet that you created previously.

Create Health Check

1. Navigate to **Compute Engine > Health checks**.

2. Click **CREATE HEALTH CHECK**.

3. Complete the form as follows:

- **Name:** `pcf-cf-public`
- **Port:** `8080`
- **Request path:** `/health`
- **Check interval:** `30`
- **Timeout:** `5`
- **Healthy threshold:** `10`
- **Unhealthy threshold:** `2`

4. Click **Create**.

Configure Back End

1. Navigate to **Network services > Load balancing**.

2. Click **CREATE LOAD BALANCER**.

3. Under **HTTP(S) Load Balancing**, click **Start configuration**.


4. For the **Name**, enter `pcf-global-pcf`.

5. Select **Backend configuration**

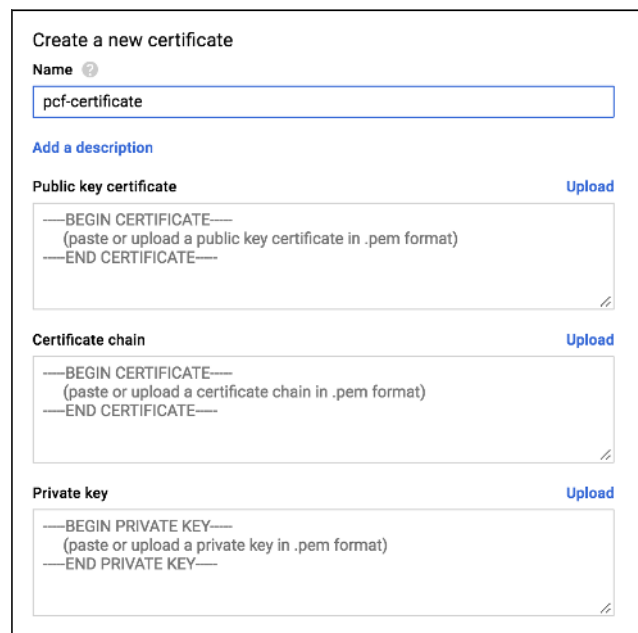
- a. From the dropdown, select **Backend services > Create a backend service**.
- b. Complete the form as follows:
 - c. **Name:** `pcf-http-lb-backend`.
 - d. **Protocol:** `HTTP`.
 - e. **Named port:** `http`.
 - f. **Timeout:** `10 seconds`.
- g. Under **Backends > New backend**, select the **Instance group** that corresponds to the first zone of the multi-zone instance group you created.
For example: `pcf-http-lb (us-west1-a)`. Click **Done**.
- h. Click **Add backend**, select the **Instance group** that corresponds to the second zone of the multi-zone instance group you created. For example:
`pcf-http-lb (us-west1-b)`. Click **Done**.
- i. Click **Add backend**, select the **Instance group** that corresponds to the third zone of the multi-zone instance group you created. For example:
`pcf-http-lb (us-west1-c)`. Click **Done**.
- j. **Health check:** Select the `pcf-cf-public` health check that you created.
- k. **Cloud CDN:** Ensure Cloud CDN is disabled.
- l. Click **Create**.

Configure Front End

1. Click **Host and path rules** to populate the default fields and a green check mark.
2. Select **Frontend configuration**, and add the following:
 - **Name:** `pcf-cf-lb-http`
 - **Protocol:** `HTTP`
 - **IP:** Perform the following steps:
 1. Select **Create IP address**.
 2. Enter a **Name** for the new static IP address and an optional description. For example, `pcf-global-pcf`.
 3. Click **Reserve**.
 - **Port:** `80`
3. If you use a trusted SSL certificate or already have a self-signed certificate, proceed to step 5.
4. If you want to use a self-signed certificate generated during [PAS network configuration](#), skip over the next step of adding the HTTPS frontend configuration until after you generate the certificate in PAS. After you generate the certificate, return to step 5 using the following guidelines:
 - Copy and paste the generated contents of the **Router SSL Termination Certificate and Private Key** fields from PAS into the public certificate and private key fields.
 - Since you are using a self-signed certificate, do not enter a value in the **Certificate Chain** field.
5. Click **Add Frontend IP and port** and add the following:

 **Note:** Skip this step if you do not have either a self-signed or trusted SSL certificate. When you configure the tile for your chosen runtime, you are given the opportunity to create a new self-signed certificate. Upon creating a certificate, you can complete the **Add Frontend IP and port** section.

- **Name:** `pcf-cf-lb-https`
- **Protocol:** `HTTPS`
- **IP address:** Select the `pcf-global-pcf` address you create for the previous **Frontend IP and Port**.
- **Port:** `443`
- Select **Create a new certificate**. The **Create a New Certificate** dialog is displayed.



- In the **Name** field, enter a name for the certificate.
- In the **Public key certificate** field, copy in the contents of your public certificate, or upload your certificate as a .pem file. If the certificate is runtime-generated, copy and paste the generated contents from the runtime's Certificate field into the Ops Manager **Public key certificate** field.
- In the **Certificate chain** field, enter or upload your certificate chain in the .pem format. If you are using a self-signed certificate, such as a PAS or PKS-generated certificate, do not enter a value in the **Certificate Chain** field.
- In the **Private key** field, copy in the contents or upload the .pem file of the private key for the certificate. If the certificate is runtime-generated, copy and paste the generated contents from the runtime's Private Key field into the Ops Manager **Private key** field.

6. Review the completed front end configuration.
7. Click **Review and finalize** to verify your configuration.

8. Click **Create**.

Step 9: Create TCP WebSockets Load Balancer

The load balancer for tailing logs with WebSockets for PCF on GCP operates on TCP port `443`.

1. From the GCP console, select **Network services > Load balancing > Create load balancer**
2. Under **TCP Load Balancing**, click **Start configuration**.

3. In the **Create a load balancer** configuration screen, make the following selections:
 - Under **Internet facing or internal only**, select **From Internet to my VMs**.
 - Under **Multiple regions or single region**, select **Single region only**.

- Under **Connection termination**, select **No (TCP)**.
4. Click **Continue**.
5. In the **New TCP load balancer** window, enter `pcf-wss-logs` in the **Name** field.
6. Click **Backend configuration** to configure the **Backend service**:

Backend configuration

Name ?

pcf-wss-logs

Region ?

us-central1

Backends ?

Select existing instance groups

Select existing instances

No instance groups in this region

Backup pool ? (Optional)

None

Failover ratio ?

10

%

Health check ?

pcf-gorouter (HTTP)

port: 8080, timeout: 5s, check interval: 5s, unhealthy threshold: 2 attempts

Session affinity ?

None

- Region: Select the region you used to create the network in [Create a GCP Network with Subnets](#).
- From the **Health check** dropdown, create a health check with the following details:
 - Name: `pcf-gorouter`
 - Port: `8080`
 - Request path: `/health`
 - Check interval: `30`
 - Timeout: `5`
 - Healthy threshold: `10`
 - Unhealthy threshold: `2` The **Backend configuration** section shows a green check mark.

7. Click **Frontend configuration** to open its configuration window and complete the fields:

- Protocol: `TCP`
- IP: Perform the following steps:
 - Select **Create IP address**.
 - For name **Name** for the new static IP address and an optional description. For example, `pcf-gorouter-wss`.
 - Click **Reserve**.

- Port: 443

Review and finalize

Backend

Name: **pcf-wss-logs** Region: **us-central1** Session affinity: **None** Health check: **pcf-gorouter**

Frontend

| Protocol ^ | IP:Port |
|------------|---------|
| TCP | :443 |

8. Click **Review and finalize** to verify your configuration.

9. Click **Create**.

Step 10: Create SSH Proxy Load Balancer

- From the GCP console, select **Network services > Load balancing > Create load balancer**
- Under **TCP Load Balancing**, click **Start configuration**.
- Under **Internet facing or internal only**, select **From Internet to my VMs**.

Create a load balancer

Please answer a few questions to help us select the right load balancing type for your application

Internet facing or internal only

Do you want to load balance traffic from the Internet to your VMs or only between VMs in your network?

☒ From Internet to my VMs
☐ Only between my VMs

Multiple regions or single region

Do you want to place the backends for your load balancer in a single region or across multiple regions?

☐ Multiple regions (or not sure yet)
☒ Single region only

Connection termination

Do you want to offload TCP or SSL processing to the Load Balancer?

☐ Yes (TCP Proxy or SSL Proxy - recommended)
☒ No (TCP)

Continue

4. Under **Connection termination**, select **No (TCP)**.

5. Click **Continue**.

6. In the **New TCP load balancer** window, enter **pcf-ssh-proxy** in the **Name** field.

7. Select **Backend configuration**, and enter the following field values:

- Region:** Select the region you used to create the network in [Create a GCP Network with Subnet](#).
- Backup pool:** None
- Failover ratio:** 10%
- Health check:** No health check

Backend configuration

Name ?

pcf-ssh-proxy

Region ?

us-central1

Backends ?

Select existing instance groups

Select existing instances

No instance groups in this region

Backup pool ? (Optional)

None

Failover ratio ?

10

%

Health check ?

No health check

Session affinity ?

None

8. Select **Frontend configuration**, and add the following:

- Protocol: `TCP`
- IP: Perform the following steps:
 1. Select **Create IP address**.
 2. Enter a **Name** for the new static IP address and an optional description. For example, `pcf-ssh-proxy`.
 3. Click **Reserve**.
- Port: `2222`

9. (Optional) Review and finalize your load balancer.

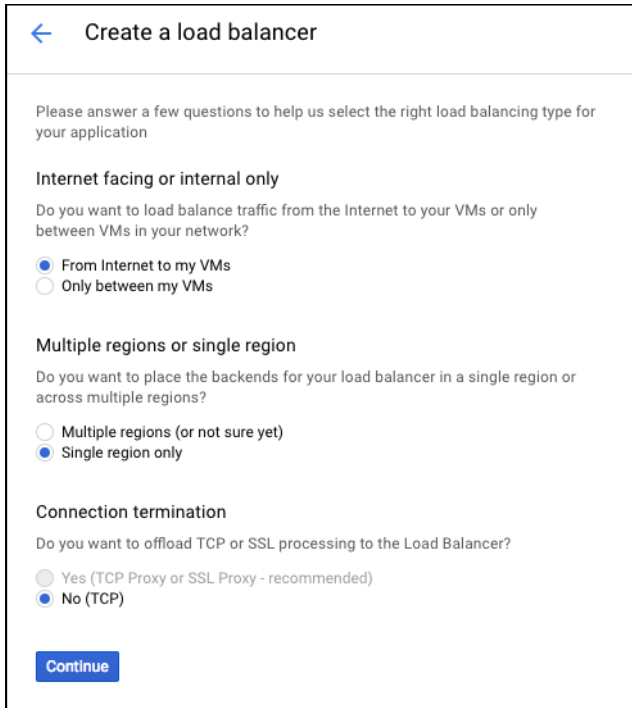
10. Click **Create**.

Step 11: Create Load Balancer for TCP Router

 **Note:** This step is optional and only required if you enable TCP routing in your deployment.

To create a load balancer for TCP routing in GCP, do the following:

1. From the GCP console, select **Network services > Load balancing > Create load balancer**
2. Under **TCP Load Balancing**, click **Start configuration**.
3. Under **Connection termination**, select **No (TCP)**. Click **Continue**.



Create a load balancer

Please answer a few questions to help us select the right load balancing type for your application

Internet facing or internal only
Do you want to load balance traffic from the Internet to your VMs or only between VMs in your network?

☒ From Internet to my VMs
☐ Only between my VMs

Multiple regions or single region
Do you want to place the backends for your load balancer in a single region or across multiple regions?

☐ Multiple regions (or not sure yet)
☒ Single region only

Connection termination
Do you want to offload TCP or SSL processing to the Load Balancer?

☐ Yes (TCP Proxy or SSL Proxy - recommended)
☒ No (TCP)

Continue

4. On the **New TCP load balancer** screen, enter a unique name for the load balancer in the **Name** field. For example, `pcf-cf-tcp-lb`.
5. Select **Backend configuration**, and enter the following field values:
 - **Region:** Select the region you used to create the network in [Create a GCP Network with Subnet](#).
 - From the **Health check** dropdown, create a health check with the following details:
 - **Name:** `pcf-tcp-lb`
 - **Port:** `80`
 - **Request path:** `/health`
 - **Check interval:** `30`
 - **Timeout:** `5`
 - **Healthy threshold:** `10`
 - **Unhealthy threshold:** `2`
 - Click **Save and continue**.

Backend configuration

Name ?

Region ?

us-central1

Backends ?

Select existing instance groups

Select existing instances

No instance groups in this region

Backup pool ? (Optional)

None

Failover ratio ?

10

%

Health check ?

pcf-tcp-lb (HTTP)

port: 80, timeout: 5s, check interval: 30s, unhealthy threshold: 2 attempts

Session affinity ?

None

6. Select **Frontend configuration**, and add the front end IP and port entry as follows:

- **Protocol:**
- **IP:** Perform the following steps:
 1. Select **Create IP address**.
 2. Enter a **Name** for the new static IP address and an optional description. For example, .
 3. Click **Reserve**.
- **Port:**

← New TCP load balancer

Name ?

pcf-cf-tcp-lb

✓ Backend configuration

Your backend is configured

✓ Frontend configuration

Your frontend is configured →

ⓘ Review and finalize

Optional

Create

Cancel

Frontend configuration

Specify an IP address, port and protocol. This IP address is the frontend IP for your clients requests.

Protocol:TCP, IP:35, Port:1024-65535

Not saved

+ Add Frontend IP and port

7. Click **Review and finalize** to verify your configuration.

8. Click **Create**.

Step 12: Add DNS Records for Your Load Balancers

In this step you redirect queries for your domain to the IP addresses of your load balancers.

1. Locate the static IP addresses of the load balancers you created in [Step 8: Create HTTP Load Balancer](#):

- An HTTP(S) load balancer named `pcf-global-pcf`
- A TCP load balancer for WebSockets named `pcf-wss-logs`
- A TCP load balancer named `pcf-ssh-proxy`
- A TCP load balancer named `pcf-cf-tcp-lb`

Note: You can locate the static IP address of each load balancer by clicking its name under **Network services > Load balancing** in the GCP console.

2. Log in to the DNS registrar that hosts your domain. Examples of DNS registrars include Network Solutions, GoDaddy, and Register.com.

3. Create **A records** with your DNS registrar that map domain names to the public static IP addresses of the load balancers located above:

| Create and map this record... | To the IP of this load balancer | Required |
|---|---------------------------------|---|
| <code>*.sys.MY-DOMAIN</code> Example: <code>*.sys.example.com</code> | <code>pcf-global-pcf</code> | Yes |
| <code>*.apps.MY-DOMAIN</code> Example: <code>*.apps.example.com</code> | <code>pcf-global-pcf</code> | Yes |
| <code>doppler.sys.MY-DOMAIN</code> Example: <code>doppler.sys.example.com</code> | <code>pcf-wss-logs</code> | Yes |
| <code>loggregator.sys.MY-DOMAIN</code> Example: <code>loggregator.sys.example.com</code> | <code>pcf-wss-logs</code> | Yes |
| <code>ssh.sys.MY-DOMAIN</code> Example: <code>ssh.sys.example.com</code> | <code>pcf-ssh-proxy</code> | Yes, to allow SSH access to apps |
| <code>tcp.MY-DOMAIN</code> Example: <code>tcp.example.com</code> | <code>pcf-cf-tcp-lb</code> | No, only set up if you have enabled the TCP routing feature |

4. Save changes within the web interface of your DNS registrar.

5. In a terminal window, run the following `dig` command to confirm that you created your A record successfully:

```
dig SUBDOMAIN.EXAMPLE-URL.com
```

Where `SUBDOMAIN.EXAMPLE-URL` is the subdomain for your load balancer.

You should see the A record that you just created:

```
;; ANSWER SECTION:
xyz.EXAMPLE.COM. 1767 IN A 203.0.113.1
```

Next Steps

- (Optional) To prepare for deploying either a PAS or PKS tile on GCP, you can download the needed runtime tile in advance:
 - To download PAS, log in to [Pivotal Network](#), select your desired release version, and download **Pivotal Application Service**.
 - To download PKS, log in to [Pivotal Network](#), select your desired release version, and download **Pivotal Container Service**.
- After initiating the tile download, proceed to the next step, [Deploying Ops Manager on GCP Manually](#).

Deploying Ops Manager on GCP Manually

Page last updated:

This topic describes how to deploy Ops Manager for Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP).

Before you deploy Ops Manager, see the preparation steps in [Preparing to Deploy Ops Manager on GCP Manually](#).

After you complete this procedure, follow the instructions in [Configuring BOSH Director on GCP Manually](#).

Step 1: Locate the Ops Manager Installation File

1. Log in to the [Pivotal Network](#), and click **Pivotal Cloud Foundry Operations Manager**.
2. From the **Releases** dropdown, select the release to install.
3. Select one of the following download files:
 - **Pivotal Cloud Foundry Ops Manager for GCP**
 - **Pivotal Cloud Foundry Ops Manager YAML for GCP**

When you click the download link, your browser downloads or opens the `OpsManager_VERSION_onGCP.pdf` or `OpsManager_VERSION_onGCP.yml` file.

These documents provide the GCP location of the Ops Manager `.tar.gz` installation file based on the geographic location of your installation.

4. Copy the filepath string of the Ops Manager image based on your deployment location.

Step 2: Create a Private VM Image

1. Log in to the [GCP console](#).
2. In the left navigation panel, click **Compute Engine**, and select **Images**.
3. Click **Create Image**.
4. Complete the following fields:
 - **Name:** Enter a name. For example, `om-pcf`.
 - **Encryption:** Leave **Automatic (recommended)** selected.
 - **Source:** Choose **Cloud Storage file**.
 - **Cloud Storage file:** Paste in the Google Cloud Storage filepath you copied from the PDF file in the [previous step](#).

Create an image

Name ?
om-pcf

Family (Optional) ?

Description (Optional)

Encryption ?
Automatic (recommended)

Source ?
Cloud Storage file

Cloud Storage file ?
☒ r-images/pivotal-ops-manager-20160916101000-01001000.tar.gz

Equivalent [REST](#) or [command line](#)

- Click **Create**. The file might take a few minutes to import.

Step 3: Create the Ops Manager VM Instance

- Select the checkbox for the image that you created above.

| Images [+] CREATE IMAGE ↻ REFRESH + CREATE INSTANCE ⌵ DEPRECATE 🗑 DELETE | | | | | |
|---|-------|------------|--------|---------------------------|--|
| Filter by label or name Columns ▾ Labels | | | | | |
| <input type="checkbox"/> Name | Size | Created by | Family | Creation time | |
| <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> om-pcf | 50 GB | CF-Docs | | Nov 22, 2016, 10:07:54 AM | |

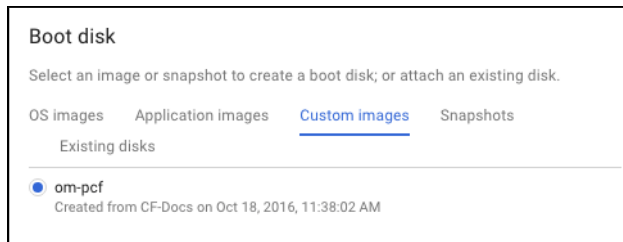
- Click **Create Instance**.
- In the **Create an instance form**, complete the following fields:
 - Name**: Enter a name that matches the naming conventions of your deployment.
 - Zone**: Choose a zone from the region in which you created your network.
 - Machine type**: Choose `n1-standard-2`.
 - Click **Customize** to manually configure the vCPU and memory. An Ops Manager VM instance requires the following minimum specifications:

| Machine Spec | Minimum Value |
|--------------|---------------|
| CPU | 2 vCPUs |
| Memory | 8 GB |

- Boot disk**: Click **Change**, then perform the following steps:
 - Click **Custom images** if it is not already selected.
 - Select the **Boot disk type**. If your environment has high performance needs, select **SSD**. As an example, environments used to [develop PCF tiles](#) might benefit from a higher performing Ops Manager VM boot disk. For most environments, you can select **Standard**.
 - Set the **Size (GB)** of the boot disk to the minimum or higher.

| Machine Spec | Minimum Value |
|--------------|---------------|
| Boot disk | 100 GB |

- Select the Ops Manager image you created in the previous step if it is not already selected.




- Click **Select** to save.

- Under **Identity and API access**, choose the **Service account** you created when preparing your environment during the step [Set up an IAM Service Account](#).
- **Allow HTTP traffic**: Leave this checkbox unselected.
- **Allow HTTPS traffic**: Leave this checkbox unselected.
- **Networking**: Select the **Networking** tab, and perform the following steps:
 - Under **Network interfaces**, perform the following steps:
 - Remove the `default` network interface if this interface still exists.
 - Select the network you created when preparing your environment in the [Create a GCP Network with Subnet](#) section of the *Preparing to Deploy Ops Manager on GCP Manually* topic. For example, `pcf-virt-net`.
 - Under **Subnetwork**, select the `pcf-infrastructure-subnet-GCP-REGION` subnet that you created when preparing your environment in the [Create a GCP Network with Subnet](#) section of the *Preparing to Deploy Ops Manager on GCP Manually* topic.
 - For **Primary internal IP**, select **Ephemeral (Custom)**. Enter an IP address (for example, `192.168.101.5`) in the **Custom ephemeral IP address** field. Specify the next available internal IP address located within the reserved IP range that you [configure later in BOSH Director](#). Do not use the **Gateway IP**, for example `192.168.101.1`.
 - For **External IP**, select **Create IP address**. In the next form, enter a name for the static IP. For example, `om-public-ip`. Click **Reserve**. In the **External IP** dropdown, select the static IP address you just reserved.
 - For **Network tags**, enter `pcf-opsman` and `allow-https`. These tags apply the firewall rules you created in [Create Firewall Rules for the Network](#) to the Ops Manager VM.

4. Click **Create** to deploy the new Ops Manager VM. This might take a few moments.

5. Navigate to your DNS provider, and create an entry that points a fully qualified domain name (FQDN) `opsman.MY-DOMAIN` to the `pcf-opsman` static IP address of Ops Manager that you created in a previous step.

 **Note:** In order to set up Ops Manager authentication correctly, Pivotal recommends using an FQDN to access Ops Manager. Using an ephemeral IP address to access Ops Manager can cause authentication errors upon subsequent access.

Next Steps


After you complete this procedure, follow the instructions in the [Configuring BOSH Director on GCP Manually](#) topic.

Later on, if you need to SSH into the Ops Manager VM to perform diagnostic troubleshooting, see [SSH into Ops Manager](#).

Configuring BOSH Director on GCP Manually


Page last updated:

This topic describes how to configure the BOSH Director in Ops Manager for Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP).

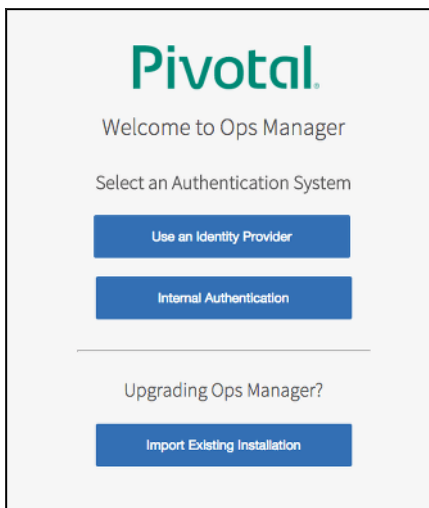
 **Note:** You can also perform the procedures in this topic using the Ops Manager API. For more information, see the [Using the Ops Manager API](#) topic.

Step 1: Access Ops Manager

1. In a web browser, navigate to the fully qualified domain name (FQDN) of Ops Manager that you set up in [Deploying Ops Manager on GCP Manually](#).

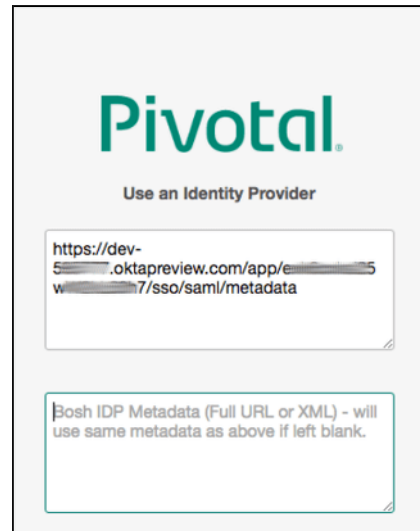
 **Note:** In order to set up Ops Manager authentication correctly, Pivotal recommends using a Fully Qualified Domain Name (FQDN) to access Ops Manager. Using an ephemeral IP address to access Ops Manager can cause authentication errors upon subsequent access.

2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you use an Identity Provider, an external identity server maintains your user database.
 - [Internal Authentication](#): If you use Internal Authentication, Ops Manager maintains your user database.



Use an Identity Provider (IdP)

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.



2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.

Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a `500` error.

Note: These attributes are case-sensitive.

- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.

5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.

6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

Note: To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.

- **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
- **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
- **Name ID:** Email Address
- SAML authentication requests are always signed

8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.

- **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
- **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
- **Name ID:** Email Address
- SAML authentication requests are always signed

9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

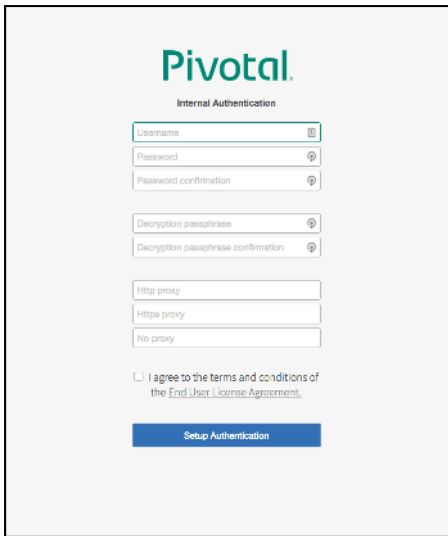
Internal Authentication

1. When redirected to the **Internal Authentication** page, do the following:

- Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
- Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not

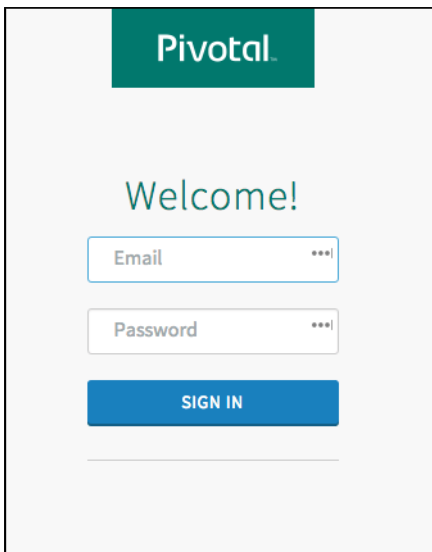
recoverable if lost.

- If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in the [Configuring Proxy Settings for the BOSH CPI](#) topic.
- Read the **End User License Agreement**, and select the checkbox to accept the terms.
- Click **Setup Authentication**.



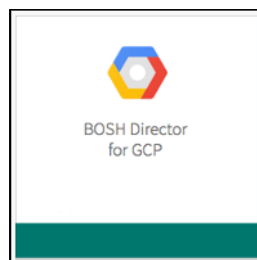
The image shows the 'Pivotal Internal Authentication' setup form. It includes fields for Username, Password, Password confirmation, Decryption passphrase, and Decryption passphrase confirmation. There are also fields for Http proxy, Https proxy, and No proxy. A checkbox for 'I agree to the terms and conditions of the End User License Agreement' is present, followed by a 'Setup Authentication' button.

2. Log in to Ops Manager with the Admin username and password that you created in the previous step.



The image shows the 'Pivotal Welcome!' login form. It features a 'Pivotal' logo at the top, followed by 'Welcome!' text. Below this are input fields for 'Email' and 'Password', both with masked characters (***). A blue 'SIGN IN' button is at the bottom.

Step 2: Google Cloud Platform Config



1. Click the **Google Cloud Platform** tile within the **Installation Dashboard**.
2. Select **Google Config**. Complete the following fields:
 - **Project ID**: Enter your GCP project ID in lowercase, such as: `your-gcp-project-id`.
 - **Default Deployment Tag**: Enter the prefix that you used when creating the GCP resources for this PCF installation. For example, `pcf`.
 - Select **AuthJSON** and in the field below enter the contents of the JSON file that you downloaded in the [Set up an IAM Service Account](#) section

of the *Preparing to Deploy Ops Manager on GCP Manually* topic.

Note: As an alternative, you can select **The Ops Manager VM Service Account** option to use the service account automatically created by GCP for the Ops Manager VM. To use this option, the project-wide service account that you set up in [Set up an IAM Service Account](#) must be assigned the **Service Account Actor** role.

3. Click **Save**.


Step 3: Director Config Page

1. Select **Director Config** to open the **Director Config** page.


2. In the **NTP Servers (comma delimited)** field, enter `169.254.169.254` to designate the `metadata.google.internal` host as NTP server.

Note: The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify the value of this field.


3. Leave the **JMX Provider IP Address** field blank.

 **Note:** Starting from PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use PCF JMX Bridge for consuming them outside of the Firehose, you might receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

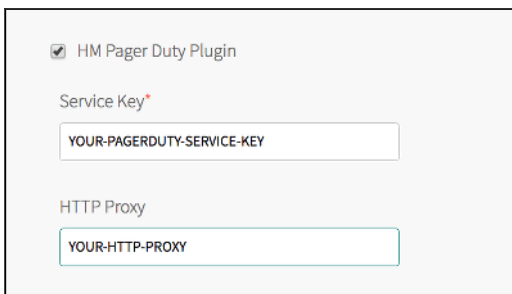
4. Leave the **Bosh HM Forwarder IP Address** field blank.

 **Note:** Starting from PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use the BOSH HM Forwarder for consuming them, you might receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

5. Select the **Enable VM Resurrector Plugin** checkbox to enable the Ops Manager Resurrector functionality and increase Pivotal Application Service (PAS) availability.
6. Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.

 **Note:** You must enable post-deploy scripts to install PKS.

7. (Optional) Select **Recreate all VMs** to force BOSH to re-create all VMs on the next deploy. This process does not destroy any persistent disk data.
8. Select **Enable bosh deploy retries** for Ops Manager to retry failed BOSH operations up to five times.
9. (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS secure communications.
10. (Optional) Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.
11. (Optional) Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.



- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.

☒ **HM Email Plugin**

Host*

Port*

Domain*

From*

Recipients*

Username

Password

☒ **Enable TLS**

12. (Optional) Select **HM Email Plugin** to enable Health Monitor integration with email.

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma-separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter the password for your email server.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

13. For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

Note: After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*


HSM Port Address*

Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**
 9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal

☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature

☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- o **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- o **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. Follow the procedures in [Sign up for Amazon S3](#) and [Creating a Bucket](#) in the AWS documentation. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.

- **GCS Blobstore:** Select this option to use an external Google Cloud Storage (GCS) endpoint. To create a GCS bucket, follow the procedures in [Creating Storage Buckets](#) in the GCS documentation. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Enter the contents of the JSON file that you downloaded in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually*.


15. For **Database Location**, if you configured an external MySQL database such as Cloud SQL, select **External MySQL Database** and complete the fields below. Otherwise, select **Internal**. For more information about creating a Cloud SQL instance, see [Quickstart for Cloud SQL for MySQL](#) in the Google Cloud documentation.

- **Host:** Enter the value of your host.
- **Port:** Enter your port number. For example, .
- **Username:** Enter your username.
- **Password:** Enter your password.
- **Database:** Enter your database name.

In addition, if you selected the **Enable TLS for Director Database** checkbox, you can fill out the following optional fields:

- **Enable TLS:** Selecting this checkbox enables TLS communication between the BOSH Director and the database.
- **TLS CA:** Enter the Certificate Authority for the TLS Certificate.
- **TLS Certificate:** Enter the client certificate for mutual TLS connections to the database.
- **TLS Private Key:** Enter the client private key for mutual TLS connections to the database.
- **Advanced DB Connection Options:** If you would like to provide additional options for the database, use this field to provide a JSON-formatted options string.

16. (Optional) Modify the **Director Workers** value, which sets the number of workers available to execute Director tasks. This field defaults to .
17. (Optional) **Max Threads** sets the maximum number of threads that the BOSH Director can run simultaneously. Pivotal recommends that you leave the field blank to use the default value, unless doing so results in rate limiting or errors on your IaaS.
18. (Optional) To add a custom URL for your BOSH Director, enter a valid hostname in **Director Hostname**. You can also use this field to configure [a load balancer in front of your BOSH Director](#).

 **warning:** In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, VMs become unavailable. This causes downtime for your environment. To restore VM availability, enable **Recreate All VMs** and redeploy. This issue is resolved in [Ops Manager v2.2.8](#) and later.


Director Workers


Max Threads

Director Hostname

19. (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.
20. (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.

 **Note:** Disabling BOSH DNS affects [Step 5: Create Networks Page](#) below when you configure your network DNS.

 **Breaking Change:** Do not disable BOSH DNS without consulting Pivotal Support.

 **Note:** If you are deploying PKS, do not disable BOSH DNS. If PAS and PKS are running on the same instance of Ops Manager, you cannot use the opt-out feature of BOSH DNS for your PAS without breaking PKS. If you want to opt out of BOSH DNS in your PAS deployment, install the tile on a separate instance of Ops Manager.


21. (Optional) To set a custom banner that users see when logging in to the Director using SSH, enter text in the **Custom SSH Banner** field.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

22. (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1, hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.
23. Click **Save**.

Step 4: Create Availability Zones Page

 **Note:** Pivotal recommends at least three availability zones for a highly available installation.

- For configuring a PAS deployment with multiple availability zones, see [Reference Architecture for Pivotal Cloud Foundry on GCP](#).
- For PKS best practices for distributing workloads across multiple availability zones and clusters, see [Maintaining Workload Uptime](#).

1. Select **Create Availability Zones**.

1. Click **Add**.

2. For **Google Availability Zone**:

- Enter one of the zones that you associated to the backend service instance groups of the HTTP(S) Load Balancer. For example, if you are using

the `us-central1` region and selected `us-central1-a` as one of the zones for your HTTP(S) Load Balancer instance groups, enter `us-central1-a`.

- Click **Add**.
- Repeat the above step for all the availability zones that you associated to instance groups in [Preparing to Deploy Ops Manager on GCP Manually](#).

- Click **Save**.

3. Repeat the above step for all the availability zones you are using in your deployment. When you are done, click **Save**.

Step 5: Create Networks Page

- Select **Create Networks**.
- Make sure **Enable ICMP checks** is not selected. GCP routers do not respond to ICMP pings.
- Click **Add Network**. Create the three networks described in the tables below.

Note: To use a shared VPC network, enter the shared VPC host project name before the network name in the format `VPC-PROJECT-NAME/NETWORK-NAME/SUBNET-NAME/REGION-NAME`. For example, `vpc-project/opsmgr/central/us-central1`. For more information, see [Configuring a Shared VPC on GCP](#).

If you disabled BOSH DNS for a PAS installation, enter `8.8.8.8` into the ****DNS Servers**** field of the PAS tile. For more information, see step 29g in the *Configure Networking* section of the [Deploying PAS on GCP](#) topic.

Infrastructure Network


| | |
|---------------------|---|
| Network Name | <code>infrastructure</code> |
| Google Network Name | Enter the name of the infrastructure network that you created in the Create a GCP Network with Subnets step of <i>Preparing to Deploy Ops Manager on GCP Manually</i> . The format is: <code>pcf-virt-net/pcf-infrastructure-subnet-MY-REGION/MY-GCP-REGION</code> |
| CIDR | Enter the name of the CIDR ending in <code>/26</code> that you used when you created the infrastructure subnet in GCP. Example: <code>192.168.101.0/26</code> |
| Reserved IP Ranges | Enter the first <code>.1</code> through <code>.9</code> addresses from the CIDR. For example, if the CIDR is <code>192.168.101.0/26</code> , enter the range <code>192.168.101.1-192.168.101.9</code> . |
| DNS | <code>169.254.169.254</code> |
| Gateway | Enter the first <code>.1</code> address from the CIDR. For example, if the CIDR is <code>192.168.101.0/26</code> , enter <code>192.168.101.1</code> . |
| Availability Zones | Select all three availability zones. |


Runtime Network

| | |
|---------------------|--|
| Name | Enter the name of the runtime that you intend to deploy in this environment. For example, <code>pas</code> or <code>pks</code> . |
| Google Network Name | Enter the name of the runtime network that you created when you prepared your GCP environment. The format is: <code>pcf-virt-net/pcf-RUNTIME-subnet-MY-REGION/MY-GCP-REGION</code> |
| CIDR | Enter the name of the CIDR ending in <code>/22</code> that you used when you created the runtime subnet in GCP. Example: <code>192.168.16.0/22</code> |
| Reserved IP Ranges | Enter the first <code>.1</code> through <code>.9</code> addresses from the CIDR. For example, if the CIDR is <code>192.168.16.0/22</code> , enter the range <code>192.168.16.1-192.168.16.9</code> . |
| DNS | <code>169.254.169.254</code> |
| Gateway | Enter the first <code>.1</code> address from the CIDR. For example, if the CIDR is <code>192.168.16.0/22</code> , enter <code>192.168.16.1</code> . |
| Availability Zones | Select all three availability zones. |

Services Network

| | |
|---------------------|--|
| Network Name | <code>services</code> |
| Google Network Name | Enter the name of the services network that you created when you prepared your GCP environment. The format is: <code>pcf-virt-net/pcf-services-subnet-MY-REGION/MY-GCP-REGION</code> |
| CIDR | Enter the name of the CIDR ending in <code>/22</code> that you used when you created the services subnet in GCP. Example: <code>192.168.20.0/22</code> |
| Reserved IP Ranges | Enter the first <code>.1</code> through <code>.9</code> addresses from the CIDR. For example, if the CIDR is <code>192.168.20.0/22</code> , enter the range <code>192.168.20.1-192.168.20.9</code> . |
| DNS | <code>169.254.169.254</code> |
| Gateway | Enter the first <code>.1</code> address from the CIDR. For example, if the CIDR is <code>192.168.16.0/22</code> , enter <code>192.168.16.1</code> . |
| Availability Zones | Select all three availability zones. |

 **Note:** After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

 **Note:** Ensure `169.254.169.254`, the IP address of the `metadata.google.internal` metadata server, is always specified at the beginning of this step's DNS resolver lists.

Step 6: Assign AZs and Networks Page

1. Select **Assign AZs and Networks**.
2. Use the dropdown to select a **Singleton Availability Zone**. The BOSH Director installs in this Availability Zone.
3. Under **Network**, select the `infrastructure` network for your BOSH Director.
4. Click **Save**.

Step 7: Security Page

Security

Trusted Certificates

-----BEGIN CERTIFICATE-----
THXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

These certificates enable BOSH-deployed components to trust a custom root certificate.

Generate VM passwords or use single password for all VMs

☒ Generate passwords

☐ Use default BOSH password

Save

1. Select **Security**.
2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:

```

-----BEGIN CERTIFICATE-----
ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678AB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BCDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CDEFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABBB
EFGH12345678ABCEDEFGH12345678ABCEDEFGH12345678ABCEDEF
GH12345678ABCEDEFGH12345678ABCEDEFGH12345678...
-----END CERTIFICATE-----

```

 Note: If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#) for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 8: Syslog Page

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
 ☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

⌵

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save

- (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
- In the **Address** field, enter the IP address or DNS name for the remote server.
- In the **Port** field, enter the port number that the remote server listens on.
- In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
- (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
 - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
- Click **Save**.

Step 9: Resource Config Page

- Select **Resource Config**.
- Ensure that the **Internet Connected** checkboxes are not selected for any jobs. The checkbox gives VMs a public IP address that enables outbound

internet access. In [Preparing to Deploy Ops Manager on GCP Manually](#), you provisioned a Network Address Translation (NAT) box to provide internet connectivity to your VMs. For more information about using NAT in GCP, see the [GCP documentation](#).

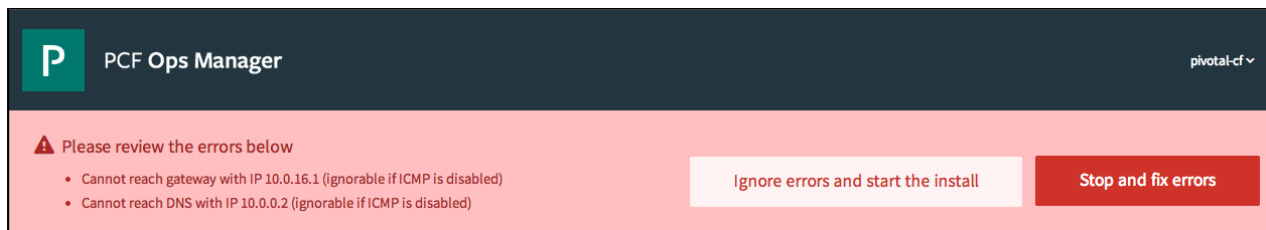
Note: If you install PAS for Windows, provision your **Master Compilation Job** with at least 100 GB of disk space.

Step 10: (Optional) Add Custom VM Extensions

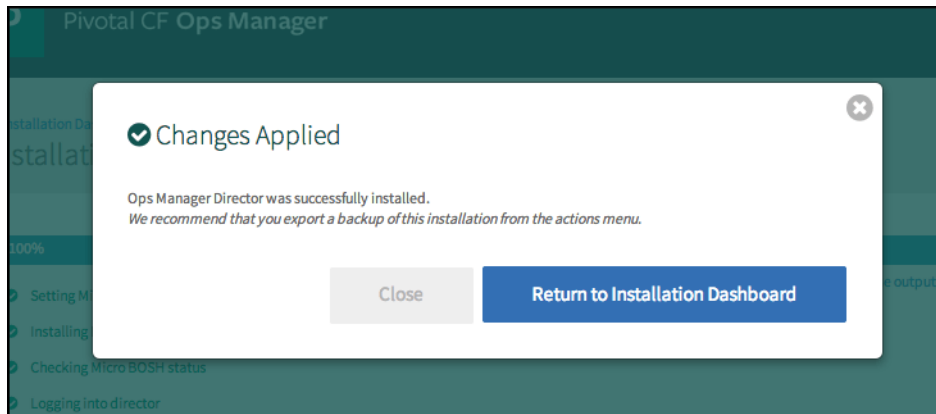
Use the Ops Manager API to add custom properties to your VMs such as associated security groups and load balancers. For more information, see [Managing Custom VM Extensions](#).

Step 11: Complete the BOSH Director Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**. If the following ICMP error message appears, return to the [Network Config](#) screen, and ensure you have deselected the **Enable ICMP Checks** box. Then click **Apply Changes** again.



3. BOSH Director installs. This might take a few moments. When the installation process successfully completes, the **Changes Applied** window appears.



Next Steps

After you complete this procedure, follow the instructions for the runtime you intend to install.

- To deploy PAS, see [Deploying PAS on GCP](#).
- To prepare to deploy PKS, see [Installing PKS on GCP](#).

Deploying PAS on GCP

Page last updated:

This topic describes how to install and configure Pivotal Application Service (PAS) on Google Cloud Platform (GCP).

Before beginning this procedure, ensure that you have successfully completed the [Configuring BOSH Director on GCP](#) topic.

Note: If you plan to [install the PCF IPsec add-on](#), you must do so before installing any other tiles. Pivotal recommends installing IPsec immediately after Ops Manager, and before installing the PAS tile.

Step 1: Download the PAS Tile

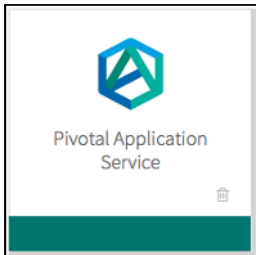
1. If you have not already downloaded PAS, log in to [Pivotal Network](#), and click PAS.
2. From the **Releases** drop-down, select the release to install and choose one of the following:
 - a. Click PAS to download the PAS `.pivotal` file.
 - b. Click **PCF Small Footprint Runtime** to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).

Step 2: Add PAS to Ops Manager

1. Navigate to the Pivotal Cloud Foundry Operations Manager Installation Dashboard.
2. Click **Import a Product** to add the PAS tile to Ops Manager. This may take a while depending on your connection speed.

Tip: After you import a tile to Ops Manager, you can view the latest available version of that tile in the Installation Dashboard by enabling the Pivotal Network API. For more information, refer to the [Adding and Deleting Products](#) topic.

3. On the left, click the plus icon next to the imported PAS product to add it to the Installation Dashboard.
4. Click the newly added PAS tile in the Installation Dashboard.



Step 3: Assign Availability Zones and Networks

1. Select **Assign AZ and Networks**. These are the Availability Zones that you created in [Step 4: Create Availability Zones Page](#) of the *Configuring BOSH Director on GCP* topic.
2. Select the first Availability Zone under **Place singleton jobs**. Ops Manager runs any job with a single instance in this Availability Zone.
3. Select all Availability Zones under **Balance other jobs**. Ops Manager balances instances of jobs with more than one instance across the Availability Zones that you specify.

Note: For production deployments, Pivotal recommends at least three Availability Zones for a highly available installation of PAS.


4. From the **Network** dropdown, choose the network you created in [Step 5: Create Networks Page](#) of the *Configuring BOSH Director on GCP Manually* topic.

- Click **Save**.

Step 4: Add DNS Records for Your Load Balancers

In this step, you redirect queries for your domain to the IP addresses of your load balancers.

- Locate the static IP addresses of the load balancers you created in [Preparing to Deploy Ops Manager on GCP Manually](#):
 - An HTTP(S) load balancer named `MY-PCF-global-pcf`
 - A TCP load balancer for WebSockets named `MY-PCF-wss-logs`
 - A TCP load balancer for SSH access to applications named `MY-PCF-ssh-proxy`
 - A TCP load balancer for the TCP router named `MY-PCF-cf-tcp-lb` if you plan on enabling the TCP routing feature

 **Note:** You can locate the static IP address of each load balancer by clicking its name under **Networks > Load balancing** in the GCP Console.

- Log in to the DNS registrar that hosts your domain. Examples of DNS registrars include Network Solutions, GoDaddy, and Register.com.
- Create **A records** with your DNS registrar that map domain names to the public static IP addresses of the load balancers located above:


| If your DNS entry is: | Set to the public IP of this load balancer: | Required | Example |
|------------------------------|---|---|--------------------------------|
| *.YOURSYSTEMDOMAIN | <code>MY-PCF-global-pcf</code> | Yes | *.system.example.com |
| *.YOURAPPSDOMAIN | <code>MY-PCF-global-pcf</code> | Yes | *.apps.example.com |
| doppler.YOURSYSTEMDOMAIN | <code>MY-PCF-wss-logs</code> | Yes | doppler.system.example.com |
| loggregator.YOURSYSTEMDOMAIN | <code>MY-PCF-wss-logs</code> | Yes | loggregator.system.example.com |
| ssh.YOURSYSTEMDOMAIN | <code>MY-PCF-ssh-proxy</code> | Yes, to allow SSH access to apps | ssh.system.example.com |
| tcp.YOURDOMAIN | <code>MY-PCF-cf-tcp-lb</code> | No, only set up if you have enabled the TCP routing feature | tcp.example.com |

- Save changes within the web interface of your DNS registrar.
- In a terminal window, run the following `dig` command to confirm that you created your A record successfully:

```
dig xyz.EXAMPLE.COM
```

You should see the A record that you just created:

```
:: ANSWER SECTION:
xyz.EXAMPLE.COM. 1767 IN A 203.0.113.1
```

 **Note:** You **must** complete this step before proceeding to Cloud Controller configuration. A difficult-to-resolve problem can occur if the wildcard domain is improperly cached before the A record is registered.

Step 5: Configure Domains

- Select **Domains**.

Application Service hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain *

Apps Domain *

Save

2. Enter the system and application domains that you created in [Step 12: Add DNS Records for Your Load Balancers](#) of the *Preparing GCP* topic.
 - The **System Domain** defines your target when you push apps to PAS.
 - The **Apps Domain** defines where PAS serves your apps.

Note: Pivotal recommends that you use the same domain name but different subdomain names for your system and app domains. For example, use `system.example.com` for your system domain, and `apps.example.com` for your apps domain.

3. Click **Save**.

Step 6: Configure Networking

1. Select **Networking**.
2. Leave the **Router IPs**, **SSH Proxy IPs**, **HAProxy IPs**, and **TCP Router IPs** fields blank. You do not need to complete these fields when deploying PCF to GCP.

Note: You specify load balancers in the **Resource Config** section of PAS later on in the installation process. See the [Configure Load Balancers](#) section of this topic for more information.

3. Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate and Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.
 - a. Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

Certificates and Private Keys for HAProxy and Router

Add

▼ example-cert

Name *

example-cert

A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

Generate RSA Certificate

▼ example-cert-2

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed

certificate in Ops Manager.

- b. If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see *Configure Front End* in [Preparing to Deploy Ops Manager on GCP Manually](#).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

4. (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

5. In the **Minimum version of TLS supported by HAProxy and Router** field, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

☐ TLSv1.0
☐ TLSv1.1
☒ TLSv1.2

6. Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- o If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- o If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

☒ Log client IPs
☐ Disable logging of X-Forwarded-For header only
☐ Disable logging of both source IP and X-Forwarded-For header

To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.

7. Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.

Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

- ☒ TLS terminated for the first time at infrastructure load balancer
- ☐ TLS terminated for the first time at HAProxy
- ☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|--|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to the instances of HAProxy, and HAProxy instance count is > 0 | TLS terminated for the first time at HAProxy. | <p>HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header.</p> <p>Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option.</p> |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | TLS terminated for the first time at the Gorouter. | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p> <p>Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option.</p> |

For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).

- To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation *

- ☒ HAProxy does not request client certificates.
- ☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.

Warning: Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

- To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- o **Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- o **Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- o **Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

⚠ warning: Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client Certificate Validation** in the **Networking** pane.

10. In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

`ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384`

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.


💡 Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

11. In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:
`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384` If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384`

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

12. Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable

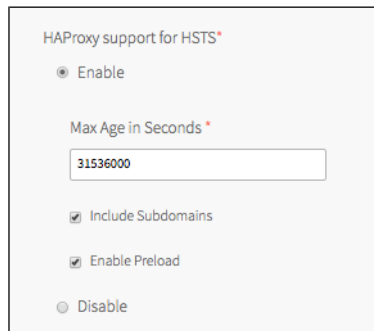
- **Enable HAProxy forwarding of requests to Router over TLS**

| | |
|--------------------------------------|---|
| If you want to: | Encrypt communication between HAProxy and the Gorouter |
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

- **Disable HAProxy forwarding of requests to Router over TLS**

| | |
|--------------------------------------|---|
| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |

13. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field and complete



HAProxy support for HSTS*

☒ Enable

Max Age in Seconds*

31536000

☒ Include Subdomains


☒ Enable Preload

☐ Disable

the following optional configuration steps:

- a. (Optional) **Enter a Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
- b. (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
- c. (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from HAProxy.

14. If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

15. (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

16. (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
17. (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
18. (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
19. By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#).

20. (Optional) By default, Gorouter support for the PROXY protocol is disabled. To enable the PROXY protocol, select **Enable support for PROXY protocol in CF Router**. When enabled, client-side load balancers that terminate TLS but do not support HTTP can pass along information from the originating client. Enabling this option may impact Gorouter performance. For more information about enabling the PROXY protocol in Gorouter, see the *HTTP Header Forwarding* sections in the [Securing Traffic in Cloud Foundry](#) topic.
21. In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details.
 - a. If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
22. (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

0

500

23. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router*

☒ Enable
 ☐ Disable

24. (Optional) To accommodate larger uploads over connections with high latency, increase the number of seconds in the **Router Timeout to Backends** field.
25. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

26. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
27. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

20

Load Balancer Healthy Threshold *

20

28. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

29. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

30. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.

HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.

HAProxy Trusted CIDRs

31. The **Loggregator Port** defaults to **443** if left blank. Enter a new value to override the default.

Container Network Interface Plugin*



32. For **Container Network Interface Plugin**, ensure **Silk** is selected and review the following fields:

Note: The **External** option exists to support NSX-T integration for vSphere deployments.

- (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to **1454**. Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses **10.255.0.0/16**.

warning: The overlay network IP range must not conflict with any other IP addresses in your network.

- Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to **1**.
- For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to **100**.
- To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- For **DNS Servers**, enter **8.8.8.8** only if you have BOSH disabled. Otherwise, you cannot use this field to override the DNS servers used in containers.

Note: If you do not want to configure your DNS servers with **8.8.8.8**, contact [Pivotal Support](#).

33. For **DNS Search Domains**, enter DNS search domains for your containers as a comma-separated list. DNS on your containers appends these names to its host names, to resolve them into full domain names.

DNS Search Domains

example.com, myapps.com

DNS search domains to be used in containers. A comma-separated list can be specified.

34. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is **120**. You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

35. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:

- a. Select **Enable TCP Routing**.
- b. For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. These are the same ports that you configured in the [Pre-Deployment Steps](#) of the *Enabling TCP Routing* topic.
 - To support multiple TCP routes, Pivotal recommends allocating multiple ports.
 - To allocate a list of ports rather than a range:
 1. Enter a single port in the **TCP Routing Ports** field.
 2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time
 ☒ Enable TCP Routing

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

- c. For GCP, you also need to specify the name of a GCP TCP load balancer in the **LOAD BALANCER** column of TCP Router job of the **Resource Config** screen. You configure this later on in PAS. See [Configure Load Balancers](#) section of this topic.

36. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) [↗](#) topic.

37. Click **Save**.

Step 7: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC

☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888


Docker Images Disk-Cleanup Scheduling on Cell VMs*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) *


10240


- The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.
- The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
- If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
- If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.

- To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting](#) in *HTTP Routing*.

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

 **Warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

7. You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
8. Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
9. Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
10. Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.



Note: In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

11. (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs*

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

12. By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.

13. Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
14. You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is seconds and the maximum configurable timeout is seconds.
15. Click **Save**.

Step 8: Configure Application Developer Controls

1. Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *

Staging Timeout (Seconds) *

☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.
4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.

5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.

Note: If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of seconds you specify in this field.
9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 9: Review Application Security Groups

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type ☐ in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 10: Configure UAA

1. Select **UAA**.
2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

3. Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN`.



Note: The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN`.

- If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
M
U
H
M
-----END CERTIFICATE-----

[Change](#)

SAML Service Provider Key Password

Secret

Password.

- (Optional) To override the default value, enter a custom SAML Entity ID in the **SAML Entity ID Override** field. By default, the SAML Entity ID is `http://login.YOUR-SYSTEM-DOMAIN` where `YOUR-SYSTEM-DOMAIN` is set in the **Domains > System Domain** field.
- For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
- (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line


The screenshot shows a configuration panel for the UAA (User Access and Authentication) service. It contains several input fields for setting various lifetimes and timeouts, each followed by a red asterisk indicating it is a required field. The fields and their values are:


- Apps Manager Access Token Lifetime (in seconds) *: 1209600
- Apps Manager Refresh Token Lifetime (in seconds) *: 1209600
- Cloud Foundry CLI Access Token Lifetime (in seconds) *: 7200
- Cloud Foundry CLI Refresh Token Lifetime (in seconds) *: 1209600
- Global Login Session Max Timeout (in seconds) *: 1800
- Global Login Session Idle Timeout (in seconds) *: 1800
- Customize Username Label (on login page) *: Email
- Customize Password Label (on login page) *: Password
- Proxy IPs Regular Expression *: 10\.\d{1,3}\.\d{1,3}\.\d{1,3}192\.168\.\d{1,3}

At the bottom of the panel is a blue "Save" button.

Interface (cf CLI) login access and refresh. Most deployments use the defaults.

8. (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:
 - **Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - **Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan
9. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
10. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Router or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
11. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** For GCP installations, Pivotal recommends selecting **External** and using Google Cloud SQL.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#) for help.

Internal Database Configuration

When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane, which can be one of two

options. See [Migrate to Internal Percona MySQL](#) for details.

1. Select **Internal MySQL**.

Choose the location of your UAA database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use AWS RDS)

2. Click **Save**.
3. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

1. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)

☒ External (preferred if, for example, you use AWS RDS)

Hostname *

TCP Port *


Username *

Password *

Secret

2. Enter the **Hostname** and **TCP Port** of the database from [Step 6: Create Database Instance and Databases](#) of the *Preparing to Deploy PCF on GCP* topic.
3. For **User Account and Authentication database username**, specify a unique username that can access this specific database on the database server.
4. For **User Account and Authentication database password**, specify a password for the provided username.
5. Click **Save**.

Step 11: Configure CredHub

 **Note:** Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

1. Select **CredHub**.
2. Select **Internal** for your CredHub database. For GCP environments, Runtime CredHub has the following limitations:
 - If you choose **External**, Runtime CredHub does not work. See [CredHub Database Cannot be External on GCP](#).
 - Runtime CredHub only works if both the [system databases](#) and the CredHub database are set to **Internal**.

- Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys

Name *

Name of the encryption key.

Provider*


Internal

Key *

Secret

☐ Primary

- Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.

 **Note:** For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

- (Optional) To configure CredHub to use an HSM, complete the following fields:

- HSM Provider Partition.** This is the name of the HSM provider partition.
- HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#) in the

HSM Provider Partition

HSM Provider Partition Password

Secret

HSM Provider Client Certificate

Certificate PEM

Private Key PEM

[Generate RSA Certificate](#)

Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

5. If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.
6. Click **Save**.
7. Select the **Resource Config** pane.
8. Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.
9. Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).

Step 12: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *


2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.


3. Click **Save**.


Step 13: Configure System Databases

You can configure PAS to use Google Cloud SQL for the databases required by PAS.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. Contact Pivotal Support for help. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration

 **Note:** For GCP installations, Pivotal recommends selecting **External** and using Google Cloud SQL. Only use internal MySQL for non-production or test installations on GCP.

 **Note:** For Runtime CredHub to work, you must use internal MySQL. See [CredHub Database Cannot be External on GCP](#).

If you want to use internal databases for your deployment, perform the following steps:

1. Select **Databases**.
2. Select one of the **Internal Databases** options:
 - **Internal Databases - MySQL - Percona XtraDB Cluster** uses [Percona Server](#) with TLS encryption between server cluster nodes.
 - **Internal Databases - MySQL - MariaDB Galera Cluster** uses [MariaDB](#) with cluster nodes communicating over plaintext.

⚠ warning: Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

3. Click **Save**.

Then proceed to [Step 14: \(Optional\) Configure Internal MySQL](#) to configure high availability for your internal MySQL databases.

External Database Configuration

Pivotal recommends using an external database such as Google Cloud SQL for high availability reasons.

On GCP, you can use Google Cloud SQL and use the automated backup and high availability replica features.

💡 Note: If you use external MySQL, you cannot use Runtime CredHub. See [CredHub Database Cannot be External on GCP](#).

💡 Note: To configure an external database for UAA, see the *External Database Configuration* section of [Configure UAA](#).

⚠ warning: Protect whichever database you use in your deployment with a password.

To specify your PAS databases, perform the following steps:

1. Select the **External Databases** option.
2. In the **Hostname** field, enter the IP address of the Google Cloud SQL instance that you created in [Step 6: Create Database Instance and Databases](#) of the *Preparing to Deploy Ops Manager on GCP Manually* topic. You can obtain this address from the Instances dashboard of the **SQL** configuration page in the GCP Console.
3. In the **TCP Port** field, enter `3306`.
4. Each component that requires a relational database has two corresponding fields: one for the database username and one for the database password. For each set of fields, specify the username that can access this specific database on the database server and a password for the provided username. You created these users in [Preparing to Deploy Ops Manager on GCP Manually](#).

Place the databases used by Elastic Runtime components.

Choose the location of your system databases*

☐ Internal Databases - MySQL (preferred for complete high-availability)

☒ External Databases (preferred if, for example, you use AWS RDS)

Hostname *

TCP Port *

App Usage Service Database Username *

App Usage Service Database Password *

[Change](#)

Autoscaling Service Database Username *

Autoscaling Service Database Password *

[Change](#)


Cloud Controller Database Username *

Cloud Controller Database Password *

[Change](#)

5. Click **Save**.

Step 14: (Optional) Configure Internal MySQL

 **Note:** You only need to configure this section if you have selected **Internal Databases - MySQL** in the **Databases** section.

1. Select **Internal MySQL**.
2. In the **MySQL Proxy IPs** field, enter one or more comma-delimited IP addresses that are not in the reserved CIDR range of your network. If a MySQL node fails, these proxies re-route connections to a healthy node. See the [MySQL Proxy](#) topic for more information.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.


A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.

The automated backups functionality works with any S3-compatible file store that can receive your backup files.


MySQL Proxy IPs

MySQL Service Hostname

- For **MySQL Service Hostname**, enter an IP address or hostname for your load balancer. If a MySQL proxy fails, the load balancer re-routes connections to a healthy proxy. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.

 **warning:** You must configure a load balancer to achieve complete high availability.

- In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
- In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.
- (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
- To prohibit the creation of command line history files on the MySQL nodes, deselect the **Allow Command History** checkbox.
- To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

- For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the

Replication canary time period *

Replication canary read delay *

E-mail address (required) *

☒ Allow Command History

Cluster Probe Timeout

default value is 10 seconds.

10. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.

11. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.

- a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.

Server Activity Logging*

☐ Disable server activity logging

☒ Enable server activity logging

Event types *

Load Balancer Healthy Threshold *

Load Balancer Unhealthy Threshold *

Save

12. Enter values for the following fields:

- o **Load Balancer Healthy Threshold:** Specifies the amount of time, in seconds, to wait until declaring the MySQL proxy instance started. This allows an external load balancer time to register the instance as healthy.
- o **Load Balancer Unhealthy Threshold:** Specifies the amount of time, in seconds, that the MySQL proxy continues to accept connections before shutting down. During this period, the healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.

13. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.

14. Click **Save**.

Step 15: Configure File Storage

To minimize system downtime, Pivotal recommends using highly resilient and redundant *external* filestores for your Pivotal Application Service (PAS) file storage.

When configuring file storage for the Cloud Controller in PAS, you can select one of the following:

- Internal WebDAV filestore
- External S3-compatible or Ceph-compatible filestore
- External Google Cloud Storage with Access Key and Secret Key
- External Google Cloud Storage with Service Account
- External Azure Cloud Storage

For production-level PCF deployments on GCP, Pivotal recommends selecting **External Google Cloud Storage**. For more information about production-level PCF deployments on GCP, see the [Reference Architecture for Pivotal Cloud Foundry on GCP](#).

For additional factors to consider when selecting file storage, see the [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#) topic.

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External Google Cloud Storage

PAS can use Google Cloud Storage (GCS) as its external filestore by using either a GCP interoperable storage access key or your GCS Service Account. See below for how to configure each option.

External Google Cloud Storage with Access Key and Secret Key

1. Select the **External Google Cloud Storage with Access Key and Secret Key** option

This section determines where you would like to place your Application Service Cloud Controller's file storage.

Configure your Cloud Controller's filesystem*

- ☐ Internal WebDAV (provided by Application Service)
- ☐ External S3-Compatible File Store (if you want to use a service like S3 or Ceph)
- ☒ External Google Cloud Storage with Access Key and Secret Key

Access Key *

Secret Key *

Buildpacks Bucket Name *

Bucket for storing app buildpacks.

Droplets Bucket Name *

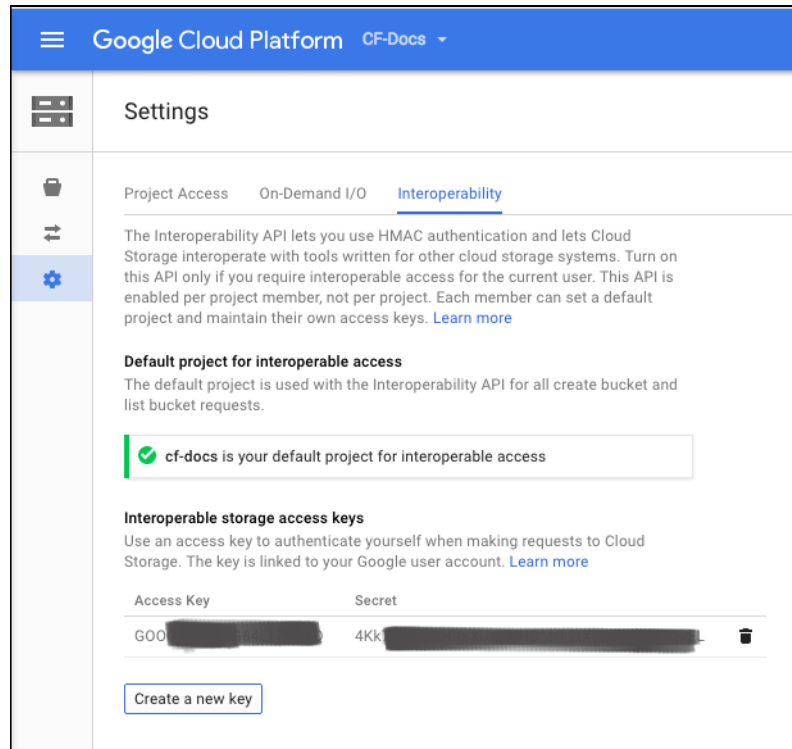
Packages Bucket Name *

Resources Bucket Name *

- ☐ External Google Cloud Storage with Service Account
- ☐ External Azure Storage

2. Enter values for **Access Key** and **Secret Key**. To obtain the values for these fields:

- a. In the GCP Console, navigate to the **Storage** tab, then click **Settings**.
- b. Click **Interoperability**.
- c. If necessary, click **Enable interoperability access**. If interoperability access is already enabled, confirm that the default project matches the project where you are installing PCF.



- d. Click **Create a new key**.
- e. Copy and paste the generated values into the corresponding PAS fields. PCF uses these values for authentication when connecting to Google Cloud Storage.
- f. Enter the names of the storage buckets you created in [Preparing to Deploy Ops Manager on GCP Manually](#):
 - **Buildpacks Bucket Name:** MY-PCF-buildpacks
 - **Droplets Bucket Name:** MY-PCF-droplets
 - **Resources Bucket Name:** MY-PCF-resources
 - **Packages Bucket Name:** MY-PCF-packages
- g. Click **Save**.

External Google Cloud Storage with Service Account

1. Select the **External Google Cloud Storage with Service Account** option

Configure your Cloud Controller's filesystem*

☐ Internal WebDAV (provided by Application Service)
☐ External S3-Compatible File Store (if you want to use a service like S3 or Ceph)
☐ External Google Cloud Storage with Access Key and Secret Key
☒ External Google Cloud Storage with Service Account

GCP Project ID *

GCP Service Account Email *

 Your Google Cloud Platform Service Account Email.

GCP Service Account Key JSON *

Buildpacks Bucket Name *

- a. For **GCP Project ID** enter the Project ID on your GCP Console that you want to use for your PAS file storage.
- b. For **GCP Service Account Email** enter the email address associated with your GCP account.
- c. For **GCP Service Account JSON** enter the account key that you use to access the specified GCP project, in JSON format.
- d. Enter the names of the storage buckets you created in [Preparing to Deploy Ops Manager on GCP Manually](#):
 - **Buildpacks Bucket Name:** MY-PCF-buildpacks
 - **Droplets Bucket Name:** MY-PCF-droplets
 - **Resources Bucket Name:** MY-PCF-resources
 - **Packages Bucket Name:** MY-PCF-packages
- e. Click **Save**.

Other IaaS Storage Options

[Azure Storage](#) and [External S3-Compatible File Storage](#) are also available as file storage options, but Pivotal does not recommend these for a typical PCF on GCP installation.

Step 16: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

Note: The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

- ☒ No
☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging

☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration

Save


2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.



Note: The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.

 **Note:** Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 17: (Optional) Customize Apps Manager

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑
- ▶ Docs 🗑
- ▶ Tools 🗑

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

4. Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
5. Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
6. Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
7. Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
8. The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
9. The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 18: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials


[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

Note: If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 19: (Optional) Configure App Autoscaler

To use App Autoscaler, you must create an instance of the service and bind it to an app. To create an instance of App Autoscaler and bind it to an app, see [Set Up App Autoscaler](#) in the *Scaling an Application Using App Autoscaler* topic.

- Click **App Autoscaler**.

Configure the App Autoscaler

Autoscaler Instance Count (min: 1) *

Autoscaler API Instance Count (min: 1) *

Metric Collection Interval (min: 60, max: 3600) (min: 60, max: 3600) *

Scaling Interval (min: 15, max: 120) (min: 15, max: 120) *

☐ Verbose Logging

☐ Disable API Connection Pooling

☒ Enable Notifications

- Review the following settings:

- Autoscaler Instance Count:** How many instances of the App Autoscaler service you want to deploy. The default value is `3`. For high availability, set this number to `3` or higher. You should set the instance count to an odd number to avoid split-brain scenarios during leadership elections. Larger environments may require more instances than the default number.
- Autoscaler API Instance Count:** How many instances of the App Autoscaler API you want to deploy. The default value is `1`. Larger environments may require more instances than the default number.
- Metric Collection Interval:** How many seconds of data collection you want App Autoscaler to evaluate when making scaling decisions. The minimum interval is 60 seconds, and the maximum interval is 3600 seconds. The default value is `120`. Increase this number if the metrics you use in your scaling rules are emitted less frequently than the existing Metric Collection Interval.
- Scaling Interval:** How frequently App Autoscaler evaluates an app for scaling. The minimum interval is 15 seconds, and the maximum interval is 120 seconds. The default value is `35`.
- Verbose Logging** (checkbox): Enables verbose logging for App Autoscaler. Verbose logging is disabled by default. Select this checkbox to see more detailed logs. Verbose logs show specific reasons why App Autoscaler scaled the app, including information about minimum and maximum instance limits, App Autoscaler's status. For more information about App Autoscaler logs, see [App Autoscaler Events and Notifications](#).
- Disable API Connection Pooling:** API connection pooling increases performance by reducing the cost associated with establishing new connections. If you do not want to keep connections open for reuse, select this option.

3. Click **Save**.

Step 20: Configure Cloud Controller

1. Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
 ☒ Disable

Save

2. Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

3. CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

4. Click **Save**.

Step 21: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

1. Select **Smoke Tests**.
2. If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

- ☐ Temporary space within the system organization (This is deleted after smoke tests finish.)
- ☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.

Step 22: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

Note: Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.

Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.

Whitelist for non-RFC-1918 Private Networks *

allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.

CF CLI Connection Timeout

15

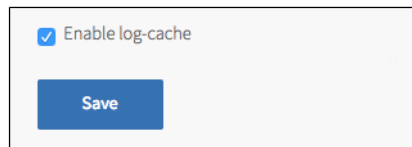
2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PASTopic*.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



A screenshot of a configuration panel. It contains a checkbox labeled 'Enable log-cache' which is checked. Below the checkbox is a blue button labeled 'Save'.

2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

⚠ warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 23: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

💡 Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.

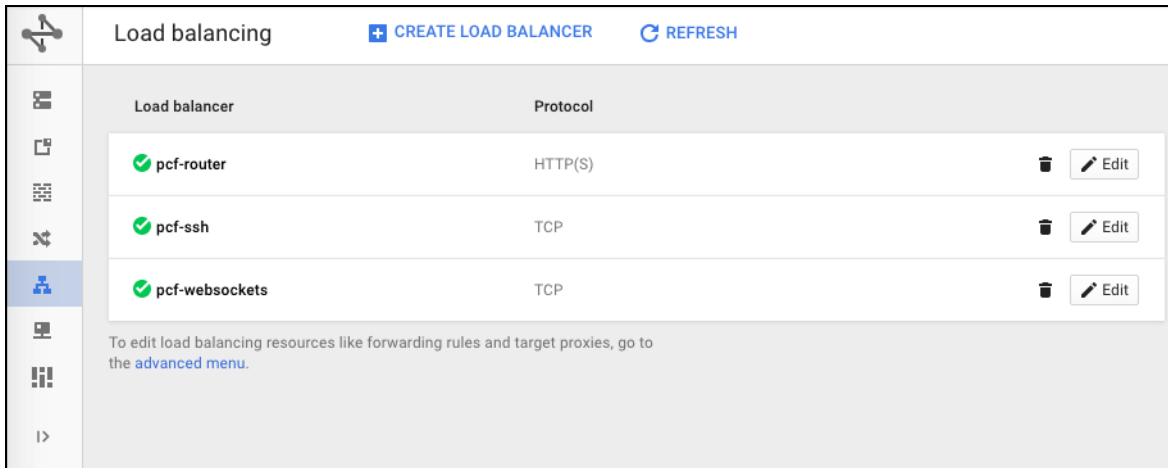
- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

💡 Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.

- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.
- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

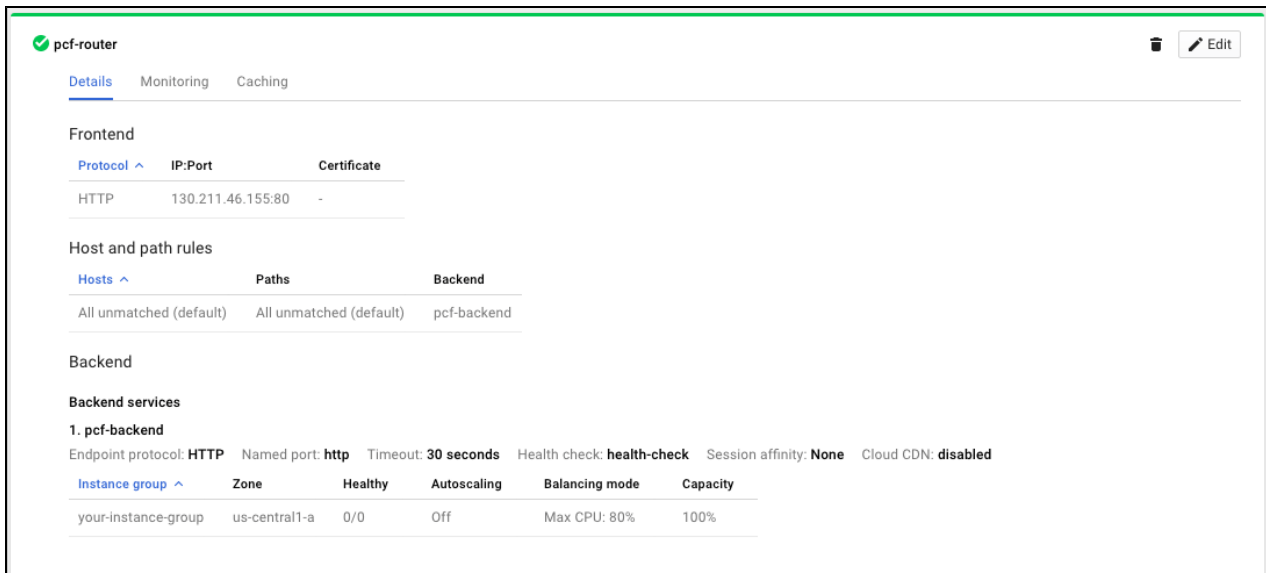
Step 24: Configure Load Balancers

1. Navigate to the GCP Console and click **Load balancing**.



You should see the SSH load balancer, the HTTP(S) load balancer, the TCP WebSockets load balancer, and the TCP router that you created in the *Preparing to Deploy Ops Manager on GCP* topic.

- Record the name of your SSH load balancer and your TCP WebSockets load balancer, `MY-PCF-wss-logs` and `MY-PCF-ssh-proxy`.
- Click your HTTP(S) load balancer, `MY-PCF-global-pcf`.




- Under **Backend services**, record the name of the backend service of the HTTP(S) load balancer, `MY-PCF-http-lb-backend`.
- In the PAS tile, click **Resource Config**.


Resource Config

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|-------------------------------|--------------|----------------------|---|----------------|-------------------------------------|
| Consul | 1 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| NATS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| File Storage | Automatic: 1 | Automatic: 100 GB | Automatic: medium.mem (cpu: 1, ram: 6 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Proxy | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Server | 1 | Automatic: 100 GB | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 64 GB) | | <input checked="" type="checkbox"/> |
| Backup Prepare Node | Automatic: 1 | Automatic: 200 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego BBS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| UAA | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| HAProxy | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Router | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-web-elb | <input checked="" type="checkbox"/> |
| MySQL Monitor | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Clock Global | Automatic: 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller Worker | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego Brain | 1 | Automatic: 1 GB | Automatic: small (cpu: 1, ram: 2 GB, disk: 8 GB) | pcf-ssh-elb | <input checked="" type="checkbox"/> |
| Diego Cell | 1 | None | Automatic: xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB) | | <input checked="" type="checkbox"/> |
| Loggregator Trafficcontroller | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Adapter | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Scheduler | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Doppler Server | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| TCP Router | 0 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-tcp-elb | <input checked="" type="checkbox"/> |
| CredHub | Automatic: 0 | None | Automatic: large (cpu: 2, ram: 8 GB, disk: 16 GB) | | <input checked="" type="checkbox"/> |


Save

6. Under the **LOAD BALANCERS** column of the **Router** row, enter a comma-delimited list consisting of the name of your TCP WebSockets load balancer and the name of your HTTP(S) load balancer backend with the protocol prepended. For example, `tcp:MY-PCF-wss-logs,http:MY-PCF-http-lb-backend`.

 **Note:** Do not add a space between key/value pairs in the **LOAD BALANCER** field or it will fail.


 **Note:** If you are using HAProxy in your deployment, then enter the above load balancer values in the **LOAD BALANCERS** field of the **HAProxy** row instead of the **Router** row. For a high availability configuration, scale up the HAProxy job to more than one instance.


7. If you have enabled TCP routing in the [Networking](#) pane and set up the [TCP Load Balancer in GCP](#), add the name of your TCP load balancer, prepended with `tcp:`, to the **LOAD BALANCERS** column of the TCP Router row. For example, `tcp:pcf-tcp-router`.
8. Enter the name of you SSH load balancer depending on which release you are using.
- PAS:** Under the **LOAD BALANCERS** column of the **Diego Brain** row, enter the name of your SSH load balancer prepended with `tcp:`. For example, `tcp:MY-PCF-ssh-proxy`.
 - Small Footprint Runtime:** Under the **LOAD BALANCERS** column of the **Control** row, enter the name of your SSH load balancer prepended with `tcp:`.
9. Verify that the **Internet Connected** checkbox for every job is unchecked. When preparing your GCP environment, you provisioned a Network Address Translation (NAT) box to provide Internet connectivity to your VMs instead of providing them with public IP addresses to allow the jobs to reach the Internet.

 **Note:** If you want to provision a Network Address Translation (NAT) box to provide Internet connectivity to your VMs instead of providing them with public IP addresses, deselect the **Internet Connected** checkboxes. For more information about using NAT in GCP, see the [GCP documentation](#).

10. Click **Save**.

Step 25: (Optional) Scale Down and Disable Resources

 **Note:** The **Resource Config** pane has fewer VMs if you are installing the [Small Footprint Runtime](#).

 **Note:** The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to instances and scale the **Control** VM to instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by navigating to the **Resource Config** section and using the dropdowns under **Instances** for each job.


By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding system-provided resources in Ops Manager to reduce costs and administrative overhead.

To disable specific VMs in Ops Manager, do the following:

1. Click **Resource Config**.
2. If you configured PAS to use an external S3-compatible filestore, enter in **Instances** in the **File Storage** field.
3. If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:
 - **MySQL Proxy:** Enter in **Instances**.
 - **MySQL Server:** Enter in **Instances**.
 - **MySQL Monitor:** Enter in **Instances**.
4. If you disabled TCP routing, enter **Instances** in the **TCP Router** field.
5. If you are not using HAProxy, enter **Instances** in the **HAProxy** field.
6. Click **Save**.

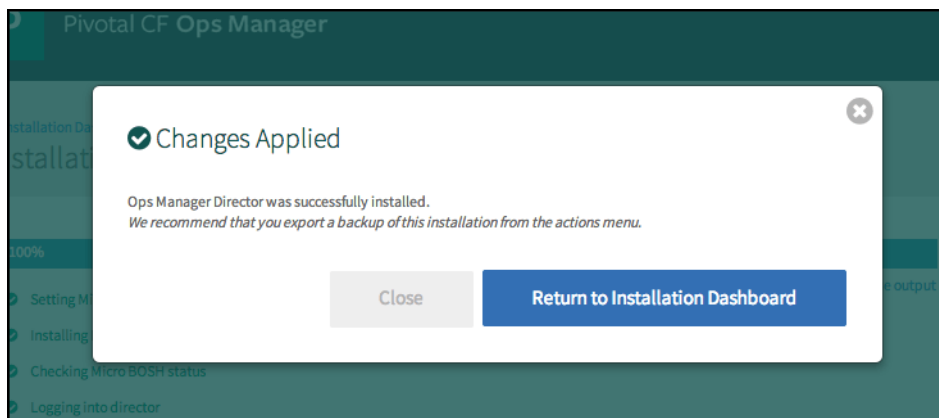
Step 26: Download Stemcell

This step is only required if your Ops Manager does not already have the stemcell version required by PAS. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

1. Open the [Stemcell product page](#)  in the Pivotal Network. *Note, you may have to log in.*
2. Download the appropriate stemcell version targeted for your IaaS.
3. Navigate to **Stemcell Library** in the **Installation Dashboard**.
4. Click **Import Stemcell** to import the downloaded stemcell file.
5. When prompted, enable the Ops Manager product checkbox to stage your stemcell.
6. Click **Apply Stemcell to Products**.

Step 27: Complete the PAS Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**.
The install process generally requires a minimum of 90 minutes to complete. The image shows the Changes Applied window that displays when the installation process successfully completes.



Installing PCF on GCP Using Terraform

This topic explains how to install PCF on GCP using Terraform.

Overview

You can install PCF on GCP with either the Pivotal Application Service (PAS) or Pivotal Container Service (PKS) runtime.

To install PCF on GCP using Terraform, do one of the following:

- Install with PAS. See [Install on PAS Using Terraform](#).
- Install with PKS. See [Install on PKS Using Terraform](#).

Install with PAS Using Terraform

To install with PAS using Terraform, do the following:

1. Deploy Ops Manager. See [Deploying Ops Manager on GCP Using Terraform](#).
2. Configure BOSH Director. See [Configuring BOSH Director on GCP Using Terraform](#).
3. (Optional) Configure a shared VPC. See [\(Optional\) Configuring a Shared VPC on GCP](#).
4. Configure PAS. See [Deploying PAS on GCP Using Terraform](#).

Install with PKS Using Terraform

To install with PKS using Terraform, do the following:

1. Deploy Ops Manager. See [Deploying Ops Manager on GCP Using Terraform](#).
2. Configure BOSH Director. See [Configuring BOSH Director on GCP Using Terraform](#).
3. (Optional). Configure a shared VPC. See [\(Optional\) Configuring a Shared VPC on GCP](#).
4. Configure PKS. See [Installing PKS on GCP](#) [↗](#).

Deploying Ops Manager on GCP Using Terraform

Page last updated:

This guide describes the preparation steps required to install Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP) using Terraform templates.

The Terraform template for PCF on GCP describes a set of GCP resources and properties. For more information about how Terraform creates resources in GCP, see the [Google Cloud Provider](#) topic on the Terraform site.

You may also find it helpful to review different deployment options in the [Reference Architecture for Pivotal Cloud Foundry on GCP](#).

Prerequisites

In addition to fulfilling the prerequisites listed in the [Installing Pivotal Cloud Foundry on GCP](#) topic, ensure you have the following:

- The [Terraform CLI](#)
- The [Google Cloud SDK](#)
- In your GCP project, enable the following APIs:
 - [Identity and Access Management](#)
 - [Cloud Resource Manager](#)
 - [Cloud DNS](#)
 - [Cloud SQL API](#)
 - [Compute Engine API](#)

Step 1: Obtain a GCP Service Account Key File

To use the Terraform templates to create the necessary infrastructure resources for PCF, you need a service account key file.

To create an account key file, follow the procedure below corresponding to your own use case.

- **I already have a service account I want to use:**

1. Navigate to the GCP console.
2. Select **IAM** and locate your service account.
3. From the **Options** column, open the dropdown and click **Create Key**.

- **I want to create a new service account:**

1. Open a terminal window.
2. To create a service account using the gcloud CLI, run the following command:

```
gcloud iam service-accounts create ACCOUNT-NAME
```

3. To create a key file for your service account, run the following command:

```
gcloud iam service-accounts keys create "terraform.key.json" --iam-account "ACCOUNT-NAME@PROJECT-ID.iam.gserviceaccount.com"
```

4. To bind the service account to your project and give it the owner role, run the following command:

```
gcloud projects add-iam-policy-binding PROJECT-ID --member 'serviceAccount:ACCOUNT-NAME@PROJECT-ID.iam.gserviceaccount.com' --role 'roles
```

Where:

- `ACCOUNT-NAME` is the name you want to apply to the new account.
- `PROJECT-ID` is your Google Cloud Platform Project ID.

Step 2: Download Templates and Edit Variables File

Before you can run Terraform commands to provision infrastructure resources, you must download the GCP Terraform Templates and create a Terraform template variables file as described below:

1. On [Pivotal Network](#), navigate to the Pivotal Application Service (PAS) release.
2. Download the GCP Terraform ZIP file.
3. Extract the contents of the ZIP file.
4. Move the extracted folder to the `workspace` directory on your local machine.
5. On the command line, navigate to the directory. For example:

```
$ cd ~/workspace/pivotal-cf-terraforming-gcp
```

6. Navigate to the `terraforming-pas` or `terraforming-pks` directory that contains the Terraform files for your runtime.
7. In the runtime directory, create a text file named `terraform.tfvars`.
8. Open the `terraform.tfvars` file and add the following:

```
env_name      = "YOUR-ENVIRONMENT-NAME"
opsman_image_url = "YOUR-OPS-MAN-IMAGE-URL"
region       = "YOUR-GCP-REGION"
zones        = ["YOUR-AZ-1", "YOUR-AZ-2", "YOUR-AZ-3"]
project      = "YOUR-GCP-PROJECT"
dns_suffix    = "YOUR-DNS-SUFFIX"

ssl_cert = <<SSL_CERT
-----BEGIN CERTIFICATE-----
YOUR-CERTIFICATE
-----END CERTIFICATE-----
SSL_CERT

ssl_private_key = <<SSL_KEY
-----BEGIN EXAMPLE RSA PRIVATE KEY-----
YOUR-PRIVATE-KEY
-----END EXAMPLE RSA PRIVATE KEY-----
SSL_KEY

service_account_key = <<SERVICE_ACCOUNT_KEY
YOUR-KEY-JSON
SERVICE_ACCOUNT_KEY
```

9. Edit the values in the file according to the table below.

| Value to replace | Guidance |
|--|--|
| <code>YOUR-ENVIRONMENT-NAME</code> | Enter a name to use to identify resources in GCP. Terraform prepends the names of the resources it creates with this environment name. Example: <code>pcf</code> . |
| <code>YOUR-OPS-MAN-IMAGE-URL</code> | Enter the source URL of the Ops Manager image you want to boot. You can find this URL in the PDF included with the Ops Manager release on Pivotal Network . |
| <code>YOUR-GCP-REGION</code> | Enter the name of the GCP region in which you want Terraform to create resources. Example: <code>us-central1</code> . |
| <code>YOUR-AZ-1</code> <code>YOUR-AZ-2</code> <code>YOUR-AZ-3</code> | Enter three availability zones from your region. Example: <code>us-central1-a</code> , <code>us-central1-b</code> , <code>us-central1-c</code> . |
| <code>YOUR-GCP-PROJECT</code> | Enter the name of the GCP project in which you want Terraform to create resources. |
| <code>YOUR-DNS-SUFFIX</code> | Enter a domain name to use as part of the system domain for your PCF deployment. Terraform creates DNS records in GCP using <code>YOUR-ENVIRONMENT-NAME</code> and <code>YOUR-DNS-SUFFIX</code> . For example, if you enter <code>example.com</code> for your DNS suffix and have <code>pcf</code> as your environment name, Terraform creates DNS records at <code>pcf.example.com</code> . |
| <code>YOUR-CERTIFICATE</code> | Enter a certificate to use for HTTP load balancing. For production environments, use a certificate from a Certificate Authority (CA). For test environments, you can use a self-signed certificate. Your certificate must specify your system domain as the common name. Your system domain |


| | |
|-------------------------------|--|
| | is <code>YOUR-ENVIRONMENT-NAME.YOUR-DNS-SUFFIX</code> . It also must include the following subdomains: <code>*.sys.YOUR-SYSTEM-DOMAIN</code> , <code>*.login.sys.YOUR-SYSTEM-DOMAIN</code> , <code>*.uaa.sys.YOUR-SYSTEM-DOMAIN</code> , <code>*.apps.YOUR-SYSTEM-DOMAIN</code> . |
| <code>YOUR-PRIVATE-KEY</code> | Enter a private key for the certificate you entered. |
| <code>YOUR-KEY-JSON</code> | Enter the contents of your service account key file. This file is in JSON format. |

Step 3: Add Optional Variables

Complete this step if you want to do any of the following:

- Change the default CIDR ranges
- Deploy the Isolation Segment tile
- Use an external Google Cloud SQL database
- Use external Google Storage buckets
- Disable generated GCP service account key for blobstore

In your `terraform.tfvars` file, specify the appropriate variables from the sections below.

 **Note:** You can see the configurable options by opening the `variables.tf` file and looking for variables with default values.

CIDR Ranges for Subnets

If you want to change the CIDR ranges for the management, your runtime, or services networks that Terraform creates, add the following variables to your `terraform.tfvars` file, replacing `YOUR-MANAGEMENT-CIDR`, `YOUR-RUNTIME-CIDR` and `YOUR-SERVICES-CIDR` with your desired values.

```
management_cidr = YOUR-MANAGEMENT-CIDR
pas_cidr = YOUR-RUNTIME-CIDR
services_cidr = YOUR-SERVICES-CIDR
```

Isolation Segments

If you plan to deploy the Isolation Segment tile, add the following variables to your `terraform.tfvars` file, replacing `YOUR-CERTIFICATE` and `YOUR-PRIVATE-KEY` with a certificate and private key. This causes Terraform to create an additional HTTP load balancer across three availability zones to use for the Isolation Segment tile.

```
isolation_segment = true
iso_seg_ssl_cert = <<ISO_SEG_SSL_CERT
-----BEGIN CERTIFICATE-----
YOUR-CERTIFICATE
-----END CERTIFICATE-----
ISO_SEG_SSL_CERT
iso_seg_ssl_cert_private_key = <<ISO_SEG_SSL_KEY
-----BEGIN EXAMPLE RSA PRIVATE KEY-----
YOUR-PRIVATE-KEY
-----END EXAMPLE RSA PRIVATE KEY-----
ISO_SEG_SSL_KEY
```

External Database

1. If you want to use an external Google Cloud SQL database for Ops Manager and Pivotal Application Service (PAS), add the following to your `terraform.tfvars` file:

```
external_database = true
```

2. If you want to specify a single host from which users can connect to the Ops Manager and runtime databases, add the following to your `terraform.tfvars` file.

```
opsman_sql_db_host = HOST-IP-ADDRESS
pas_sql_db_host = HOST-IP-ADDRESS
```

Where `HOST-IP-ADDRESS` is your desired IP address(es).

External Storage Buckets

If you want to use Google Cloud Storage buckets for the PAS Cloud Controller, add the following to your `terraform.tfvars` file:

```
create_gcs_buckets = true
```

GCP Service Account Key for Blobstore

If you want to provide your own service account for blob storage instead of using a generated service account, add the following to your `terraform.tfvars` file:

```
create_blobstore_service_account_key = false
```

Step 4: Create GCP Resources with Terraform

Follow these steps to use the Terraform CLI to create resources on GCP:

1. From the directory that contains the Terraform files, run the following command to initialize the directory based on the information you specified in the `terraform.tfvars` file.

```
terraform init
```

2. Run the following command to create the execution plan for Terraform.

```
terraform plan -out=plan
```

3. To execute the plan from the previous step, run the following command:

```
terraform apply plan
```



Note: It may take several minutes for Terraform to create all the resources in GCP.

Step 5: Create DNS Record

1. In a browser, navigate to the DNS provider for the DNS suffix you entered in your `terraform.tfvars` file.
2. Create a new NS (Name server) record for your PCF system domain. Your system domain is `YOUR-ENVIRONMENT-NAME.YOUR-DNS-SUFFIX`.
 - a. In this record, enter the name servers included in `env_dns_zone_name_servers` from your Terraform output.

Next Steps

After you complete this procedure, follow the instructions in the [Configuring BOSH Director on GCP Using Terraform](#) topic.

Configuring BOSH Director on GCP Using Terraform

Page last updated:

This topic describes how to configure the BOSH Director for Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP) after [Preparing to Deploy Ops Manager on GCP Using Terraform](#).

Note: You can also perform the procedures in this topic using the Ops Manager API. For more information, see the [Using the Ops Manager API](#) topic.

Prerequisite

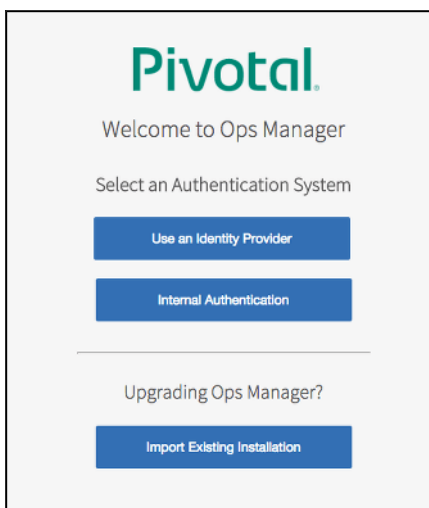
To complete the procedures in this topic, you must have access to the output from when you ran `terraform apply` to create resources for this deployment. You can view this output at any time by running `terraform output`. You use the values in your Terraform output to configure the BOSH Director tile.

Step 1: Access Ops Manager

1. In a web browser, navigate to the fully qualified domain name (FQDN) of the BOSH Director. Use the `ops_manager_dns` value from running `terraform output`.

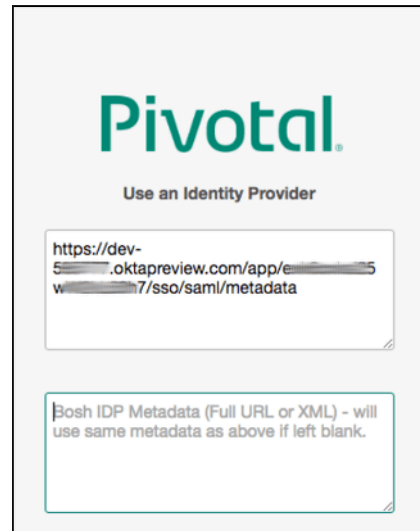
Note: In order to set up Ops Manager authentication correctly, Pivotal recommends using a Fully Qualified Domain Name (FQDN) to access Ops Manager. Using an ephemeral IP address to access Ops Manager can cause authentication errors upon subsequent access.

2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you use an Identity Provider, an external identity server maintains your user database.
 - [Internal Authentication](#): If you use Internal Authentication, Ops Manager maintains your user database.



Use an Identity Provider (IdP)

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.



2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.

Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a `500` error.

Note: These attributes are case-sensitive.

- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.

5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.

6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

Note: To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.

- **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
- **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
- **Name ID:** Email Address
- SAML authentication requests are always signed

8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.

- **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
- **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
- **Name ID:** Email Address
- SAML authentication requests are always signed

9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

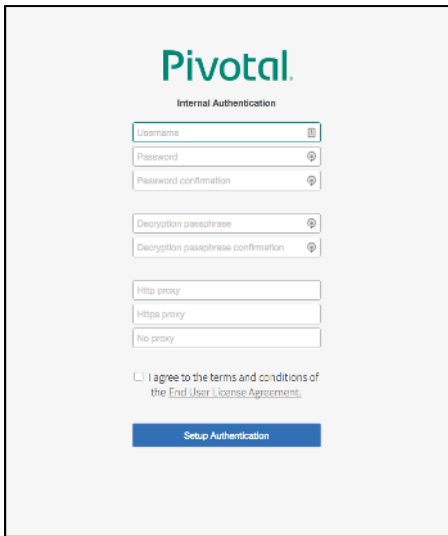
Internal Authentication

1. When redirected to the **Internal Authentication** page, do the following:

- Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
- Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not

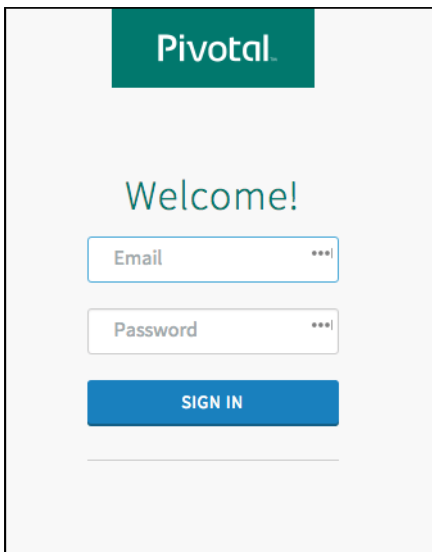
recoverable if lost.

- If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in the [Configuring Proxy Settings for the BOSH CPI](#) topic.
- Read the **End User License Agreement**, and select the checkbox to accept the terms.
- Click **Setup Authentication**.



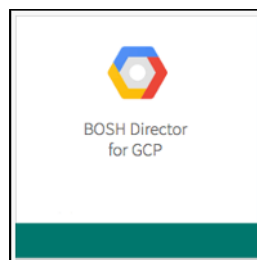
The image shows the 'Pivotal Internal Authentication' setup form. It includes fields for Username, Password, Password confirmation, Decryption passphrase, and Decryption passphrase confirmation. There are also fields for Http proxy, Https proxy, and No proxy. A checkbox for 'I agree to the terms and conditions of the End User License Agreement' is present, followed by a 'Setup Authentication' button.

2. Log in to Ops Manager with the Admin username and password that you created in the previous step.




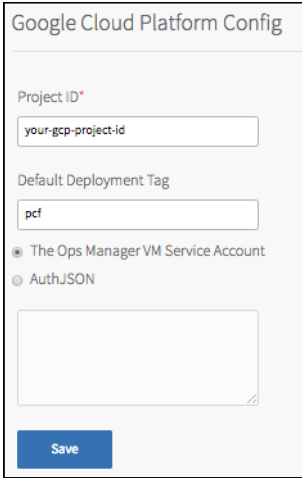
The image shows the 'Pivotal Welcome!' login form. It features a 'Pivotal' logo at the top, followed by a 'Welcome!' message. Below this are input fields for 'Email' and 'Password', both with masked characters (***). A blue 'SIGN IN' button is positioned below the password field.

Step 2: Google Cloud Platform Config



1. Click the **Google Cloud Platform** tile within the **Installation Dashboard**.
2. Select **Google Config**. Complete the following fields:
 - **Project ID**: Enter the value of `project` from your `terraform.tfvars` file.
 - **Default Deployment Tag**: Enter the value of `env_name` from your `terraform.tfvars` file.
 - Select **AuthJSON** and in the field below enter the contents of the JSON file for your service account key.

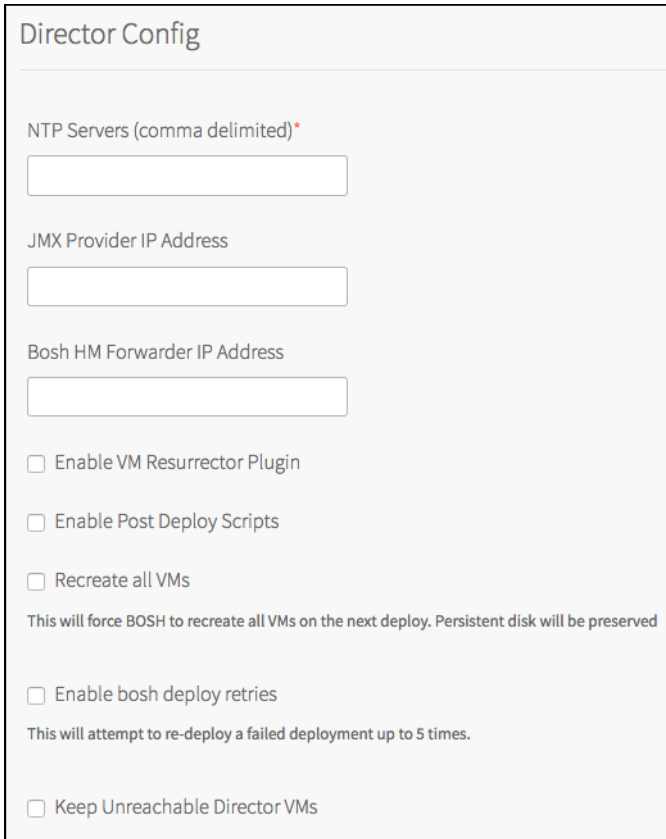
 **Note:** As an alternative, you can select **The Ops Manager VM Service Account** option to use the service account automatically created by GCP for the Ops Manager VM.




3. Click **Save**.


Step 3: Director Config Page

1. Select **Director Config** to open the **Director Config** page.




2. In the **NTP Servers (comma delimited)** field, enter `metadata.google.internal`.

 **Note:** To resolve `metadata.google.internal` as the NTP server hostname, you must provide the two IP addresses for DNS configuration as described in [Step 5: Create Networks Page](#) of this procedure.


 **Note:** The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify

the value of this field.


3. Leave the **JMX Provider IP Address** field blank.

 **Note:** Starting from PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use PCF JMX Bridge for consuming them outside of the Firehose, you may receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

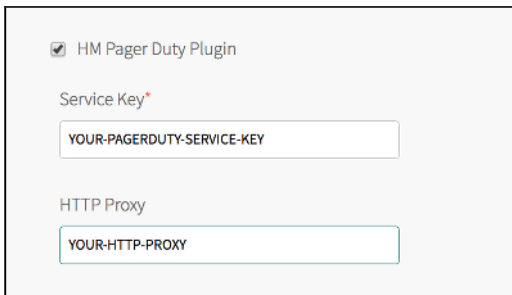
4. Leave the **Bosh HM Forwarder IP Address** field blank.

 **Note:** Starting from PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. Therefore, if you continue to use the BOSH HM Forwarder for consuming them, you may receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#).

5. Select the **Enable VM Resurrector Plugin** checkbox to enable the Ops Manager Resurrector functionality and increase Pivotal Application Service (PAS) availability.
6. (Optional) Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.

 **Note:** You must enable post-deploy scripts to install PKS.

7. (Optional) Select **Recreate all VMs** to force BOSH to recreate all VMs on the next deploy. This process does not destroy any persistent disk data.
8. Select **Enable bosh deploy retries** for Ops Manager to retry failed BOSH operations up to five times.
9. (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS secure communications.
10. (Optional) Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.
11. (Optional) Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.



☒ HM Pager Duty Plugin

Service Key*

YOUR-PAGERDUTY-SERVICE-KEY

HTTP Proxy

YOUR-HTTP-PROXY

- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.

☒ **HM Email Plugin**

Host*

Port*

Domain*

From*

Recipients*

Username

Password


☒ **Enable TLS**

12. (Optional) Select **HM Email Plugin** to enable Health Monitor integration with email.

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma-separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter the password for your email server.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

13. For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

 **Note:** After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*


HSM Port Address*

Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**
 9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal
☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature
☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- o **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- o **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. Follow the procedures in [Sign up for Amazon S3](#) and [Creating a Bucket](#) in the AWS documentation. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.


- **GCS Blobstore:** Select this option to use an external Google Cloud Storage (GCS) endpoint. To create a GCS bucket, follow the procedures in [Creating Storage Buckets](#) in the GCS documentation. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Enter the contents of the JSON file that you downloaded in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually*.

15. For **Database Location**, if you configured your `terraform.tfvars` file to create an external database for Ops Manager, select **External MySQL Database** and complete the fields below. Otherwise, select **Internal**.


- **Host:** Enter the value of `sql_db_ip` from your Terraform output.
- **Port:** Enter `3306`.
- **Username:** Enter the value of `opsman_sql_username` from your Terraform output.
- **Password:** Enter the value of `opsman_sql_password` from your Terraform output.
- **Database:** Enter the value of `opsman_sql_db_name` from your Terraform output.

In addition, if you selected **External MySQL Database**, you can fill out the following optional fields:

- **Enable TLS:** Selecting this checkbox enables TLS communication between the BOSH Director and the database.
- **TLS CA:** Enter the Certificate Authority for the TLS Certificate.
- **TLS Certificate:** Enter the client certificate for mutual TLS connections to the database.
- **TLS Private Key:** Enter the client private key for mutual TLS connections to the database.
- **Advanced DB Connection Options:** If you would like to provide additional options for the database, use this field to provide a JSON-formatted options string.

 **Note:** You must select **Enable TLS for Director Database** to configure the TLS-related fields.

16. (Optional) Modify the **Director Workers** value, which sets the number of workers available to execute Director tasks. This field defaults to `5`.
17. (Optional) **Max Threads** sets the maximum number of threads that the BOSH Director can run simultaneously. Pivotal recommends that you leave the field blank to use the default value, unless doing so results in rate limiting or errors on your IaaS.
18. (Optional) To add a custom URL for your BOSH Director, enter a valid hostname in **Director Hostname**. You can also use this field to configure [a load balancer in front of your BOSH Director](#).

 **warning:** In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, VMs become unavailable. This causes PCF downtime. To restore VM availability, enable **Recreate All VMs** and redeploy. This issue is resolved in [Ops Manager v2.2.8](#) and later.

Director Workers


5


Max Threads

Director Hostname

opsdirector.example.com

19. (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.
20. (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.

 **Note:** Disabling BOSH DNS affects [Step 5: Create Networks Page](#) below when you configure your network DNS. You must first navigate to your PAS tile and enter `8.8.8.8` into the **DNS Servers** field.

 **Breaking Change:** Do not disable BOSH DNS without consulting Pivotal Support.

21. (Optional) To set a custom banner that users see when logging in to the Director using SSH, enter text in the **Custom SSH Banner** field.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

22. (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1,hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.
23. Click **Save**.

Step 4: Create Availability Zones Page


 **Note:** Pivotal recommends at least three availability zones for a highly available installation of PAS. For an example of a three availability zone deployment, see [Reference Architecture for Pivotal Cloud Foundry on GCP](#).


1. Select **Create Availability Zones**.
2. Use the **Add** button to add three availability zones corresponding to those listed in the `azs` field in your Terraform output.
3. Click **Save**.

Step 5: Create Networks Page

1. Select **Create Networks**.
2. Make sure **Enable ICMP checks** is not selected. GCP routers do not respond to ICMP pings.

- Use the **Add Network** button to create the following three networks:

 **Note:** To use a shared VPC network, enter the shared VPC host project name before the network name in the format `VPC-PROJECT-NAME/NETWORK-NAME/SUBNET-NAME/REGION-NAME`. For example, `vpc-project/opsmgr/central/us-central1`. For more information, see [Configuring a Shared VPC on GCP](#).

 **Note:** If you disabled BOSH DNS, enter `8.8.8.8` into the **DNS Servers** field of the PAS tile. For more information, see step 29g in the *Configure Networking* section of the [Deploying PAS on GCP Using Terraform](#) topic.

Infrastructure Network

| | |
|---------------------|---|
| Network Name | infrastructure |
| Google Network Name | Use the <code>network_name</code> , <code>infrastructure_subnet_name</code> , and <code>region</code> fields from your Terraform output to enter the name of the infrastructure network created by Terraform. The format is: <code>network_name/infrastructure_subnet_name/region</code> |
| CIDR | Enter the value of <code>infrastructure_subnet_cidrs</code> from your Terraform output. |
| Reserved IP Ranges | Enter the first <code>.1</code> through <code>.9</code> addresses from the CIDR. For example, if the CIDR is <code>192.168.101.0/26</code> , enter the range <code>192.168.101.1-192.168.101.9</code> . |
| DNS | 169.254.169.254 |
| Gateway | Enter the value of <code>infrastructure_subnet_gateway</code> from your Terraform output. |
| Availability Zones | Select all three availability zones. |

Runtime Network

| | |
|---------------------|--|
| Network Name | pas |
| Google Network Name | Use the <code>network_name</code> , <code>pas_subnet_name</code> , and <code>region</code> fields from your Terraform output to enter the name of the PAS network created by Terraform. The format is: <code>network_name/pas_subnet_name/region</code> |
| CIDR | Enter the value of <code>pas_subnet_cidrs</code> from your Terraform output. |
| Reserved IP Ranges | Enter the first <code>.1</code> through <code>.9</code> addresses from the CIDR. For example, if the CIDR is <code>192.168.16.0/22</code> , enter the range <code>192.168.16.1-192.168.16.9</code> . |
| DNS | 169.254.169.254 |
| Gateway | Enter the value of <code>pas_subnet_gateway</code> from your Terraform output. |
| Availability Zones | Select all three availability zones. |

Services Network

| | |
|---------------------|---|
| Network Name | services |
| Google Network Name | Use the <code>network_name</code> , <code>services_subnet_name</code> , and <code>region</code> fields from your Terraform output to enter the name of the services network created by Terraform. The format is: <code>network_name/services_subnet_name/region</code> |
| CIDR | Enter the value of <code>services_subnet_cidrs</code> from your Terraform output. |
| Reserved IP Ranges | Enter the first <code>.1</code> through <code>.9</code> addresses from the CIDR. For example, if the CIDR is <code>192.168.16.0/22</code> , enter the range <code>192.168.20.1-192.168.20.9</code> . |
| DNS | 169.254.169.254 |
| Gateway | Enter the value of <code>services_subnet_gateway</code> from your Terraform output. |
| Availability Zones | Select all three availability zones. |



Note: After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

Step 6: Assign AZs and Networks Page

1. Select **Assign AZs and Networks**.
2. Use the dropdown to select a **Singleton Availability Zone**. The BOSH Director installs in this Availability Zone.
3. Under **Network**, select the **infrastructure** network for your BOSH Director.
4. Click **Save**.

Step 7: Security Page

Security

Trusted Certificates

-----BEGIN CERTIFICATE-----

THE-----

-----END CERTIFICATE-----

These certificates enable BOSH-deployed components to trust a custom root certificate.

Generate VM passwords or use single password for all VMs

☒ Generate passwords
 ☐ Use default BOSH password

Save

1. Select **Security**.
2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:

```
-----BEGIN CERTIFICATE-----
ABCDEF12345678ABCDEF12345678ABCDEF12345678AB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BCDEF12345678ABCDEF12345678ABCDEF12345678ABB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CDEF12345678ABCDEF12345678ABCDEF12345678ABBB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
-----END CERTIFICATE-----
```



Note: If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#) for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 8: Syslog Page

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

⌵

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save


2. (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
3. In the **Address** field, enter the IP address or DNS name for the remote server.
4. In the **Port** field, enter the port number that the remote server listens on.
5. In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**P. This selection determines which transport protocol is used to send the logs to the remote server.
6. (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.


- In the **SSL Certificate** field, enter the SSL certificate for the remote server.

7. Click **Save**.

Step 9: Resource Config Page

1. Select **Resource Config**.
2. Verify that the **Internet Connected** checkbox for every job is checked. The Terraform templates do not provision a Network Address Translation (NAT) box for Internet connectivity to your VMs so instead they will be provided with ephemeral public IP addresses to allow the jobs to reach the Internet.

 **Note:** If you want to provision a Network Address Translation (NAT) box to provide Internet connectivity to your VMs instead of providing them with public IP addresses, deselect the **Internet Connected** checkboxes. For more information about using NAT in GCP, see the [GCP documentation](#).

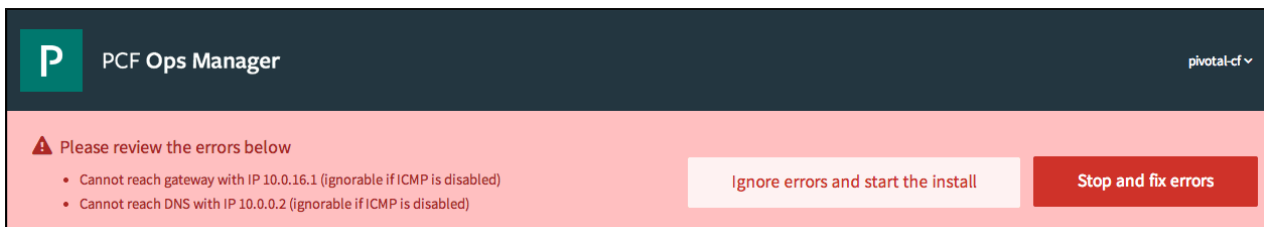
 **Note:** If you install PAS for Windows, provision your **Master Compilation Job** with at least 100 GB of disk space.

Step 10: (Optional) Add Custom VM Extensions

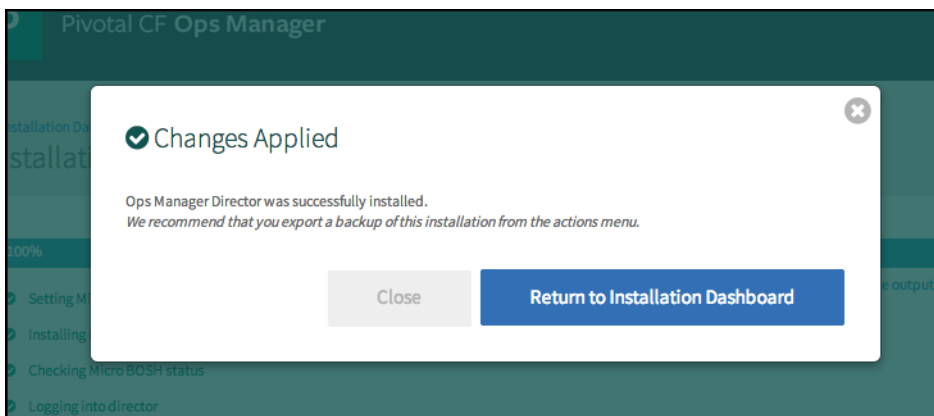
Use the Ops Manager API to add custom properties to your VMs such as associated security groups and load balancers. For more information, see [Managing Custom VM Extensions](#).

Step 11: Complete the BOSH Director Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**. If the following ICMP error message appears, return to the [Network Config](#) screen, and make sure you have deselected the **Enable ICMP Checks** box. Then click **Apply Changes** again.



3. BOSH Director installs. This may take a few moments. When the installation process successfully completes, the **Changes Applied** window appears.



What to Do Next

After you complete this procedure, follow the instructions in the [Deploying PAS on GCP](#) topic.

Deploying PAS on GCP Using Terraform

Page last updated:

This topic describes how to install and configure Pivotal Application Service (PAS) on Google Cloud Platform (GCP).

Before beginning this procedure, ensure that you have successfully completed the [Configuring BOSH Director on GCP Using Terraform](#) topic.

Note: If you plan to [install the PCF IPsec add-on](#), you must do so before installing any other tiles. Pivotal recommends installing IPsec immediately after Ops Manager, and before installing the PAS tile.

Prerequisite

To complete the procedures in this topic, you must have access to the output from when you ran `terraform apply` to create resources for this deployment. You can view this output at any time by running `terraform output`. You use the values in your Terraform output to configure the BOSH Director tile.

Step 1: Download the PAS Tile

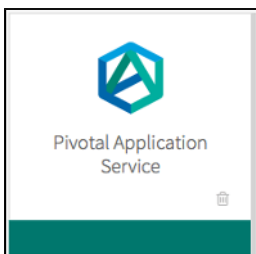
1. If you have not already downloaded PAS, log in to [Pivotal Network](#), and click on **Pivotal Application Service**.
2. From the **Releases** dropdown, select the release to install and choose one of the following:
 - a. Click **Pivotal Application Service** to download the PAS `.pivotal` file.
 - b. Click **PCF Small Footprint Runtime** to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).

Step 2: Add PAS to Ops Manager

1. Navigate to the Pivotal Cloud Foundry Operations Manager Installation Dashboard.
2. Click **Import a Product** to add the PAS tile to Ops Manager. This may take a while depending on your connection speed.

Note: After you import a tile to Ops Manager, you can view the latest available version of that tile in the Installation Dashboard by enabling the Pivotal Network API. For more information, refer to the [Adding and Deleting Products](#) topic.

3. On the left, click the plus icon next to the imported PAS product to add it to the Installation Dashboard.
4. Click the newly added PAS tile in the Installation Dashboard.



Step 3: Assign Availability Zones and Networks

1. Select **Assign AZ and Networks**. These are the Availability Zones that you [create](#) when configuring BOSH Director.
2. Select the first Availability Zone under **Place singleton jobs**. Ops Manager runs any job with a single instance in this Availability Zone.
3. Select all Availability Zones under **Balance other jobs**. Ops Manager balances instances of jobs with more than one instance across the Availability Zones that you specify.



Note: For production deployments, Pivotal recommends at least three Availability Zones for a highly available installation of PAS.

4. From the **Network** dropdown, choose the network you created in [Step 5: Create Networks Page](#) of the *Configuring BOSH Director on GCP Using Terraform* topic.
5. Click **Save**.

Step 5: Configure Domains

1. Select **Domains**.

Application Service hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain *

Apps Domain *

Save

2. Enter the system and application domains that were created by Terraform:
 - **System Domain:** Enter the value of `sys_domain` from your Terraform output.
 - **Apps Domain:** Enter the value of `apps_domain` from your Terraform output.
3. Click **Save**.

Step 6: Configure Networking

1. Select **Networking**.
2. Leave the **Router IPs**, **SSH Proxy IPs**, **HAProxy IPs**, and **TCP Router IPs** fields blank. You do not need to complete these fields when deploying PCF to GCP.



Note: You specify load balancers in the **Resource Config** section of PAS later on in the installation process. See the [Configure Load Balancers](#) section of this topic for more information.

3. Under **Certificates and Private Keys for HAProxy and Router**, you must provide an **SSL Certificate and Private Key**. Starting in PCF v.1.12, HAProxy and the Gorouter are enabled to receive TLS communication by default.

Certificates and Private Keys for HAProxy and Router

Add

▼ example-cert

Name *

example-cert

A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END RSA PRIVATE KEY-----

Generate RSA Certificate

▼ example-cert-2

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *


-----BEGIN CERTIFICATE-----

MIIE...

-----END RSA PRIVATE KEY-----

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager. Ensure the certificate includes `*.YOUR-SYSTEM-DOMAIN`, `*.apps.YOUR-SYSTEM-DOMAIN`, and `*.sys.YOUR-SYSTEM-DOMAIN`.

For details about generating certificates in Ops Manager for your wildcard system domains, see [Providing a Certificate for Your SSL/TLS Termination Point](#).

 **Note:** Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

- (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Router** field, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower

minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

- ☐ TLSv1.0
- ☐ TLSv1.1
- ☒ TLSv1.2

6. Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

- ☒ Log client IPs
 - ☐ Disable logging of X-Forwarded-For header only
 - ☐ Disable logging of both source IP and X-Forwarded-For header
- To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.



7. Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.

Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

- ☒ TLS terminated for the first time at infrastructure load balancer
- ☐ TLS terminated for the first time at HAProxy
- ☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|---|
| <ul style="list-style-type: none"> ◦ The Load Balancer is terminating TLS, and ◦ Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| <ul style="list-style-type: none"> ◦ The Load Balancer is configured to pass through the TLS handshake via TCP to the instances of HAProxy, and ◦ HAProxy instance count is > 0 | TLS terminated for the first time at HAProxy. | HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header. <div>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. </div> |
| <ul style="list-style-type: none"> ◦ The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | TLS terminated for the first time at the Gorouter. | The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header. <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p> <div>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. </div> |

For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).

8. To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

- ☒ HAProxy does not request client certificates.
- ☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- **HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- **HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.

⚠ warning: Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

9. To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- **Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- **Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- **Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

⚠ warning: Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client Certificate Validation** in the **Networking** pane.

10. In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.



Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

11. In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:

DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384 If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format.

Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.



Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

12. Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable

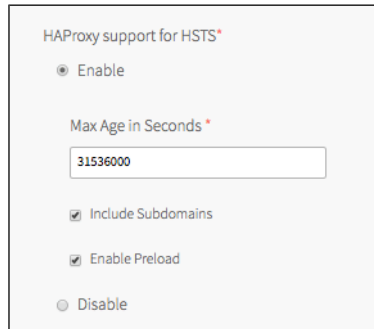
◦ Enable HAProxy forwarding of requests to Router over TLS

| If you want to: | Encrypt communication between HAProxy and the Gorouter |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

◦ Disable HAProxy forwarding of requests to Router over TLS

| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |


13. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field and complete



the following optional configuration steps:

- a. (Optional) **Enter a Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
- b. (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
- c. (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from HAProxy.

14. If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

15. (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

16. (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
17. (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
18. (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
19. By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#).

20. In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details.
 - a. If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
21. (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

0

500.

22. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router*


☒ Enable
 ☐ Disable

23. (Optional) To accommodate larger uploads over connections with high latency, increase the number of seconds in the **Router Timeout to Backends** field.
24. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

25. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
26. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

20

Load Balancer Healthy Threshold *

20

27. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

28. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.
29. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:
- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
 - **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.

HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.


HAProxy Trusted CIDRs

30. The **Loggregator Port** defaults to `443` if left blank. Enter a new value to override the default.


Container Network Interface Plugin*

☒ Silk


31. For **Container Network Interface Plugin**, ensure **Silk** is selected and review the following fields:

 **Note:** The **External** option exists to support NSX-T integration for vSphere deployments.

- (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to `1454`. Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses `10.255.0.0/16`.

 **warning:** The overlay network IP range must not conflict with any other IP addresses in your network.

- Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to `1`.
- For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to `100`.
- To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- For **DNS Servers**, enter `8.8.8.8` only if you have BOSH disabled. Otherwise, you cannot use this field to override the DNS servers used in containers.

 **Note:** If you do not want to configure your DNS servers with `8.8.8.8`, contact [Pivotal Support](#).

32. For **DNS Search Domains**, enter DNS search domains for your containers as a comma-separated list. DNS on your containers appends these names to its host names, to resolve them into full domain names.

DNS Search Domains

example.com, myapps.com

DNS search domains to be used in containers. A comma-separated list can be specified.

33. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is `120`. You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.
34. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:
- Select **Enable TCP Routing**.
 - For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. These are the same ports that you configured in the [Pre-Deployment Steps](#) of the *Enabling TCP Routing* topic.
 - To support multiple TCP routes, Pivotal recommends allocating multiple ports.

- To allocate a list of ports rather than a range:

1. Enter a single port in the **TCP Routing Ports** field.
2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time
☒ Enable TCP Routing

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

1024-1123

- c. For GCP, you also need to specify the name of a GCP TCP load balancer in the **LOAD BALANCER** column of TCP Router job of the **Resource Config** screen. You configure this later on in PAS. See the [Configure Load Balancers](#) section of this topic.

35. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) [↗](#) topic.

36. Click **Save**.

Step 7: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

☒ Enable Custom Buildpacks
☒ Allow SSH access to app containers
☒ Enable SSH when an app is created
☒ Enable the GrootFS container image plugin for Garden RunC
☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888

Docker Images Disk-Cleanup Scheduling on Cell VMs*

☐ Never clean up Cell disk-space
☐ Routinely clean up Cell disk-space
☒ Clean up disk-space once threshold is reached


Threshold of Disk-Used (MB) (min: 1) *

10240

2. The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more


information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.


3. The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
4. If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
5. If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.


6. To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting in HTTP Routing](#).

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

 **Warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

7. You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
8. Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
9. Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
10. Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.

 **Note:** In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

11. (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs*

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

- By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.
- Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
- You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is `60` seconds and the maximum configurable timeout is `600` seconds.
- Click **Save**.

Step 8: Configure Application Developer Controls

- Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *

Staging Timeout (Seconds) *

☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.
4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.
5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.



Note: If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of

seconds you specify in this field.

9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 9: Review Application Security Groups

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 10: Configure UAA

1. Select **UAA**.
2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

3. Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN`.



Note: The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN`.

4. If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
M
U
H
M

Change

SAML Service Provider Key Password

Secret

Password.

- For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
- (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line

Apps Manager Access Token Lifetime (in seconds) *

1209600

Apps Manager Refresh Token Lifetime (in seconds) *

1209600

Cloud Foundry CLI Access Token Lifetime (in seconds) *

7200

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

1209600

Global Login Session Max Timeout (in seconds) *

1800

Global Login Session Idle Timeout (in seconds) *

1800

Customize Username Label (on login page) *

Email

Customize Password Label (on login page) *

Password

Proxy IPs Regular Expression *


10\.\d{1,3}\.\d{1,3}\.\d{1,3}|192\.168\.\d{1,3}



Save

Interface (cf CLI) login access and refresh. Most deployments use the defaults.

- (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:
 - Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan

8. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
9. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Gorouter or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
10. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** For GCP installations, Pivotal recommends selecting **External** and using Google Cloud SQL.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#)  for help.

Internal Database Configuration

If you chose to not deploy a Google Cloud SQL database with Terraform, follow these steps.

When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane, which can be one of two options. See [Migrate to Internal Percona MySQL](#) for details.

1. Select **Internal MySQL**.

Choose the location of your UAA database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use AWS RDS)

2. Click **Save**.
3. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

If you chose to deploy a Google Cloud SQL database with Terraform, follow these steps.

1. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)

☒ External (preferred if, for example, you use AWS RDS)

Hostname *

TCP Port *

Username *


Password *

2. Complete the fields as follows:

- **Hostname:** Enter the value of `sql_db_ip` from your Terraform output.
- **TCP Port:** Enter `3306`.
- **User Account and Authentication database username:** Enter the value of `pas_sql_username` from your Terraform output.
- **User Account and Authentication database password:** Enter the value of `pas_sql_password` from your Terraform output.

3. Click **Save**.

Step 11: Configure CredHub

 **Note:** Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

1. Select **CredHub**.
2. Select **Internal** for your CredHub database. For GCP environments, Runtime CredHub has the following limitations:
 - If you choose **External**, Runtime CredHub does not work. See [CredHub Database Cannot be External on GCP](#).
 - Runtime CredHub only works if both the [system databases](#) and the CredHub database are set to **Internal**.
3. Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys

Name *

Name of the encryption key.

Provider*


Internal

Key *


Secret

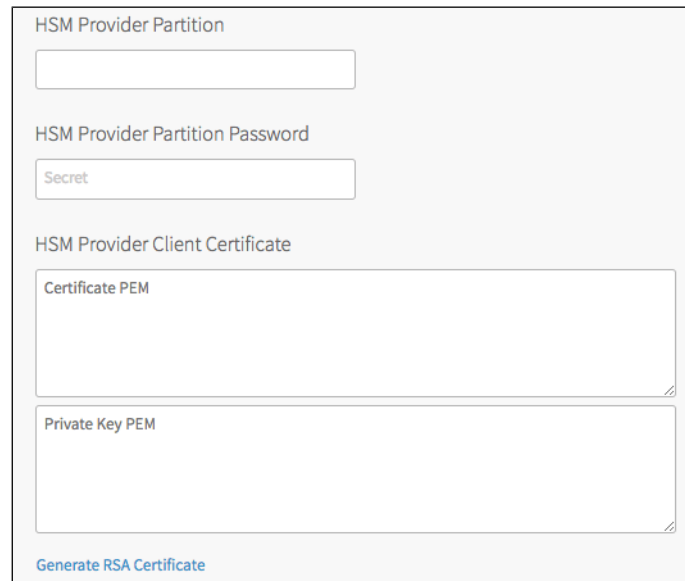
☐ Primary

- **Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- **Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- **Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- **Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.

 **Note:** For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

4. (Optional) To configure CredHub to use an HSM, complete the following fields:

- **HSM Provider Partition.** This is the name of the HSM provider partition.
- **HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- **HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#)  in the



Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

5. If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.
6. Click **Save**.
7. Select the **Resource Config** pane.
8. Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.
9. Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).

Step 12: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *


2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.


3. Click **Save**.


Step 13: Configure System Databases


You can configure PAS to use Google Cloud SQL for the databases required by PAS.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. Contact Pivotal Support for help. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration


 **Note:** For GCP installations, Pivotal recommends selecting **External** and using Google Cloud SQL. Only use internal MySQL for non-production or test installations on GCP.

 **Note:** For Runtime CredHub to work, you must use internal MySQL. See [CredHub Database Cannot be External on GCP](#).

 **Note:** Follow these steps if you did not modify your Terraform variables file to deploy an Google CloudSQL instance.

If you want to use internal databases for your deployment, perform the following steps:

1. Select **Databases**.
2. Select one of the **Internal Databases** options:
 - **Internal Databases - MySQL - Percona XtraDB Cluster** uses [Percona Server](#) with TLS encryption between server cluster nodes.
 - **Internal Databases - MySQL - MariaDB Galera Cluster** uses [MariaDB](#) with cluster nodes communicating over plaintext.

 **warning:** Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)


Save

3. Click **Save**.

Then proceed to [Step 14: \(Optional\) Configure Internal MySQL](#) to configure high availability for your internal MySQL databases.

External Database Configuration


 **Note:** If you use external MySQL, you cannot use Runtime CredHub. See [CredHub Database Cannot be External on GCP](#).

 **Note:** Follow these steps if you modified your Terraform variables file to deploy an Google CloudSQL instance.

Pivotal recommends using an external database such as Google Cloud SQL for high availability reasons.

On GCP, you can use Google Cloud SQL and use the automated backup and high availability replica features.

 **Note:** To configure an external database for UAA, see the *External Database Configuration* section of [Configure UAA](#).

 **warning:** Protect whichever database you use in your deployment with a password.

To specify your PAS databases, perform the following steps:

1. Select the **External Databases** option.
2. Complete the following fields:
 - **Hostname:** Enter the value of `sql_db_ip` from your Terraform output.
 - **TCP Port:** Enter `3306`.
 - For the username and password field for each relational database, enter the values of `pas_sql_username` and `pas_sql_password` from your

Place the databases used by Elastic Runtime components.

Choose the location of your system databases *

☐ Internal Databases - MySQL (preferred for complete high-availability)

☒ External Databases (preferred if, for example, you use AWS RDS)

Hostname *

35[REDACTED]

TCP Port *

3306

App Usage Service Database Username *

v[REDACTED]

App Usage Service Database Password *

[Change](#)

Autoscaling Service Database Username *

VA[REDACTED]

Autoscaling Service Database Password *

[Change](#)

Cloud Controller Database Username *

IA[REDACTED]


Cloud Controller Database Password *

[Change](#)

Terraform output.

3. Click **Save**.

Step 14: (Optional) Configure Internal MySQL

 **Note:** You only need to configure this section if you have selected one of the **Internal Databases - MySQL** options in the **Databases** section.


To use internal MySQL in High Availability configuration, you define a load balancer rule that lets PAS components send queries a single hostname backed by two redundant proxies. Each proxy then directs query traffic to three MySQL server nodes.

1. Allocate an internal load balancer rule to balance traffic between two static IP addresses. The static IP addresses cannot be within the range that you have reserved for PAS.

The load balancer rule is separate from the software provided by Pivotal, and you need to define it within your infrastructure.

- **Make your idle time out long enough to not interrupt long-running queries.** When queries take a long time, the load balancer can time out and interrupt the query.
For example, [AWS's Elastic Load Balancer](#) has a default idle timeout of 60 seconds, so queries that take longer than this duration sever the MySQL connection and return an error.
- **Configure a healthcheck or monitor, using TCP against port 1936.** This defaults to TCP port `1936`, to maintain backwards compatibility with previous releases. This port is not configurable. Unauthenticated healthchecks against port 3306 may cause the service to become unavailable and require manual intervention to fix.
- **Configure the load balancer to route traffic for TCP port 3306 to the IPs of all proxy instances on TCP port 3306.**

- Record the hostname of the load balancer rule and the two static IP addresses.

 **warning:** You must configure a load balancer to achieve complete high availability.

- From the PAS tile in Ops Manager, Select **Internal MySQL**.
- In the **MySQL Proxy IPs** field, enter the static IP addresses used by the internal MySQL load balancer rule.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.


A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.

The automated backups functionality works with any S3-compatible file store that can receive your backup files.

MySQL Proxy IPs

MySQL Service Hostname

- For **MySQL Service Hostname**, enter the IP address or hostname for your load balancer. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.
- In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
- In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.
- (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
- To prohibit the creation of command line history files on the MySQL nodes, disable the **Allow Command History** checkbox.
- To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

- For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the default value is 10 seconds.

Replication canary time period *

Replication canary read delay *

E-mail address (required) *

☒ Allow Command History

Cluster Probe Timeout

11. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.
12. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.
 - a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.

Server Activity Logging *

☐ Disable server activity logging

☒ Enable server activity logging

Event types *

Load Balancer Healthy Threshold *

Load Balancer Unhealthy Threshold *

Save


13. Enter values for the following fields:
 - **Load Balancer Healthy Threshold:** Specifies the amount of time, in seconds, to wait until declaring the MySQL Proxy instance started. This allows an external load balancer time to register the instance as healthy.
 - **Load Balancer Unhealthy Threshold:** Specifies the amount of time, in seconds, that the MySQL Proxy continues to accept connections before shutting down. During this period, the Healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.
14. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.
15. Click **Save**.

For more information on how to monitor the node health of your MySQL Proxy instances, see [Using the MySQL Proxy](#).

Step 15: Configure File Storage

When configuring file storage for the Cloud Controller in PAS, you can select one of the following:

- Internal WebDAV filestore
- External S3-compatible or Ceph-compatible filestore
- External Google Cloud Storage with Access Key and Secret Key
- External Google Cloud Storage with Service Account
- External Azure Cloud Storage

 **Note:** Use one of the Google Cloud Storage options if you added `create_gcs_buckets = true` to your `terraform.tfvars` file.

For production-level PCF deployments on GCP, Pivotal recommends selecting **External Google Cloud Storage** to minimize downtime. For more information about production-level PCF deployments on GCP, see the [Reference Architecture for Pivotal Cloud Foundry on GCP](#).

For additional factors to consider when selecting file storage, see the [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#) topic.

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External Google Cloud Storage

PAS can use Google Cloud Storage (GCS) as its external filestore by using either a GCP interoperable storage access key or your GCS Service Account. See below for how to configure each option.

External Google Cloud Storage with Access Key and Secret Key

1. Select the **External Google Cloud Storage with Access Key and Secret Key** option

This section determines where you would like to place your Application Service Cloud Controller's file storage.

Configure your Cloud Controller's filesystem*

- ☐ Internal WebDAV (provided by Application Service)
- ☐ External S3-Compatible File Store (if you want to use a service like S3 or Ceph)
- ☒ External Google Cloud Storage with Access Key and Secret Key

Access Key *

Secret Key *

Buildpacks Bucket Name *

Bucket for storing app buildpacks.

Droplets Bucket Name *

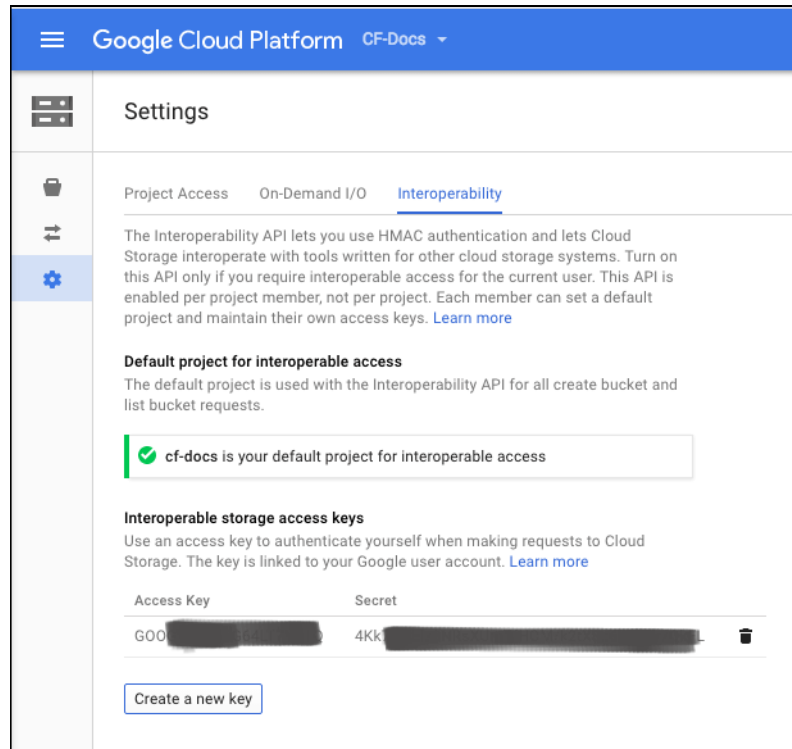
Packages Bucket Name *

Resources Bucket Name *

- ☐ External Google Cloud Storage with Service Account
- ☐ External Azure Storage

2. Enter values for **Access Key** and **Secret Key**. To obtain the values for these fields:

- a. In the GCP Console, navigate to the **Storage** tab, then click **Settings**.
- b. Click **Interoperability**.
- c. If necessary, click **Enable interoperability access**. If interoperability access is already enabled, confirm that the default project matches the project where you are installing PCF.



- d. Click **Create a new key**.
- e. Copy and paste the generated values into the corresponding PAS fields. PCF uses these values for authentication when connecting to Google Cloud Storage.
- f. Enter the names of the storage buckets you created in [Deploying Ops Manager on GCP Using Terraform](#):
 - **Buildpacks Bucket Name:** Enter the value of `buildpacks_bucket` from your Terraform output.
 - **Droplets Bucket Name:** Enter the value of `droplets_bucket` from your Terraform output.
 - **Resources Bucket Name:** Enter the value of `packages_bucket` from your Terraform output.
 - **Packages Bucket Name:** Enter the value of `resources_bucket` from your Terraform output.
- g. Click **Save**.

External Google Cloud Storage with Service Account

1. Select the **External Google Cloud Storage with Service Account** option

Configure your Cloud Controller's filesystem*

☐ Internal WebDAV (provided by Application Service)
☐ External S3-Compatible File Store (if you want to use a service like S3 or Ceph)
☐ External Google Cloud Storage with Access Key and Secret Key
☒ External Google Cloud Storage with Service Account

GCP Project ID *

GCP Service Account Email *

 Your Google Cloud Platform Service Account Email.

GCP Service Account Key JSON *

Buildpacks Bucket Name *

- For **GCP Project ID** enter the Project ID on your GCP Console that you want to use for your PAS file storage.
- For **GCP Service Account Email** enter the email address associated with your GCP account.
- For **GCP Service Account JSON** enter the account key that you use to access the specified GCP project, in JSON format.
- Enter the names of the storage buckets you created in [Deploying Ops Manager on GCP Using Terraform](#):
 - **Buildpacks Bucket Name**: Enter the value of `buildpacks_bucket` from your Terraform output.
 - **Droplets Bucket Name**: Enter the value of `droplets_bucket` from your Terraform output.
 - **Resources Bucket Name**: Enter the value of `packages_bucket` from your Terraform output.
 - **Packages Bucket Name**: Enter the value of `resources_bucket` from your Terraform output.
- Click **Save**.

Other IaaS Storage Options

[Azure Storage](#) and [External S3-Compatible File Storage](#) are also available as file storage options, but Pivotal does not recommend these for a typical PCF on GCP installation.

Step 16: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

Note: The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

- In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

- ☒ No
☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging

☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration

Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.



Note: The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.



Note: Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 17: (Optional) Customize Apps Manager

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

Add

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑️
- ▶ Docs 🗑️
- ▶ Tools 🗑️

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

4. Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
5. Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
6. Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
7. Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
8. The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
9. The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 18: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

Note: If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 19: (Optional) Configure App Autoscaler

To use App Autoscaler, you must create an instance of the service and bind it to an app. To create an instance of App Autoscaler and bind it to an app, see [Set Up App Autoscaler](#) in the *Scaling an Application Using App Autoscaler* topic.

- Click **App Autoscaler**.

Configure the App Autoscaler

Autoscaler Instance Count (min: 1) *

Autoscaler API Instance Count (min: 1) *

Metric Collection Interval (min: 60, max: 3600) (min: 60, max: 3600) *

Scaling Interval (min: 15, max: 120) (min: 15, max: 120) *

☐ Verbose Logging

☐ Disable API Connection Pooling

☒ Enable Notifications

- Review the following settings:

- Autoscaler Instance Count:** How many instances of the App Autoscaler service you want to deploy. The default value is `3`. For high availability, set this number to `3` or higher. You should set the instance count to an odd number to avoid split-brain scenarios during leadership elections. Larger environments may require more instances than the default number.
- Autoscaler API Instance Count:** How many instances of the App Autoscaler API you want to deploy. The default value is `1`. Larger environments may require more instances than the default number.
- Metric Collection Interval:** How many seconds of data collection you want App Autoscaler to evaluate when making scaling decisions. The minimum interval is 60 seconds, and the maximum interval is 3600 seconds. The default value is `120`. Increase this number if the metrics you use in your scaling rules are emitted less frequently than the existing Metric Collection Interval.
- Scaling Interval:** How frequently App Autoscaler evaluates an app for scaling. The minimum interval is 15 seconds, and the maximum interval is 120 seconds. The default value is `35`.
- Verbose Logging** (checkbox): Enables verbose logging for App Autoscaler. Verbose logging is disabled by default. Select this checkbox to see more detailed logs. Verbose logs show specific reasons why App Autoscaler scaled the app, including information about minimum and maximum instance limits, App Autoscaler's status. For more information about App Autoscaler logs, see [App Autoscaler Events and Notifications](#).
- Disable API Connection Pooling:** API connection pooling increases performance by reducing the cost associated with establishing new connections. If you do not want to keep connections open for reuse, select this option.

3. Click **Save**.

Step 20: Configure Cloud Controller

1. Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
 ☒ Disable

Save

2. Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

3. CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

4. Click **Save**.

Step 21: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

1. Select **Smoke Tests**.
2. If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

- ☐ Temporary space within the system organization (This is deleted after smoke tests finish.)
- ☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.

Step 22: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

Note: Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.

Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.

Whitelist for non-RFC-1918 Private Networks *

allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.

CF CLI Connection Timeout

15

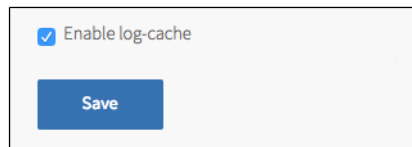
2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PASTopic*.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

⚠ warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 23: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

💡 Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.

- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

💡 Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.


- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.
- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

Step 24: Configure Load Balancers


1. Click **Resource Config**.

- Under the **LOAD BALANCERS** column of the **Router** row, enter a comma-delimited list consisting of the values of `ws_router_pool` and `http_lb_backend_name` from your Terraform output. For example, `tcp:pcf-cf-ws,http:pcf-httpslb`. These are the names of the TCP WebSockets and HTTP(S) load balancers for your deployment.

 **Note:** Do not add a space between key/value pairs in the `LOAD BALANCER` field or it will fail.

 **Note:** If you are using HAProxy in your deployment, then enter the above load balancer values in the `LOAD BALANCERS` field of the **HAProxy** row instead of the **Router** row. For a high availability configuration, scale up the HAProxy job to more than one instance.


- If you have enabled TCP routing in the **Networking** pane, add the value of `tcp_router_pool` from your Terraform output, prepended with `tcp:`, to the **LOAD BALANCERS** column of the **TCP Router** row. For example, `tcp:pcf-cf-tcp`.
- Enter the name of your SSH load balancer depending on which release you are using.
 - PAS:** Under the **LOAD BALANCERS** column of the **Diego Brain** row, enter the value of `ssh_router_pool` from your Terraform output, prepended with `tcp:`. For example, `tcp:MY-PCF-ssh-proxy`.
 - Small Footprint Runtime:** Under the **LOAD BALANCERS** column of the **Control** row, enter the value of `ssh_router_pool` from your Terraform output, prepended with `tcp:`.
- Verify that the **Internet Connected** checkbox for every job is checked. The terraform templates do not provision a Network Address Translation (NAT) box for Internet connectivity to your VMs so instead they will be provided with ephemeral public IP addresses to allow the jobs to reach the Internet.

 **Note:** If you want to provision a Network Address Translation (NAT) box to provide Internet connectivity to your VMs instead of providing them with public IP addresses, deselect the **Internet Connected** checkboxes. For more information about using NAT in GCP, see the [GCP documentation](#).

- Click **Save**.

Step 25: (Optional) Scale Down and Disable Resources

 **Note:** The **Resource Config** pane has fewer VMs if you are installing the [Small Footprint Runtime](#).

 **Note:** The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to `3` instances and scale the **Control** VM to `2` instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by navigating to the **Resource Config** section and using the dropdowns under **Instances** for each job.

By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding system-provided resources in Ops Manager to reduce costs and administrative overhead.

To disable specific VMs in Ops Manager, do the following:

- Click **Resource Config**.
- If you configured PAS to use an external S3-compatible filestore, enter `0` in **Instances** in the **File Storage** field.
- If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:
 - MySQL Proxy:** Enter `0` in **Instances**.
 - MySQL Server:** Enter `0` in **Instances**.
 - MySQL Monitor:** Enter `0` in **Instances**.
- If you disabled TCP routing, enter `0` **Instances** in the **TCP Router** field.
- If you are not using HAProxy, enter `0` **Instances** in the **HAProxy** field.

6. Click **Save**.

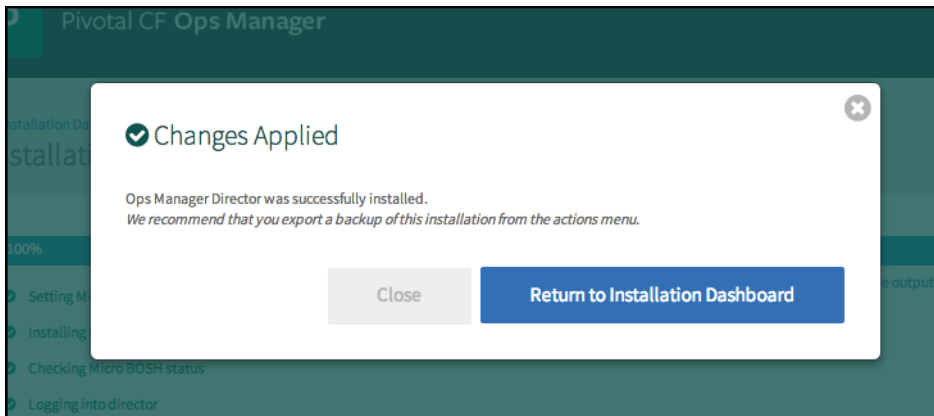
Step 26: Download Stemcell

This step is only required if your Ops Manager does not already have the stemcell version required by PAS. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

1. Open the [Stemcell product page](#) in the Pivotal Network. *Note, you may have to log in.*
2. Download the appropriate stemcell version targeted for your IaaS.
3. Navigate to **Stemcell Library** in the **Installation Dashboard**.
4. Click **Import Stemcell** to import the downloaded stemcell `.tgz` file.
5. When prompted, enable the Ops Manager product checkbox to stage your stemcell.
6. Click **Apply Stemcell to Products**.

Step 27: Complete the PAS Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**. The install process generally requires a minimum of 90 minutes to complete. The image shows the Changes Applied window that displays when the installation process successfully completes.



Configuring a Shared VPC on GCP

Page last updated:

This guide describes the preparation steps required to configure and integrate a shared Virtual Private Cloud (VPC) on Google Cloud Platform (GCP) with Pivotal Cloud Foundry (PCF).

GCP Shared VPC, formerly known as Google Cross-Project Networking (XPN), enables you to assign GCP resources to individual projects within an organization but allows communication and shared services between projects. For more information about shared VPCs, see [Shared VPC Overview](#) in the GCP documentation.

Prerequisites

To configure a shared VPC, you must assign your project to a Cloud Organization. Confirm that you have a Cloud Organization associated with your GCP account using one of the following methods:

- **GCP Console:** From <https://console.cloud.google.com>, click the **Organization** dropdown at the top of the page to display all organizations you belong to.
- **gcloud Command Line Interface (CLI):** From the command line, run `gcloud organizations list` to display all organizations you belong to. See [gcloud Overview](#) in the Google documentation to install the gcloud CLI.

For more information, see [Creating and Managing Organizations](#) in the GCP documentation. If you do not have a Cloud Organization, contact GCP support.

Step 1: Provision the Shared VPC

Follow the [Enabling a shared VPC host project](#) procedure in the GCP documentation. This procedure requires shared VPC admin permissions.

Step 2: Create a Shared VPC Network

Use the procedures in the [Preparing to Deploy Ops Manager on GCP Manually](#) topic to create a new network with firewall rules. Do the following:

- [Step 3: Create a GCP Network with Subnet](#)
- [Step 5: Create Firewall Rules for the Network](#)

Step 3: Connect the Shared VPC to Ops Manager

You can use the [GCP console](#) or the gcloud CLI to connect the shared VPC host project with Ops Manager.

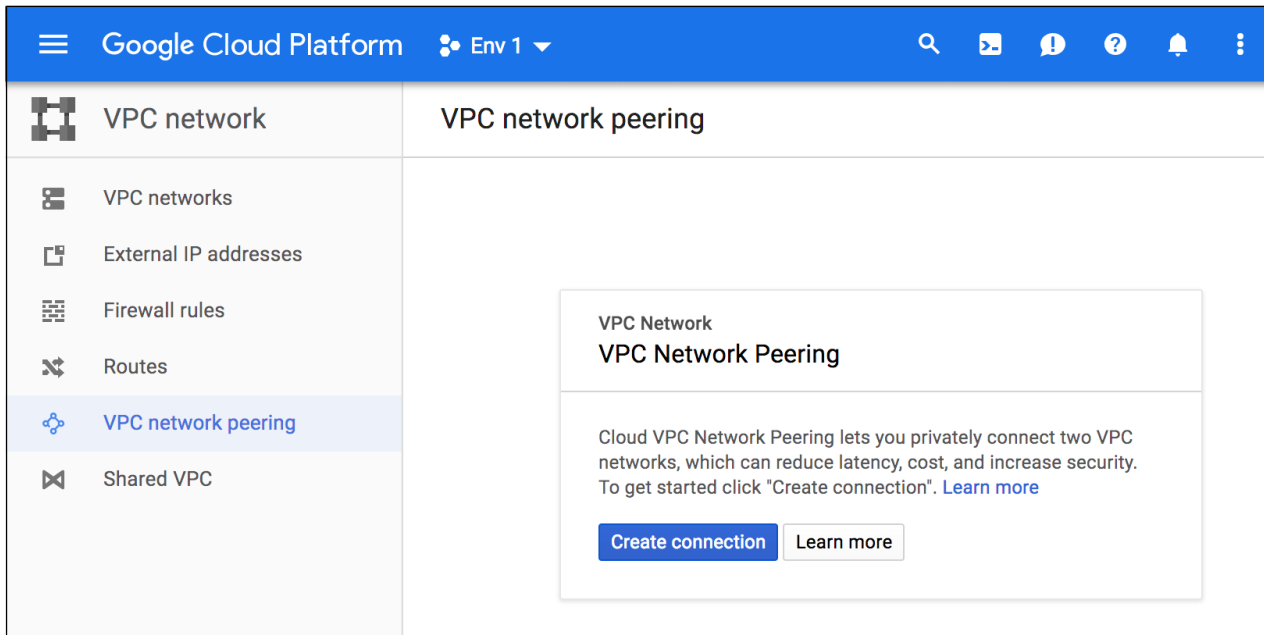
For more information, see [VPC Network Peering](#) in the GCP documentation.

⚠ warning: VPC Network Peering is currently in beta and intended for evaluation and test purposes only.

Set Up VPC Network Peering with GCP Console

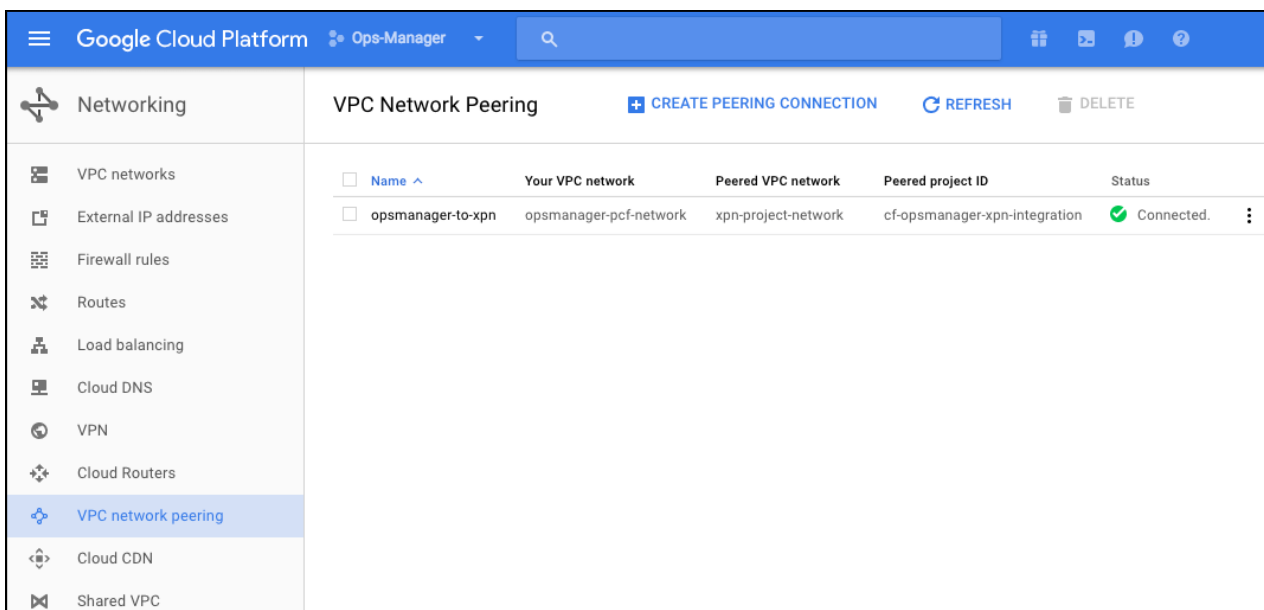
To set up VPC network peering with the GCP console, do the following:

1. From the GCP console, click **Networking**, then **VPC network peering**.



2. Click **Create Connection**.

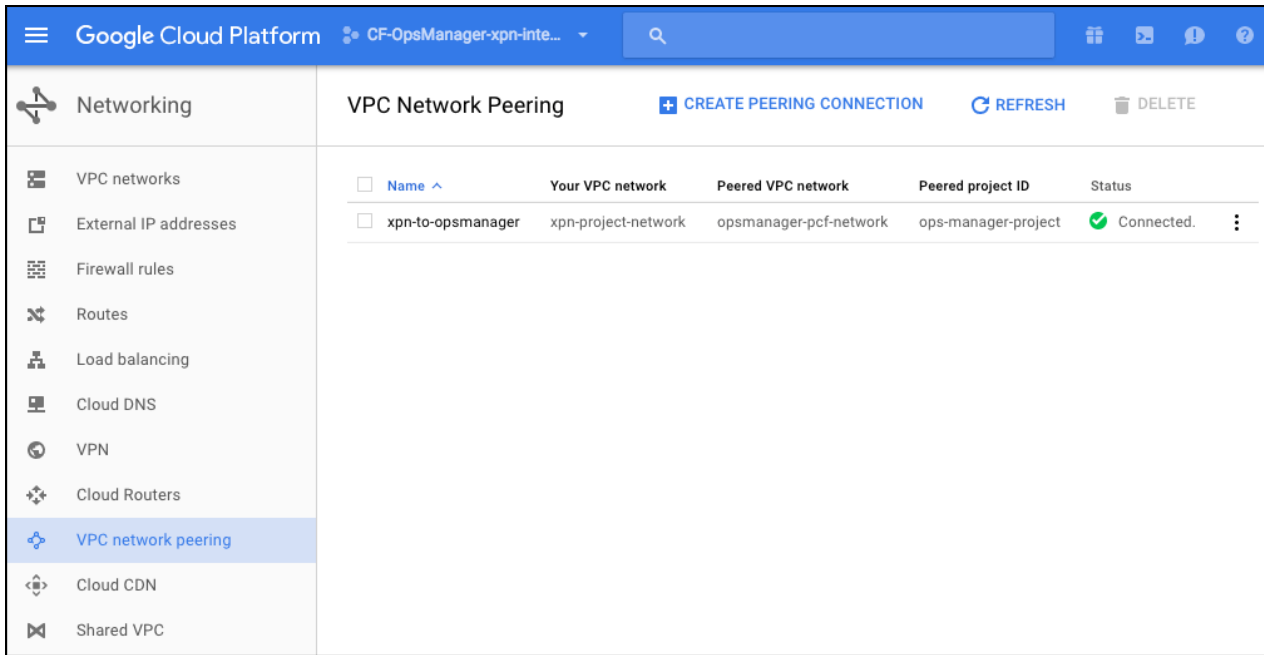
3. Enter a name for the network connection from the Ops Manager project to the new shared network, such as `opsmanager-to-xpn`.



4. Click **Save**.

5. Click **Create Connection**.

6. Enter a name for the network connection from the new shared network to the Ops Manager project, such as `xpn-to-opsmanager`.



7. Click **Save**.

Set Up VPC Network Peering with gcloud CLI

To set up VPC network peering with the gcloud CLI, do the following:

1. Enter the following command, replacing `OPSMANAGER-PROJECT` with the name of the project that contains your Ops Manager installation:

```
$ gcloud config set project OPSMANAGER-PROJECT
```

2. Enter the following command to create a connection from the Ops Manager project to the new shared VPC project:

```
$ gcloud beta compute networks peerings create OPSMANAGER-TO-VPC \
  --network OPSMANAGER-NETWORK \
  --peer-project VPC-HOST-PROJECT \
  --peer-network VPC-NETWORK \
  --auto-create-routes
```

Replace the following text in the command above:

- `OPSMANAGER-TO-VPC` : Choose a name for the connection, such as `om-to-vpc`.
- `OPSMANAGER-NETWORK` : Enter the name of the network assigned to the Ops Manager project in GCP, such as `my-om-project`.
- `VPC-HOST-PROJECT` : Enter the name you gave the shared VPC project in [Step 1: Provision the Shared VPC](#).
- `VPC-NETWORK` : Enter the name of the network you gave the shared VPC project in [Step 2: Create Shared VPC Networks](#).

3. Enter the following command, replacing `VPC-HOST-PROJECT` with the new shared VPC project you created in [Step 1: Provision the Shared VPC](#):

```
$ gcloud config set project VPC-HOST-PROJECT
```

4. Enter the following command to create a connection from the new shared VPC project to the Ops Manager project:

```
$ gcloud beta compute networks peerings create VPC-TO-OPSMANAGER \
  --network VPC-NETWORK \
  --peer-project OPSMANAGER-PROJECT \
  --peer-network OPSMANAGER-NETWORK \
  --auto-create-routes
```

Replace the following text and run the following command:

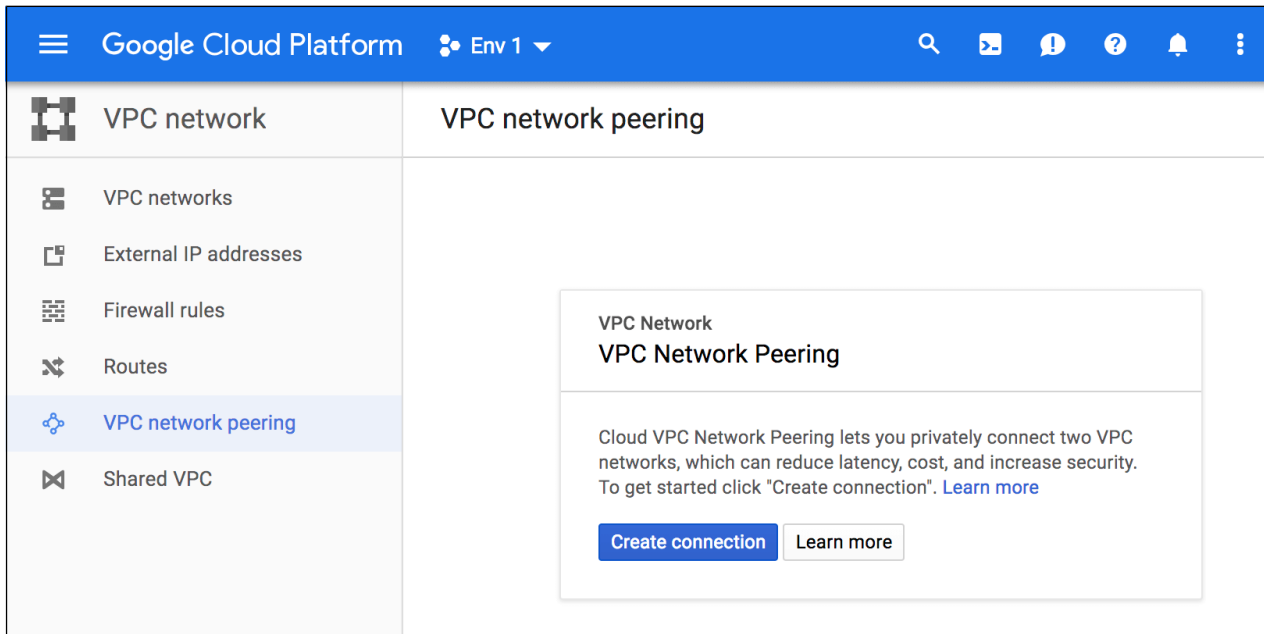
- `VPC-TO-OPSMANAGER` : Choose a name for the connection, such as `vpc-to-om`.
- `VPC-NETWORK` : Enter the name of the network you gave the shared VPC project in [Step 2: Create Shared VPC Networks](#).
- `OPSMANAGER-PROJECT` : Enter the name of the project that contains your Ops Manager installation.

- `OPSMANAGER-NETWORK` : Enter the name of the network assigned to the Ops Manager project in GCP.

Step 4: Verify the Shared VPC Configuration

After configuring a shared VPC, use the following procedure to verify that the shared VPC host project VM appears in the Ops Manager project.

1. From <https://console.cloud.google.com>, select the Ops Manager project from the drop-down menu at the top of the page.
2. Click **Networking**, then **VPC networks**.



3. Confirm that the shared VPC network name appears in the **Subnets** list.
4. Confirm that the shared VPC network **IP address ranges** match what you set for the new VPC project in [Step 2: Create a Shared VPC Network](#).

Deleting PCF from GCP

Page last updated:

When you deploy [Pivotal Cloud Foundry](#) (PCF) to Google Cloud Platform (GCP), you provision a set of resources. This topic describes how to delete the resources associated with a PCF deployment.

You can delete the resources in one of two ways:

- If you created a separate project for your PCF deployment, perform the procedure in the [Delete the Project](#) delete the project.
- If the project that contains your PCF deployment also contains other resources that you want to preserve, perform the procedure in the [Delete PCF Resources](#) section.

Delete the Project

Perform the following steps to delete the project for your PCF deployment:

1. Navigate to the GCP Console Dashboard.
2. Under your **Project**, click **Manage project settings**.
3. Click **DELETE PROJECT**.
4. Enter your project ID and click **SHUT DOWN** to confirm.

Delete PCF Resources

Perform the following steps to delete the resources associated with your PCF deployment:

1. Navigate to the GCP Console Dashboard.
2. Click the upper left icon and select **Networking**.
3. Click **Load balancing**.
4. Perform the following steps for all load balancers associated with your PCF deployment:
 - a. Click the trashcan icon next to the load balancer.
 - b. In the next dialog, select any **health checks** and **backend services** associated with the load balancer.
 - c. Click **DELETE LOAD BALANCER AND THE SELECTED RESOURCES**.
5. Click the upper left icon and select **Compute Engine**.
6. Perform the following steps for **VM instances**, **Instance groups**, and **Disks**:
 - a. Select the checkbox next to the PCF resource.
 - b. When all PCF resources are selected, click **DELETE** in the upper right.
 - c. Click **DELETE** to confirm.
7. Click the upper left icon and select **Networking**.
8. Click **External IP addresses**.
9. Select all external IP addresses associated with your PCF deployment, and click **RELEASE STATIC ADDRESS**.
10. Click on **Networks**, and perform the following steps for any networks you created for PCF:
 - a. Click the name of the network.
 - b. Click **DELETE NETWORK**.
 - c. Click **DELETE** to confirm.
11. Click the upper left icon and select **IAM & Admin**.
12. Click the trashcan icon next to the `bosh` service account you created for PCF and click **REMOVE**.

13. Navigate to **Compute Engine > Metadata > SSH Keys**. Delete the `vcap` SSH key that you created for the project.

Troubleshooting PCF on GCP

Page last updated:

This topic describes how to troubleshoot known issues when deploying Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP).

Problems Connecting with Single Sign-On (SSO)

Users may be unable to connect to applications running on PCF using SSO.

Explanation

SSO does not support multi-subnets.

Solution

Ensure that you have configured only one subnet. See [Preparing to Deploy Ops Manager on GCP Manually](#).

Uploading PAS Tile Causes Ops Manager Rails Application Crash

Uploading the Pivotal Application Service (PAS) tile causes the Ops Manager Rails application to crash.

Explanation

In compressed format, the PAS tile is 5 GB in size. However, when uncompressed during installation, the PAS tile requires additional disk space that can exhaust the space allocated to the boot disk.

Solution

Ensure that the boot disk is allocated at least 50 GB of space. See *Step 3: Create the Ops Manager VM Instance* in [Deploying Ops Manager on GCP Manually](#).

PAS Deployment Fails - MySQL Monitor replication-canary Job

During installation of the PAS tile, the replication-canary job fails to start. The error reported in the installation log resembles the following:

```
Started updating job mysql_monitor > mysql_monitor/0
(48e7ec82-3cdf-41af-9d0f-90d1f12683c8) (canary). Failed: 'mysql_monitor/0
(48e7ec82-3cdf-41af-9d0f-90d1f12683c8)' is not running after update.
Review logs for failed jobs: replication-canary (00:05:13)

Error 400007: 'mysql_monitor/0 (48e7ec82-3cdf-41af-9d0f-90d1f12683c8)'
is not running after update.
Review logs for failed jobs: replication-canary
```

Explanation

This error can appear as a result of incorrect configuration of network traffic and missed communication between the Gorouter and a load balancer.

Solution

1. Make sure you have selected the **Forward SSL to PAS Router** option in your [PAS Network Configuration](#).
 2. Verify that you have configured the firewall rules properly and that TCP ports `80`, `443`, `2222`, and `8080` are accessible on your GCP load balancers. See *Step 5: Create Firewall Rules for the Network* in [Preparing to Deploy Ops Manager on GCP Manually](#).
 3. Verify that you have configured the proper SSL certificates on your HTTP(S) load balancer in GCP. See *Step 8: Create HTTP Load Balancer* in [Preparing to Deploy Ops Manager on GCP Manually](#).
 4. If necessary, re-upload a new certificate and update any required SSL Certificate and SSH Key fields in your [PAS network configuration](#).
-

Insufficient External Database Permissions

Upgrade issues can be caused when the external database user used for the network policy DB is given insufficient permissions. To avoid this upgrade issue, ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.

Upgrading BOSH Director on GCP

This topic describes how to upgrade BOSH Director for Pivotal Cloud Foundry (PCF) on Google Cloud Platform (GCP).

Complete the tasks in this topic as part of the Ops Manager upgrade process. For more information, see [Upgrading Pivotal Cloud Foundry](#).

Overview

In this procedure, you create an Ops Manager VM instance to host the upgraded version of Ops Manager. Then, to complete the Ops Manager upgrade, you export your existing Ops Manager installation onto this new VM.

To create an Ops Manager VM instance, do the following tasks:

1. Locate the Ops Manager installation file. See [Locate the Pivotal Ops Manager Installation File](#).
2. Create a private VM image. See [Create a Private VM Image](#).
3. Create the Ops Manager VM. See [Create the Ops Manager VM Instance](#).

Prerequisites

To complete the Ops Manager upgrade, you must have your Ops Manager decryption passphrase. You defined this decryption passphrase during the initial installation of Ops Manager.

Locate the Pivotal Ops Manager Installation File

The Ops Manager installation file includes a filepath to the Ops Manager image. You use this image file to create a private VM image for the new Ops Manager VM.

To locate the Ops Manager installation file, do the following:

1. Log in to the [Pivotal Network](#), and click on **Pivotal Cloud Foundry Operations Manager**.
2. From the **Releases** drop-down, select the release for your upgrade.
3. Select one of the following download files:
 - **Pivotal Cloud Foundry Ops Manager for GCP**
 - **Pivotal Cloud Foundry Ops Manager YAML for GCP** When you click on the download link, your browser downloads or opens the `OpsManager_version_onGCP.pdf` or `OpsManager_version_onGCP.yml` file.

These documents provide the GCP location of the Ops Manager `.tar.gz` installation file based on the geographic location of your installation.

4. Copy the filepath string of the Ops Manager image based on your existing deployment location.

Create a Private VM Image

Create a private VM image to use when you create the new Ops Manager VM.

To create a private VM image, do the following:

1. Log in to the [GCP Console](#).
2. In the left navigation panel, click **Compute Engine**, and select **Images**.
3. Click **Create Image**.
4. Complete the following fields:

- **Name:** Enter a name that matches the naming convention of your existing Ops Manager image files.
- **Encryption:** Leave **Automatic (recommended)** selected.
- **Source:** Choose **Cloud Storage file**.
- **Cloud Storage file:** Paste in the Google Cloud Storage filepath you copied from the PDF or YAML file in the previous task.

Create an image

Name [?]
om-pcf

Family (Optional) [?]

Description (Optional)

Encryption [?]
Automatic (recommended)

Source [?]
Cloud Storage file

Cloud Storage file [?]
☒ r-images/pivotal-ops-manager-20160916101000-010010.tar.gz

Equivalent [REST](#) or [command line](#)

5. Click **Create**. The file may take a few minutes to import.

Create the Ops Manager VM Instance

Create an Ops Manager VM instance to host the new version of Ops Manager.

To create an Ops Manager VM instance, do the following:

1. Select the checkbox for the image that you created above.

| Images | | | | |
|---|-------|------------|--------|---------------------------|
| + CREATE IMAGE REFRESH + CREATE INSTANCE DEPRECATE DELETE | | | | |
| <input type="text" value="Filter by label or name"/> <input type="button" value="Columns"/> <input type="button" value="Labels"/> | | | | |
| Name | Size | Created by | Family | Creation time |
| <input checked="" type="checkbox"/> om-pcf | 50 GB | CF-Docs | | Nov 22, 2016, 10:07:54 AM |

2. Click **Create Instance**.
3. In the **Create an instance form**, complete the following fields:
 - **Name:** Enter a name that matches the naming conventions of your existing deployment.
 - **Zone:** Choose a zone from the region of your existing deployment.
 - **Machine type:** Click **Customize** to manually configure the vCPU and memory. An Ops Manager VM instance requires the following minimum specifications:

| Machine Spec | Minimum Value |
|--------------|---------------|
| CPU | 2 vCPUs |
| Memory | 8 GB |

- **Boot disk:** Click **Change**, then perform the following steps:
 - Click **Custom images** if it is not already selected.
 - Select the **Boot disk type**. If you have an Ops Manager environment with high performance needs, select **SSD**. As an example,

environments used to [develop PCF tiles](#) may benefit from a higher performing Ops Manager VM boot disk. For most environments, however, you can select **Standard**.

- Set the **Size (GB)** of the boot disk to the minimum or higher.

| Machine Spec | Minimum Value |
|--------------|---------------|
| Boot disk | 100 GB |

- Select the Ops Manager image you created in the previous step if it is not already selected.

Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk.

OS images Application images **Custom images** Snapshots

Existing disks

☒ **om-pcf**
Created from CF-Docs on Oct 18, 2016, 11:38:02 AM

- Click **Select** to save.

- Under **Identity and API access**, choose the **Service account** you created when you initially installed Pivotal Cloud Foundry. See [Set up an IAM Service Account](#).
- **Allow HTTP traffic**: Only select this checkbox if you selected it in your original Ops Manager VM configuration.
- **Allow HTTPS traffic**: Only select this checkbox if you selected it in your original Ops Manager VM configuration.

Name ⓘ

Zone ⓘ

Machine type

Cores ⓘ
 2 vCPU 1 - 64


Memory ⓘ
 8 GB 1.8 - 13

☐ Extend memory ⓘ

CPU platform ⓘ

GPUs ⓘ
[Choosing a machine type](#) ⓘ

Boot disk ⓘ



New 100 GB standard persistent disk
 Image
om-pcf

Change

Identity and API access ⓘ

Service account ⓘ

Access scopes ⓘ
 Use IAM roles with service accounts to control VM access [Learn more](#)

Firewall ⓘ
 Add tags and firewall rules to allow specific network traffic from the Internet
☐ Allow HTTP traffic
☐ Allow HTTPS traffic

Management, disks, networking, SSH keys ⓘ

You will be billed for this instance. [Learn more](#)

Create

Cancel

- **Networking:** Select the **Networking** tab, and perform the following steps:
 - For **Network** and **Subnetwork**, select the network and subnetwork you created when you initially deployed Pivotal Cloud Foundry. See [Create a GCP Network with Subnet](#) section of the *Preparing to Deploy Ops Manager on GCP Manually* topic.
 - For **Network tags**, enter any tags that you applied to your original Ops Manager. For example, if you used the `pcf-opsmanager` tag to apply the firewall rule you created in [Create Firewall Rules for the Network](#), then apply the same tag to this Ops Manager VM.
 - For **Internal IP**, select `Custom`. In the **Internal IP address** field, enter a spare address located within the reserved IP range [configured in your existing BOSH Director](#). Do not use `10.0.0.1`, which is configured for the Gateway.
 - For **External IP**, select **New static IP address...**. In the next form, enter a name for the static IP. For example, `om-public-ip`. Click **Reserve**. In the **External IP** drop-down, select the static IP address you just reserved.

Firewall ?
Add tags and firewall rules to allow specific network traffic from the Internet

☐ Allow HTTP traffic
☐ Allow HTTPS traffic

Management Disks **Networking** SSH Keys

Network ?
opsmgr

Subnetwork ?
opsmgr-subnet (10.0.0.0/20)

Network tags ? (Optional)
pcf-opsmanager

Internal IP ?
Custom

Internal IP address
10.0.0.4

External IP ?
Ephemeral
None
pbj-websockets-ip (10.0.0.1)
New static IP address...

[Less](#)

4. Click **Create** to deploy the new Ops Manager VM. This may take a few moments.
5. Navigate to your DNS provider, and modify the entry that points a fully qualified domain name (FQDN) to the Ops Manager VM. Replace the original Ops Manager static IP address with the public IP address of the new Ops Manager VM you created in a previous step.

Note: In order to set up Ops Manager authentication correctly, Pivotal recommends using a Fully Qualified Domain Name (FQDN) to access Ops Manager. Using an ephemeral IP address to access Ops Manager can cause authentication errors upon subsequent access.

Next Steps

After you complete this procedure, continue the upgrade instructions in [Upgrading Pivotal Cloud Foundry](#) topic.

Later on, if you need to SSH into the Ops Manager VM to perform diagnostic troubleshooting, see [SSH into Ops Manager](#).

Installing Pivotal Cloud Foundry on OpenStack

Page last updated:




This guide describes how to install Pivotal Cloud Foundry (PCF) on OpenStack with Ops Manager and Pivotal Application Service (PAS).

Overview

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter. For guidance on OpenStack service credential management, see [Open Stack Security Documents](#) below.



OpenStack Security Documents

These documents provide a general reference for OpenStack service credential management.

- [OpenStack credential configuration](#) 
- [OpenStack credential creation](#) 
- [OpenStack deployment configuration](#) 

Requirements

This section describes the requirements for installing PCF on OpenStack, including general requirements for installing PCF with Ops Manager and PAS as well as OpenStack requirements.

 **Note:** You can install PCF on OpenStack with the Pivotal Application Service (PAS) runtime. The Pivotal Container Service (PKS) runtime is not supported for OpenStack. For more information about PAS, see [PAS Concepts](#). For more information about PKS, see [Pivotal Container Service \(PKS\)](#) .

General Requirements

The following are general requirements for deploying and managing a PCF deployment with Ops Manager and Pivotal Application Service (PAS):

- A wildcard DNS record that points to your router or load balancer. Alternatively, you can use a service such as xip.io. For example, `203.0.113.0.xip.io`.
 - PAS gives each application its own hostname in your app domain.
 - With a wildcard DNS record, every hostname in your domain resolves to the IP address of your router or load balancer, and you do not need to configure an A record for each app hostname. For example, if you create a DNS record `*.example.com` pointing to your load balancer or router, every application deployed to the `example.com` domain resolves to the IP address of your router.
- At least one wildcard TLS certificate that matches the DNS record you set up above, `*.example.com`.
- Sufficient IP allocation:
 - One static IP address for either HAProxy or one of your gorouters
 - One static IP address for each job in the Ops Manager tile. See the Resource Config pane for each tile for a full list.
 - One static IP address for each job listed below:
 - Consul
 - NATS
 - File Storage
 - MySQL Proxy
 - MySQL Server
 - Backup Prepare Node
 - HAProxy
 - Router
 - MySQL Monitor
 - Diego Brain
 - TCP Router

- One IP for each VM instance created by the service.
- An additional IP address for each compilation worker. So the formula for total IPs needed is

`IPs needed = static IPs + VM instances + compilation workers`.



Note: Pivotal recommends that you allocate at least 36 dynamic IP addresses when deploying Ops Manager and PAS. BOSH requires additional dynamic IP addresses during installation to compile and deploy VMs, install PAS, and connect to services.

- One or more NTP servers if not already provided by your IaaS.
- (**Recommended**) A network without DHCP available for deploying the PAS VMs.



Note: If you have DHCP, refer to the [Troubleshooting Guide](#) to avoid issues with your installation.


- (**Optional**) External storage. When you deploy PCF, you can select internal file storage or external file storage, either network-accessible or IaaS-provided, as an option in the PAS tile. Pivotal recommends using external storage whenever possible. See [Configure File Storage](#) for a discussion of how file storage location affects platform performance and stability during upgrades.
- (**Optional**) External databases. When you deploy PCF, you can select internal or external databases for the BOSH Director and for PAS. Pivotal recommends using external databases in production deployments. An external database must be configured to use the UTC timezone.
- (**Optional**) External user stores. When you deploy PCF, you can select a SAML user store for Ops Manager or a SAML or LDAP user store for PAS, to integrate existing user accounts.
- The most recent version of the [Cloud Foundry Command Line Interface](#) (cf CLI).

OpenStack Requirements



The following are OpenStack requirements for deploying PCF:

- PCF is supported on the OpenStack Ocata, Pike, Queens, Rocky, and Stein releases. OpenStack is a collection of inter-operable components and requires general OpenStack expertise to troubleshoot issues that may occur when installing Pivotal Cloud Foundry on particular releases and distributions. To verify that your OpenStack platform is compatible with PCF, use the OpenStack Validator tool. To access the OpenStack Validator tool, see [CF OpenStack Validator](#) on GitHub.
- Pivotal recommends granting complete access to the OpenStack logs to the operator managing the PCF installation process.
- For OpenStack accounts for PCF, Pivotal recommends following the principle of least privilege by scoping privileges to the most restrictive permissions possible for a given role.
- You must have a dedicated OpenStack project, formerly known as an OpenStack tenant.
- You must have Keystone access to the dedicated OpenStack project, including the following:
 - Auth URL
 - Username and password. The `PrimaryProject` for the user must be the project you want to use to deploy PCF. For more information, see [Manage projects and users](#) in the OpenStack documentation.
 - Project name
 - Region (with multiple availability zones if you require high availability)
 - SSL certificate for your wildcard domain (see below)
- You must have the ability to do the following in OpenStack:
 - Create and modify VM flavors
 - Enable DHCP if required
 - Create a network and then connect that network with a router to an external network
 - Create an external network with a pool of floating IP addresses
 - Boot VMs directly from image
 - Create two wildcard domains for separate system and app domains
- The following are resource requirements for the dedicated OpenStack project:
 - 118 GB of RAM
 - 22 available instances
 - 16 small VMs (1 vCPU, 1024 MB of RAM, 10 GB of root disk)
 - 3 large VMs (4 vCPU, 16384 MB of RAM, 10 GB of root disk)
 - 3 extra-large VMs (8 vCPU, 16 GB of RAM, 160 GB of ephemeral disk)
 - 56 vCPUs
 - 1 TB of storage

- Nova or Neutron networking with floating IP support


 **Note:** By default, PAS deploys the number of VM instances required to run a highly available configuration of PCF. If you are deploying a test or sandbox PCF that does not require HA, then you can scale down the number of instances in your deployment. For information about the number of instances required to run a minimal, non-HA PCF deployment, see [Scaling PAS](#).

- The following are requirements for the OpenStack Cinder back-end:
 - PCF requires RAW root disk images. The Cinder back-end for your OpenStack project must support RAW.
 - Pivotal recommends that you use a Cinder back-end that supports snapshots. This is required for some BOSH functionalities.
 - Pivotal recommends enabling your Cinder back-end to delete block storage asynchronously. If this is not possible, it must be able to delete multiple 20 GB volumes within 300 seconds.
- The following are requirements for using an Overlay Network with VXLAN or GRE Protocols:
 - If an overlay network is being used with VXLAN or GRE protocols, the MTU of the created VMs must be adjusted to the best practices recommended by the plugin vendor (if any).
 - DHCP must be enabled in the internal network for the MTU to be assigned to the VMs automatically.
 - Review the [Deploying PAS on OpenStack](#) topic to adjust your MTU values.
 - Failure to configure your overlay network correctly could cause Apps Manager to fail since applications will not be able to connect to the UAA.

 **Note:** If you are using IPsec, your resource usage will increase by approximately 36 bytes. View the [Installing IPsec topic](#)  for information, including setting correct MTU values.

Install PCF on OpenStack with PAS

To install PCF on OpenStack with the PAS runtime, do the following:

1. Deploy Ops Manager. See [Deploying Ops Manager on OpenStack](#).
2. Configure BOSH Director on OpenStack. See [Configuring BOSH Director on OpenStack](#).
3. (Optional) Install the PCF IPsec add-on. See [\(Optional\) Installing the PCF IPsec Add-On](#) .
4. Configure PAS. See [Deploying PAS on OpenStack](#).

Deploying Ops Manager on OpenStack

Page last updated:

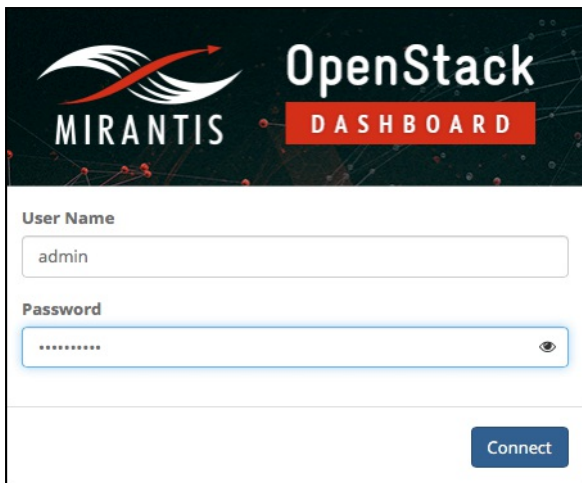
This guide describes how to provision the OpenStack infrastructure where you need to install [Pivotal Cloud Foundry](#). Use this topic when [Installing Pivotal Cloud Foundry on OpenStack](#).

After completing this procedure, complete all of the steps in the [Configuring BOSH Director on OpenStack](#) and [Deploying PAS on OpenStack](#) topics.

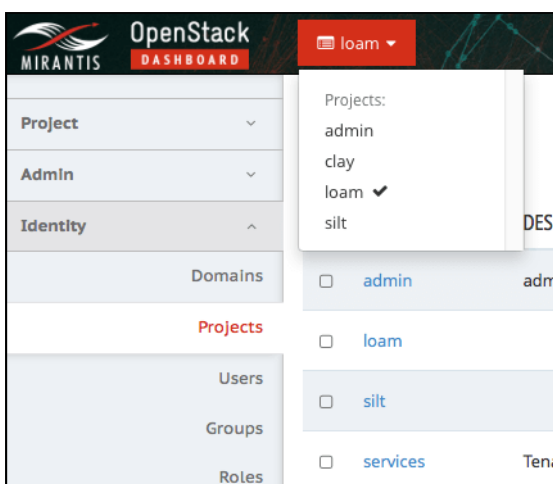
Note: This document uses Mirantis OpenStack for screenshots and examples. The screens of your OpenStack vendor configuration interface may differ.

Step 1: Log in to the OpenStack Horizon Dashboard

1. Log in to the OpenStack Horizon dashboard.



2. Click **Connect**.
3. From the OpenStack project list dropdown, set the active project by selecting the project where you will deploy PCF.



Step 2: Configure Security

Warning: If you are using OpenStack Liberty or Mitaka, do not create the key pair with the OpenStack Horizon dashboard. Instead make sure that you generate the SSH key pair manually. For example, use the `ssh-keygen` command. Then follow the procedure below to import that key pair into OpenStack. This is due to an [OpenStack bug](#).

1. In the left navigation of your OpenStack Horizon dashboard, click **Project > Compute > Access & Security**.
2. Select the **Key Pairs** tab on the **Access & Security** page.
3. Click **Import Key Pair**.
4. Enter a **Key Pair Name** and the contents of your public key in the **Public Key** field.

Import Key Pair

Key Pair Name *

Public Key *

ssh-rsa

AA

Description:

Key Pairs are how you login to your instance after it is launched.

Choose a key pair name you will recognise and paste your SSH public key into the space provided.

SSH key pairs can be generated with the ssh-keygen command:

```
ssh-keygen -t rsa -f cloud.key
```

This generates a pair of keys: a key you keep private (cloud.key) and a public key (cloud.key.pub). Paste the contents of the public key file here.

After launching an instance, you login using the private key (the username might be different depending on the image you launched):

```
ssh -i cloud.key <username>@<instance_ip>
```

5. Click **Import Key Pair**.
6. In the left navigation, click **Access & Security** to refresh the page. The new key pair appears in the list.
7. Select the **Security Groups** tab. Click **Create Security Group** and create a group with the following properties:
 - **Name:**
 - **Description:**

Create Security Group

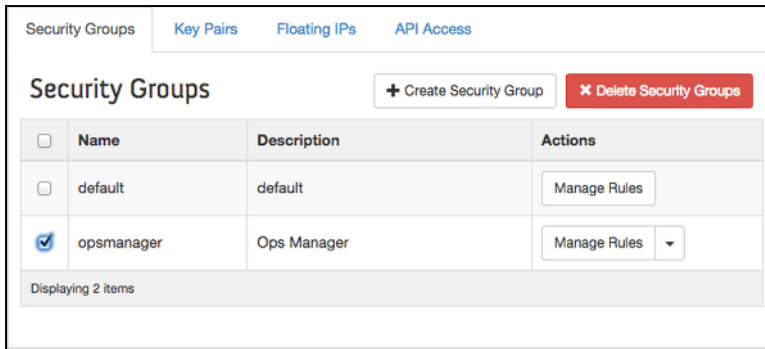
Name *

Description *

Description:

Security groups are sets of IP filter rules that are applied to the network settings for the VM. After the security group is created, you can add rules to the security group.

8. Select the checkbox for the Security Group and click **Manage Rules**.



9. Add the following ingress access rules for HTTP, HTTPS, and SSH as shown in the table below. The rules with `opsmanager` in the Remote column have restricted access to that particular Security Group.

Note: Adjust the remote sources as necessary for your own security compliance. Pivotal recommends limiting remote access to Ops Manager to IP ranges within your organization.

| Direction | Ether Type | IP Protocol | Port/Port Range | Remote |
|-----------|------------|-------------|-----------------|------------------|
| Ingress | IPv4 | TCP | 22 (SSH) | 0.0.0.0/0 (CIDR) |
| Ingress | IPv4 | TCP | 80 (HTTP) | 0.0.0.0/0 (CIDR) |
| Ingress | IPv4 | TCP | 443 (HTTPS) | 0.0.0.0/0 (CIDR) |
| Ingress | IPv4 | TCP | 25555 | 0.0.0.0/0 (CIDR) |
| Ingress | IPv4 | TCP | 1-65535 | opsmanager |
| Ingress | IPv4 | UDP | 1-65535 | opsmanager |

10. Leave the existing default egress access rules as shown in the screenshot below.

Access & Security

/ Manage Security Group Rules: opsmanager (af1 [redacted])

+ Add Rule X Delete Rules

| <input type="checkbox"/> | DIRECTION | ETHER TYPE | IP PROTOCOL | PORT RANGE | REMOTE IP PREFIX | REMOTE SECURITY GROUP | ACTIONS |
|--------------------------|-----------|------------|-------------|-------------|------------------|-----------------------|-------------|
| <input type="checkbox"/> | Egress | IPv4 | Any | Any | 0.0.0.0/0 | - | Delete Rule |
| <input type="checkbox"/> | Egress | IPv6 | Any | Any | ::/0 | - | Delete Rule |
| <input type="checkbox"/> | Ingress | IPv4 | TCP | 1 - 65535 | - | opsmanager | Delete Rule |
| <input type="checkbox"/> | Ingress | IPv4 | TCP | 22 (SSH) | 0.0.0.0/0 | - | Delete Rule |
| <input type="checkbox"/> | Ingress | IPv4 | TCP | 80 (HTTP) | 0.0.0.0/0 | - | Delete Rule |
| <input type="checkbox"/> | Ingress | IPv4 | TCP | 443 (HTTPS) | 0.0.0.0/0 | - | Delete Rule |
| <input type="checkbox"/> | Ingress | IPv4 | TCP | 25555 | 0.0.0.0/0 | - | Delete Rule |
| <input type="checkbox"/> | Ingress | IPv4 | UDP | 1 - 65535 | - | opsmanager | Delete Rule |

Displaying 8 items

Step 3: (Optional) Run the CF OpenStack Validator Tool

As an optional but recommended step, you can now run the CF OpenStack Validator tool against your OpenStack tenant to verify support for PCF.

- Follow the directions for running the [CF OpenStack Validator Tool](#).
- When configuring the CPI version used by the Validator, specify the OpenStack CPI version indicated in the [PCF Ops Manager Release Notes](#) for

the PCF release that you are planning to deploy.

Troubleshooting the output of the CF OpenStack Validator tool is beyond the scope of this document.

Step 4: Create Ops Manager Image

You can create the Ops Manager image in OpenStack using the OpenStack Horizon dashboard.

 **Note:** If your Horizon Dashboard does not support file uploads, you must use the [Glance CLI](#) client.

To create an Ops Manager image in OpenStack, do the following:

1. Download the **Pivotal Cloud Foundry Ops Manager for OpenStack** image file from [Pivotal Network](#).
2. In the left navigation of your OpenStack dashboard, click **Project > Compute > Images**.
3. Click **Create Image**. Complete the **Create An Image** page with the following information:
 - **Name:** Enter `Ops Manager`.
 - **Image Source:** Select **Image File**.
 - **Image File:** Click **Choose File**. Browse to and select the image file that you downloaded from [Pivotal Network](#).
 - **Format:** Select **Raw**.
 - **Minimum Disk (GB):** Enter `80`.
 - **Minimum RAM (MB):** Enter `8192`.
 - Deselect the **Public** checkbox.
 - Select the **Protected** checkbox.

Create An Image

Name *

Ops Manager

Description

Image Source

Image File

Image File

Choose File pcf-openstack-1.12.2.raw

Format *

Raw

Architecture

Minimum Disk (GB)

80

Minimum RAM (MB)

8192

☐ Public

☒ Protected

Cancel

Create Image

Description:

Currently only images available via an HTTP/HTTPS URL are supported. The image location must be accessible to the Image Service.

Please note: The Image Location field MUST be a valid and direct URL to the image binary. URLs that redirect or serve error pages will result in unusable images.

4. Click **Create Image**.

Step 5: Launch Ops Manager VM

1. In the left navigation of your OpenStack dashboard, click **Project > Compute > Images**.
2. Click **Launch**.

| Images | | | | | | | | |
|-------------------------------------|------------------|-------|--------|--------|-----------|--------|--------|-----------------|
| | | | | | | | | + Create Image |
| | | | | | | | | ✕ Delete Images |
| <input type="checkbox"/> | Image Name | Type | Status | Public | Protected | Format | Size | Actions |
| <input checked="" type="checkbox"/> | Ops Manager | Image | Active | No | No | RAW | 3.0 GB | Launch |
| <input type="checkbox"/> | OSBL-855-16-3-03 | Image | Active | No | No | RAW | 3.0 GB | Launch |

3. In the **Details** tab, specify the following values:

- **Instance Name:** Enter `Ops Manager`.
- **Availability Zone:** Use the dropdown to select an availability zone. You specify this availability zone in the [Complete the Availability Zones](#) [Pages](#) step of [Configuring Ops Manager Director](#).
- **Count:** Do not change from the default value of 1.

Launch Instance

Details

Source

Flavor *

Networks

Network Ports

Security Groups

Key Pair

Configuration

Metadata

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *

Ops Manager

Availability Zone

nova

Count *

1

Total Instances (No Limit)

0 Current Usage

1 Added

✕ Cancel

< Back

Next >

Launch Instance

4. In the **Source** tab, specify the following values:

- **Select Boot Source:** Select **Image**.
- **Create New Volume:** Leave **No** selected.
- **Allocated:** Make sure **Ops Manager** is selected.

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Metadata

Instance source is the template used to create an instance. You can use a snapshot of an existing instance, an image, or a volume (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source

Image

Create New Volume

Yes

No

Allocated

| NAME | UPDATED | SIZE | TYPE | VISIBILITY |
|-------------|------------------|---------|------|------------|
| Ops Manager | 10/10/17 6:49 PM | 4.39 GB | RAW | Private |

Available 2

Select one

Click here for filters.

| NAME | UPDATED | SIZE | TYPE | VISIBILITY |
|---------------|------------------|-----------|-------|------------|
| TestVM | 9/28/17 1:50 AM | 21.54 MB | QCOW2 | Public |
| ubuntu-xenial | 9/29/17 10:36 AM | 277.13 MB | QCOW2 | Public |

Cancel

Back

Next

Launch Instance

5. In the **Flavor** tab, configure the OpenStack VM flavors as follows:

Note: Do not change the names of the VM flavors.

| ID | Name | Memory_MB | Disk | Ephemeral | VCPUs |
|----|-----------|-----------|------|-----------|-------|
| 1 | m1.small | 2048 | 20 | 0 | 1 |
| 2 | m1.medium | 4096 | 40 | 0 | 2 |
| 3 | m1.large | 8192 | 80 | 0 | 4 |
| 4 | m1.xlarge | 16384 | 160 | 0 | 8 |

6. In the **Networks** tab, select a private subnet. You add a Floating IP to this network in a later step.

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Metadata

Networks provide the communication channels for instances in the cloud.

▼ Allocated 1

Select networks from those listed below.

| | NETWORK | SUBNETS ASSOCIATED | SHARED | ADMIN STATE | STATUS | |
|---|----------|--------------------|--------|-------------|--------|---|
| 1 | loam_net | | No | Up | Active | — |

▼ Available 0

Select at least one network

Click here for filters.

| NETWORK | SUBNETS ASSOCIATED | SHARED | ADMIN STATE | STATUS |
|--------------------|--------------------|--------|-------------|--------|
| No available items | | | | |

Cancel

Back

Next

Launch Instance

7. Skip the **Network Ports** tab.
8. In the **Security Groups** tab, select the **opsmanager** security group that you created in [Step 2: Configure Security](#). Deselect all other Security Groups.

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Metadata

Select the security groups to launch the instance in.

▼ Allocated 1

| NAME | DESCRIPTION |
|------------|-------------|
| opsmanager | Ops Manager |

▼ Available 2

Select one or more

Filter

| NAME | DESCRIPTION |
|---------|------------------------|
| default | Default security group |
| loam | loam Security Group |

✕ Cancel

< Back

Next >

Launch Instance

9. In the **Key Pair** tab, select the key pair that you imported in [Step 2: Configure Security](#).

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Metadata

A key pair allows you to SSH into your newly created instance. You may select an existing key pair, import a key pair, or generate a new key pair.

+ Create Key Pair

+ Import Key Pair

Allocated

| NAME | FINGERPRINT |
|-------|---------------|
| > pcf | 9d [REDACTED] |

Available 5

Q

Filter

Select one

| NAME ^ | FINGERPRINT |
|---------------|---------------|
| > clay | 9e [REDACTED] |
| > clay-bosh | 53 [REDACTED] |
| > id_rsa_bosh | d8 [REDACTED] |
| > loam | 42 [REDACTED] |
| > silt | 39 [REDACTED] |

Cancel

< Back

Next >

Launch Instance

- Skip the **Configuration** and **Metadata** tabs.
- Click **Launch Instance**. This step starts your new Ops Manager instance.

Step 6: Associate a Floating IP Address

- In the left navigation of your OpenStack dashboard, click **Project > Compute > Instances**.
- Wait until the **Power State** of the Ops Manager instance shows as *Running*.
- Record the private **IP Address** of the Ops Manager instance.

Instances

Instance Name =

Filter

Launch Instance

Delete Instances

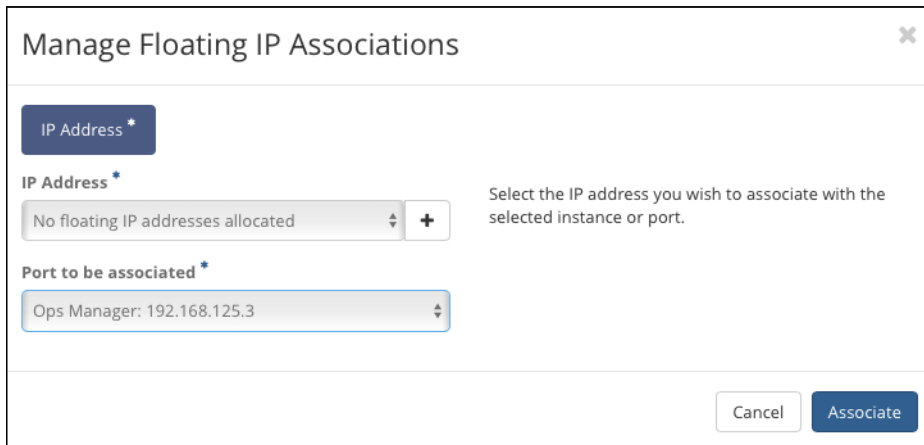
More Actions

| | INSTANCE NAME | IMAGE NAME | IP ADDRESS | SIZE | KEY PAIR | STATUS | AVAILABILITY ZONE | TASK | POWER STATE | TIME SINCE CREATED | ACTIONS |
|--------------------------|---------------|-------------|---------------|----------|----------|--------|-------------------|------|-------------|--------------------|-----------------|
| <input type="checkbox"/> | Ops Manager | Ops Manager | 192.168.125.3 | m1.large | pcf | Active | nova | None | Running | 0 minutes | Create Snapshot |

Displaying 1 item

You must provide this IP Address when you perform [Step 6: Complete the Create Networks Page](#) in Ops Manager.

- Select the **Ops Manager** checkbox. Click the **Actions** dropdown and select **Associate Floating IP**. The **Manage Floating IP Associations** screen



Manage Floating IP Associations

IP Address *

IP Address *

No floating IP addresses allocated +

Select the IP address you wish to associate with the selected instance or port.

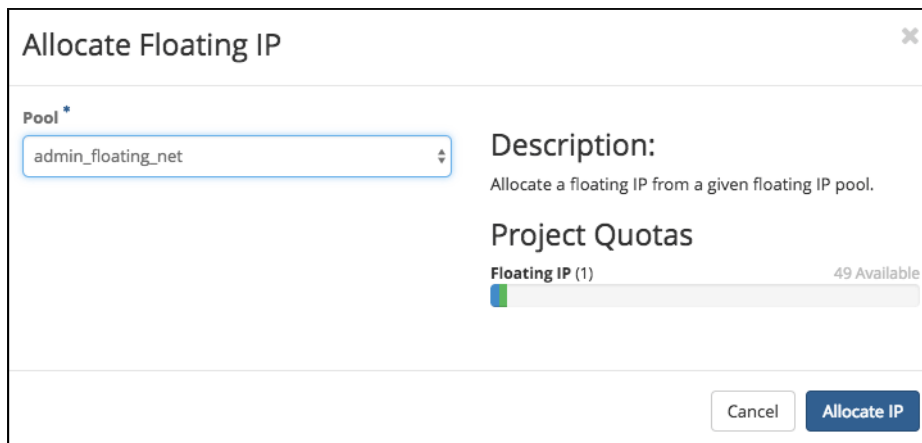
Port to be associated *

Ops Manager: 192.168.125.3

Cancel Associate

appears.

- Under **IP Address**, click the plus button (+). The **Allocate Floating IP** screen appears.
- Under **Pool**, select an IP Pool and click **Allocate IP**.



Allocate Floating IP

Pool *

admin_floating_net

Description:

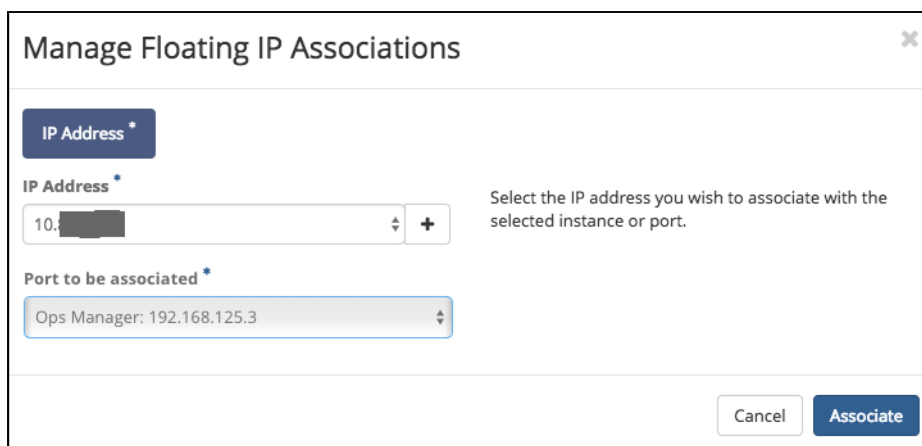
Allocate a floating IP from a given floating IP pool.

Project Quotas

Floating IP (1) 49 Available

Cancel Allocate IP

- Under **Port to be associated**, select your **Ops Manager** instance.



Manage Floating IP Associations

IP Address *

IP Address *

10. [redacted] +

Select the IP address you wish to associate with the selected instance or port.

Port to be associated *

Ops Manager: 192.168.125.3

Cancel Associate

- Click **Associate**.

Step 7: Add Blob Storage

- In the left navigation of your OpenStack dashboard, click **Project > Object Store > Containers**.
- Click **Create Container**. Create a container with the following properties:
 - Container Name:** Enter `pcf`.
 - Container Access:** Leave **public** unselected.

Create Container

Container Name *

Container Access

☐ Public

A container is a storage compartment for your data and provides a way for you to organize your data. You can think of a container as a folder in Windows® or a directory in UNIX®. The primary difference between a container and these other file system concepts is that containers cannot be nested. You can, however, create an unlimited number of containers within your account. Data must be stored in a container so you must have at least one container defined in your account prior to uploading data.

Note: A Public Container will allow anyone with the Public URL to gain access to your objects in the container.

✕ Cancel

+ Create

- Click **Create**.

Step 8: Download Credentials for S3 Blob Storage

- In the left navigation of your OpenStack dashboard, click **Project > Compute > Access & Security**. Select the **API Access** tab.

Access & Security

[Security Groups](#)
[Key Pairs](#)
[Floating IPs](#)
[API Access](#)

API Endpoints

Ⓜ Download OpenStack RC File

Ⓜ Download EC2 Credentials

+ View Credentials

| Service | Service Endpoint |
|---------|----------------------------------|
| Compute | http://213.146.132.100:8774/v2.0 |
| Network | http://213.146.132.100/ |

- Click **Download EC2 Credentials**.
- Unzip the downloaded credentials.
- If you select **S3 Compatible Blobstore** in your [BOSH Director Config](#), you need the contents of this file to complete the configuration.

Step 9: Create a DNS Entry

Note: For security, Ops Manager v1.7 and later require you to create a fully qualified domain name in order to access Ops Manager during the [initial configuration](#).

Create a DNS entry for the floating IP address that you assigned to Ops Manager in [Step 6: Associate a Floating IP Address](#).

You must use this fully qualified domain name when you log into Ops Manager for the first time.

Step 10: Configure BOSH Director for OpenStack

After completing this procedure, complete all of the steps in the [Configuring BOSH Director on OpenStack](#) and [Deploying PAS on OpenStack](#) topics.

Return to [Installing Pivotal Cloud Foundry on OpenStack](#).

Configuring BOSH Director on OpenStack

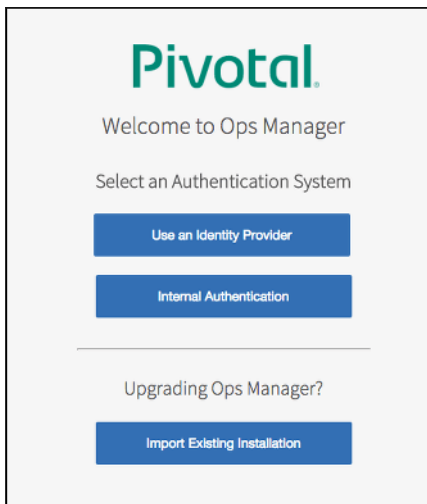
This topic describes how to configure BOSH Director after deploying [Pivotal Cloud Foundry](#) (PCF) on OpenStack. Use this topic when [Installing Pivotal Cloud Foundry on OpenStack](#).

- Before beginning this procedure, ensure that you have successfully completed all steps in [Provisioning the OpenStack Infrastructure](#).
- After you complete this procedure, follow the instructions in [Deploying PAS on OpenStack](#).

 **Note:** You can also perform the procedures in this topic using the Ops Manager API. For more information, see [Using the Ops Manager API](#).

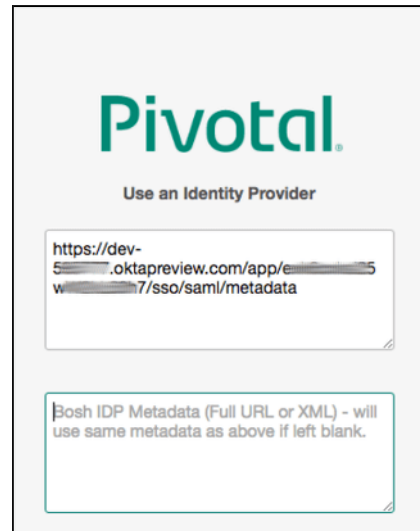
Step 1: Access Ops Manager

1. In a web browser, navigate to the fully qualified domain you created in the [Create a DNS Entry](#) step of *Provisioning the OpenStack Infrastructure*.
2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you choose **Use an Identity Provider**, an external identity server maintains your user database.
 - [Internal Authentication](#): If you choose **Internal Authentication**, Ops Manager maintains your user database.



Use an Identity Provider

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.



2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.

Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a `500` error.

Note: These attributes are case-sensitive.

- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.

5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.

6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

Note: To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.

- **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
- **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
- **Name ID:** Email Address
- SAML authentication requests are always signed

8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.

- **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
- **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
- **Name ID:** Email Address
- SAML authentication requests are always signed

9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

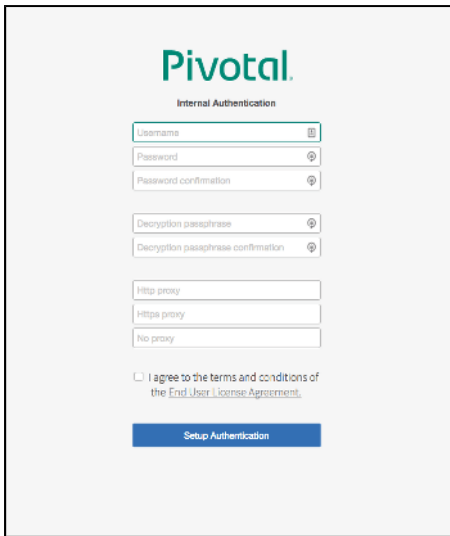
Use Internal Authentication

1. When redirected to the **Internal Authentication** page, do the following:

- Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
- Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not

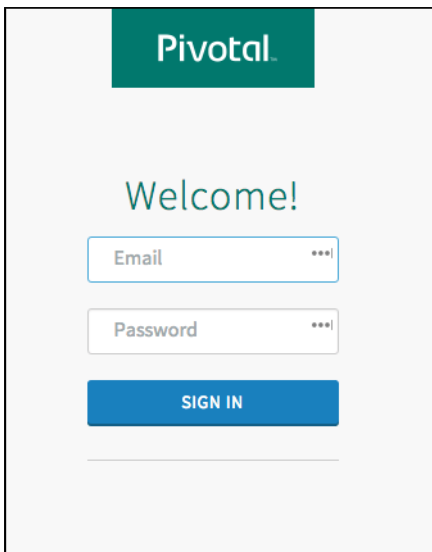
recoverable.

- If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in [Configuring Proxy Settings for the BOSH CPI](#).
- Read the **End User License Agreement**, and select the checkbox to accept the terms.
- Click **Setup Authentication**.



The screenshot shows the 'Internal Authentication' setup page in Pivotal. It features the Pivotal logo at the top. Below the logo, there are several input fields: 'Username', 'Password', 'Password confirmation', 'Decryption passphrase', and 'Decryption passphrase confirmation'. Each of these fields has a small icon to its right. Below these fields are three radio button options for 'Http proxy': 'Http proxy', 'Https proxy', and 'No proxy'. At the bottom, there is a checkbox labeled 'I agree to the terms and conditions of the End User License Agreement' and a blue button labeled 'Setup Authentication'.

2. Log in to Ops Manager with the Admin username and password you created in the previous step.



The screenshot shows the 'Welcome!' login page in Pivotal. It features the Pivotal logo at the top. Below the logo, the word 'Welcome!' is displayed. There are two input fields: 'Email' and 'Password', each with a small icon to its right. Below these fields is a blue button labeled 'SIGN IN'.

Step 2: OpenStack Config Page

1. In the left navigation of your OpenStack dashboard, click **Project > Compute > Access & Security**. Select the **API Access** tab.
2. Record the **Service Endpoint** for the **Identity** service. You use this Service Endpoint as the Authentication URL for Ops Manager in a later step.

Access & Security

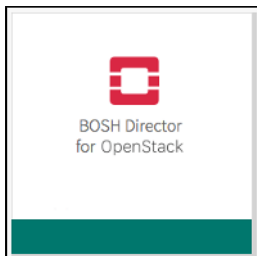
Security Groups Key Pairs Floating IPs API Access

[Download OpenStack RC File v2.0](#)
[Download OpenStack RC File v3](#)
[Download EC2 Credentials](#)
[+ View Credentials](#)

| SERVICE | SERVICE ENDPOINT |
|----------------|-------------------------------|
| Network | http://[REDACTED]:9696 |
| S3 | http://[REDACTED]:8080 |
| Cloudformation | http://[REDACTED]:8000/v1 |
| Object Store | http://[REDACTED]:80/swift/v1 |
| Artifact | http://[REDACTED]:494 |
| Compute_Legacy | http://[REDACTED] |
| Volumev3 | http://[REDACTED] |
| Compute | http://[REDACTED]:4/v2.1 |
| Image | http://[REDACTED]:292 |
| Volumev2 | http://[REDACTED] |
| Identity | http://[REDACTED]:5000/v2.0 |
| Volume | http://[REDACTED] |
| Orchestration | http://[REDACTED] |

Displaying 13 items

3. In the PCF Ops Manager Installation Dashboard, click the **BOSH Director** tile.



4. Select **OpenStack Config**.

5. Complete the **OpenStack Management Console Config** page with the following information:

- **Authentication URL:** Enter the Service Endpoint for the Identity service that you recorded in a previous step.
- **Keystone Version:** Choose a Keystone version, either **v2** or **v3**.
 - If you choose **v3**, enter the OpenStack Keystone domain to authenticate against in the **Domain** field. For more information about Keystone domains in OpenStack, see [Domains](#) in the *OpenStack documentation*.

OpenStack Config

Name*

default

Authentication URL*

http://10.87.16.4:5000/v2.0

Keystone Version

☒ v2
 ☐ v3

Domain

- **Username:** Enter your OpenStack Horizon username. The `PrimaryProject` for the user must be the project you are using to deploy PCF. For more information, see [Manage projects and users](#) in the OpenStack documentation.
- **Password:** Enter your OpenStack Horizon password.
- **Tenant:** Enter your OpenStack tenant name.
- **Region:** Enter `RegionOne`, or another region if recommended by your OpenStack administrator.
- **Select OpenStack omNetwork Type:** Select either **Nova**, the legacy OpenStack networking model, or **Neutron**, the newer networking model.
- **Ignore Server Availability Zone:** Do not select the checkbox.
- **Security Group Name:** Enter `opsmanager`. You created this Security Group in the [Configure Security](#) step of *Provisioning the OpenStack Infrastructure*.
- **Key Pair Name:** Enter the name of the key pair that you created in the [Configure Security](#) step of *Provisioning the OpenStack Infrastructure*.
- **SSH Private Key:** In a text editor, open the key pair file that you downloaded in the [Configure Security](#) step of *Provisioning the OpenStack Infrastructure*. Copy and paste the contents of the key pair file into the field.
- (Optional) **API SSL Certificate:** If you configured API SSL termination in your OpenStack Dashboard, enter your **API SSL Certificate**.
- **Disable DHCP:** Do not select the checkbox unless your configuration requires it.
- **Select OpenStack Network Type:** Select either **Nova**, the legacy networking model, or **Neutron**, the OpenStack networking model.

Openstack Management Console Config

Authentication URL*

http://10.85.55.3:5000/v2.0
URL to the Openstack Identity Endpoint

Keystone Version

☒ v2
☐ v3

Domain

Username*

admin

Password*

Change

Tenant*

loam

Region*

RegionOne

Select Openstack Network Type*

Neutron

☐ Ignore Server Availability Zone

Security Group Name

opsmanager

Key Pair Name*

pcf

SSH Private Key*

Change


API SSL Certificate*

☐ Disable DHCP

Save

6. Click **Save**.

Step 3: (Optional) Advanced Config Page

 **Note:** This is an advanced option. Most users leave this field blank.

1. In Ops Manager, select **Advanced Infrastructure Config**.

Advanced Infrastructure Configuration

Connection Options

Save

- If your OpenStack environment requires specific connection options, enter them in the **Connection Options** field in JSON format. For example:

```
'connection_options' => { 'read_timeout' => 200 }
```

- Click **Save**.

Step 4: Director Config Page

- In Ops Manager, select **Director Config**.

Director Config

NTP Servers (comma delimited)*

us.pool.ntp.org

JMX Provider IP Address

Bosh HM Forwarder IP Address

☐ Enable VM Resurrector Plugin

☐ Enable Post Deploy Scripts

☐ Recreate all VMs

This will force BOSH to recreate all VMs on the next deploy. Persistent disk will be preserved

☐ Enable bosh deploy retries

This will attempt to re-deploy a failed deployment up to 5 times.

☐ Keep Unreachable Director VMs

- Enter one or more NTP servers in the **NTP Servers (comma delimited)** field. For example, `us.pool.ntp.org`.



Note: The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify the value of this field.

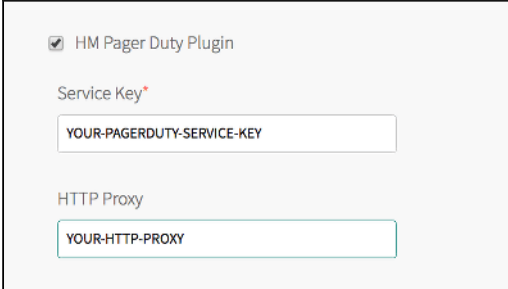
- Leave the **JMX Provider IP Address** field blank.

Note: Starting in PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. If you continue to use PCF JMX Bridge to consume these component metrics outside of the Firehose, you may receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#) in the PCF v2.0 Release Notes.

4. Leave the **Bosh HM Forwarder IP Address** field blank.

Note: Starting in PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. If you continue to use the BOSH HM Forwarder to consume these component metrics, you may receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#) in the PCF v2.0 Release Notes.

5. Select the **Enable VM Resurrector Plugin** checkbox to enable the Ops Manager Resurrector functionality and increase PAS availability.
6. Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.
7. Select **Recreate all VMs** to force BOSH to recreate all VMs on the next deploy. This process does not destroy any persistent disk data.
8. Select **Enable bosh deploy retries** to instruct Ops Manager to retry failed BOSH operations up to five times.
9. (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS secure communications.
10. Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.



The screenshot shows a configuration form for the 'HM Pager Duty Plugin'. It includes a checked checkbox for the plugin name, a 'Service Key' field with a red asterisk and a placeholder 'YOUR-PAGERDUTY-SERVICE-KEY', and an 'HTTP Proxy' field with a placeholder 'YOUR-HTTP-PROXY'.

11. Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.

- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.

☒ HM Email Plugin

Host*

Port*

Domain*

From*

Recipients*

Username

Password


☒ Enable TLS

12. Select **HM Email Plugin** to enable Health Monitor integration with email.

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma-separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter the password for your email server.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

13. For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

 **Note:** After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*


HSM Port Address*

Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**
 9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal
☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature
☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- o **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- o **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. Follow the procedures in [Sign up for Amazon S3](#) and [Creating a Bucket](#) in the AWS documentation. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.

- **GCS Blobstore:** Select this option to use an external GCS endpoint. To create a GCS bucket, you must have a GCS account. Follow the procedures in [Creating Storage Buckets](#) in the GCS documentation to create a GCS bucket. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Follow the steps in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually* to download a JSON file with a private key. Enter the contents of the JSON file into the field.

15. Select a **Database Location**. By default, Ops Manager deploys and manages a database for you. If you choose to use an **External MySQL Database**, complete the associated fields with information obtained from your external MySQL Database provider.

Database Location

☒ Internal

☐ External MySQL Database

Host*

Port*

Username*

Password*

Database*

In addition, if you selected the **Enable TLS**

for **Director Database** checkbox, you can complete the following optional fields:

- **Enable TLS:** Select this checkbox to enables TLS communication between the BOSH Director and the database.
- **TLS CA:** Enter the Certificate Authority for the TLS Certificate.
- **TLS Certificate:** Enter the client certificate for mutual TLS connections to the database.
- **TLS Private Key:** Enter the client private key for mutual TLS connections to the database.
- **Advanced DB Connection Options:** If you would like to provide additional options for the database, use this field to provide a JSON-formatted options string.

16. (Optional) **Director Workers:** Set the number of workers available to execute Director tasks. This field defaults to .

17. (Optional) **Max Threads:** Enter the number of operations the BOSH Director can perform simultaneously.

18. (Optional) **Director Hostname:** Enter a valid hostname to add a custom URL for your BOSH Director. You can also use this field to configure a load balancer in front of your BOSH Director. For more information, see [How to Set Up a Load Balancer in Front of Operations Manager Director](#) in the Pivotal Support documentation.

⚠ warning: In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, VMs become unavailable. This causes PCF downtime. To restore VM availability, enable **Recreate All VMs** and redeploy. This issue is resolved in [Ops Manager v2.2.8](#) and later.

19. (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.
20. (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.

⚡ Breaking Change: Do not disable BOSH DNS without consulting Pivotal Support.

21. (Optional) **Custom SSH Banner:** Enter text to set a custom banner that users see when logging in to the Director using SSH.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

22. (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1, hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.
23. Click **Save**.

💡 Note: If you select to use an internal database, back up your data frequently. For more information, see [Backing Up and Restoring Pivotal Cloud Foundry](#).

Step 5: Create Availability Zones Page

1. In Ops Manager, select **Create Availability Zones**.

Create Availability Zones

Availability Zones

▼ novaOpenstack Availability Zone*

nova

Save

2. Enter the name of the availability zone that you selected in the [Launch Ops Manager VM](#) step of *Provisioning the OpenStack Infrastructure*
3. Click **Save**.

Step 6: Create Networks Page

1. In the left navigation of your OpenStack dashboard, click **Project > Network > Networks**.

- Click the name of the network that contains the private subnet where you deployed the Ops Manager VM. The OpenStack Network Detail page displays your network settings.

[Networks](#) / loam_net Edit Network ▾

Network Overview

| | |
|-------------------------|---|
| Name | loam_net |
| ID | f92b1a1d-1234-5678-9012-345678901234 |
| Project ID | 8a5b1a1d-1234-5678-9012-345678901234 |
| Status | Active |
| Admin State | UP |
| Shared | No |
| External Network | No |
| MTU | 1450 |
| Provider Network | Network Type: vxlan Physical Network: - Segmentation ID: 93 |

Subnets

+ Create Subnet
Delete Subnets

| <input type="checkbox"/> | NAME | NETWORK ADDRESS | IP VERSION | GATEWAY IP | ACTIONS |
|--------------------------|-----------------|------------------|------------|---------------|----------------------------|
| <input type="checkbox"/> | (9c622786-2276) | 192.168.125.0/24 | IPv4 | 192.168.125.1 | Edit Subnet ▾ |

Displaying 1 item

Ports

| NAME | FIXED IPS | ATTACHED DEVICE | STATUS | ADMIN STATE | ACTIONS |
|-----------------|---------------|--------------------------|--------|-------------|------------------------|
| (592facc6-b7c7) | 192.168.125.2 | network:dhcp | Active | UP | Edit Port |
| (be836ab3-e9ed) | 192.168.125.3 | compute:nova | Active | UP | Edit Port |
| (75b1acc9-48ea) | 192.168.125.1 | network:router_interface | Active | UP | Edit Port |
| (1e7026a4-83ce) | 192.168.125.4 | compute:nova | Active | UP | Edit Port |

Displaying 4 items

- In Ops Manager, select **Create Networks**.

Create Networks

Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future. Contact Pivotal support for help completing such a change.

Verification Settings

☒ Enable ICMP checks

Networks

One or many IP ranges upon which your products will be deployed

▼ loam

Name*

loam

A unique name for this network

Subnets

Network ID*

CIDR*

192.168.125.0/24

Reserved IP Ranges

192.168.125.0-192.168.125.10

DNS*

8.8.8.8

Gateway*

192.168.125.1

Availability Zones*

☒ nova

Add Network

Add Subnet

Save

- Select **Enable ICMP checks** to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable. Review the [Configure Security](#) step of *Deploying BOSH and Ops Manager to OpenStack* to ensure you have configured ICMP in your Security Group.
- Use the following steps to create one or more Ops Manager networks using information from your OpenStack network:
 - Click **Add Network**.
 - Enter a unique **Name** for the network.
 - Click **Add Subnet** to create one or more subnets for the network.
 - For **Network ID**, use the **ID** from the OpenStack page.
 - For **CIDR**, use the **Network Address** from the OpenStack page.
 - For **Reserved IP Ranges**, use the first 10 IP addresses of the **Network Address** range, and the private IP address of the Ops Manager instance that you recorded in the [Associate a Floating IP Address](#) step of *Provisioning the OpenStack Infrastructure*.
 - For **DNS**, enter one or more Domain Name Servers.
 - For **Gateway**, use the **Gateway IP** from the OpenStack page.
 - For **Availability Zones**, select which Availability Zones to use with the network.

- Click **Save**.

Note: After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

Step 7: Assign AZs and Networks Page

- Select **Assign Availability Zones**.

Assign AZs and Networks

The Ops Manager Director is a single instance.

Choose the availability zone in which to place that instance. It is highly recommended that you backup this VM on a regular basis to preserve settings.

Singleton Availability Zone

nova

Network

loam

Save

- From the **Singleton Availability Zone** dropdown, select the availability zone that you created in a previous step. The BOSH Director installs in this Availability Zone.
- Use the dropdown to select the **Network** that you created in a previous step. BOSH Director installs in this network.
- Click **Save**.

Step 8: Security Page

Security

Trusted Certificates

-----BEGIN CERTIFICATE-----

TH

These certificates enable BOSH-deployed components to trust a custom root certificate.

Generate VM passwords or use single password for all VMs

☒ Generate passwords
 ☐ Use default BOSH password

Save

- Select **Security**.

2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:

```
-----BEGIN CERTIFICATE-----
ABCDEF12345678ABCDEF12345678ABCDEF12345678AB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BCDEF12345678ABCDEF12345678ABCDEF12345678ABB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CDEF12345678ABCDEF12345678ABCDEF12345678ABBB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
-----END CERTIFICATE-----
```



Note: If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#) for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 9: Syslog Page

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
 ☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

⌵

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save

- (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
- In the **Address** field, enter the IP address or DNS name for the remote server.
- In the **Port** field, enter the port number that the remote server listens on.
- In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
- (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
 - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
- Click **Save**.

Step 10: Resource Config Page

- Select **Resource Config**.

Resource Config

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE |
|------------------------|--------------|----------------------|---|
| Ops Manager Director | Automatic: 1 | Automatic: 50 GB | Automatic: medium.disk (cpu: 2, ram: 4 GE |
| Master Compilation Job | Automatic: 4 | None | Automatic: large.cpu (cpu: 4, ram: 4 GB, di |

Save

- Adjust any values as necessary for your deployment, such as increasing the persistent disk size. Select **Automatic** from the dropdown to provision the amount of persistent disk predefined by the job. If the persistent disk field reads **None**, the job does not require persistent disk space.

Note: Ops Manager requires a Director VM with at least 8 GB memory.

Note: If you set a field to **Automatic** and the recommended resource allocation changes in a future version, Ops Manager automatically uses the updated recommended allocation.

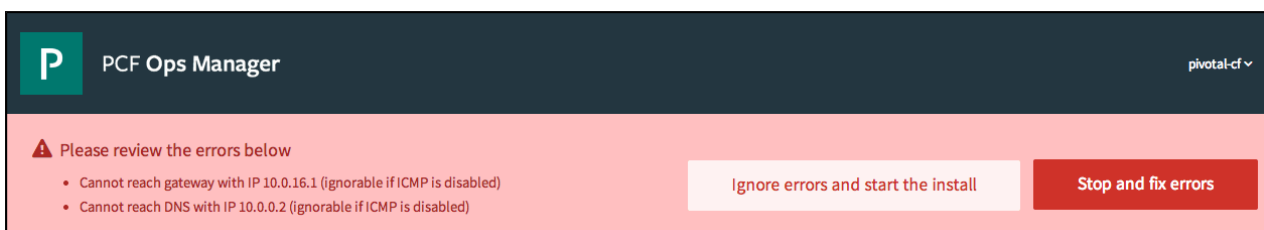
- Click **Save**.

Step 11: (Optional) Add Custom VM Extensions

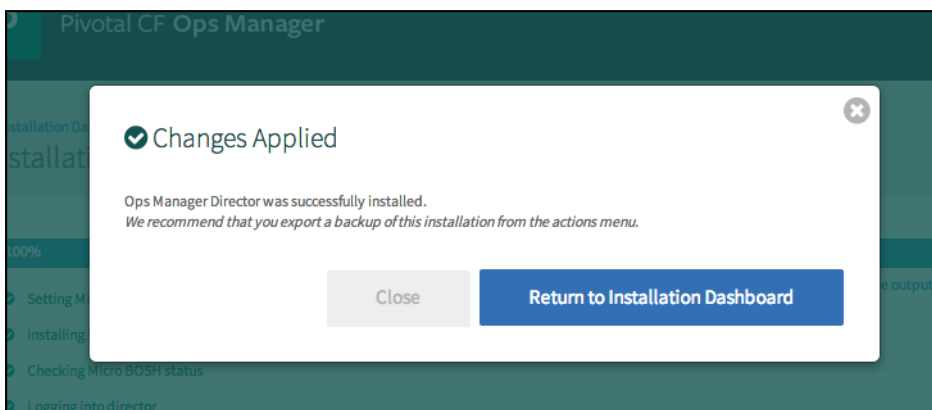
Use the Ops Manager API to add custom properties to your VMs such as associated security groups and load balancers. For more information, see [Managing Custom VM Extensions](#).

Step 12: Complete BOSH Director Installation

- Click the **Installation Dashboard** link to return to the Installation Dashboard.
- Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.



- BOSH Director installs. The image shows the **Changes Applied** message that Ops Manager displays when the installation process successfully completes.



4. After you complete this procedure, follow the instructions in [Deploying PAS on OpenStack](#).

Return to [Installing Pivotal Cloud Foundry on OpenStack](#).

Deploying PAS on OpenStack

Page last updated:

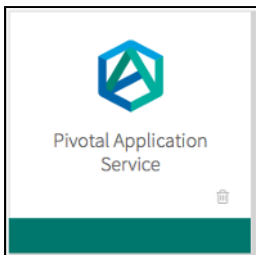
This topic describes how to install and configure Pivotal Application Service (PAS) after deploying [Pivotal Cloud Foundry](#) (PCF) on OpenStack.

Use this topic when [Installing Pivotal Cloud Foundry on OpenStack](#).

Before beginning this procedure, ensure that you have successfully completed all steps in the [Provisioning the OpenStack Infrastructure](#) topic and the [Configuring BOSH Director on OpenStack](#) topics.

Step 1: Add PAS to Ops Manager

1. If you have not already downloaded PAS, log in to [Pivotal Network](#), and click PAS.
2. From the **Releases** drop-down, select the release to install and choose one of the following:
 - a. Click PAS to download the PAS `.pivotal` file.
 - b. Click **PCF Small Footprint Runtime** to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).
3. Navigate to the Pivotal Cloud Foundry Operations Manager Installation Dashboard.
4. Click the Pivotal Network link on the left to add PAS to Ops Manager. For more information, refer to the [Adding and Deleting Products](#) topic.



Step 2: Assign Availability Zones and Networks

Note: Pivotal recommends at least three Availability Zones for a highly available installation of PAS.

1. Select **Assign AZ and Networks**. These are the Availability Zones that you [create](#) when configuring BOSH Director.
2. Select an Availability Zone under **Place singleton jobs**. Ops Manager runs any job with a single instance in this Availability Zone.
3. Select one or more Availability Zones under **Balance other jobs**. Ops Manager balances instances of jobs with more than one instance across the Availability Zones that you specify.
4. From the **Network** dropdown, choose the network on which you want to run PAS.

The screenshot shows the 'Pivotal Application Service' settings interface. At the top, there's a navigation bar with 'Settings', 'Status', 'Credentials', and 'Logs'. The 'Settings' tab is active. Below it, a list of settings categories is shown on the left, each with a green checkmark: 'Assign AZs and Networks', 'Domains', 'Networking', 'Application Containers', 'Application Developer Controls', 'Application Security Groups', 'Authentication and Enterprise SSO', and 'Databases'. The 'Assign AZs and Networks' category is selected, and its details are shown on the right. The title 'AZ and Network Assignments' is at the top of this section. It contains two radio buttons for 'Place singleton jobs in': 'first-az' (selected) and 'Balance other jobs in'. Below this, there's a checkbox for 'first-az' under 'Balance other jobs in', which is checked. A 'Network' dropdown menu is set to 'first-network'. A blue 'Save' button is at the bottom right of this section.

5. Click **Save**.

Note: When you save this form, a verification error displays because the PCF security group blocks ICMP. You can ignore this error.

The screenshot shows a red error message box from 'PCF Ops Manager'. It contains a warning icon and the text 'Please review the errors below'. The errors listed are: 'Cannot reach gateway with IP 10.0.16.1 (ignorable if ICMP is disabled)' and 'Cannot reach DNS with IP 10.0.0.2 (ignorable if ICMP is disabled)'. It concludes with 'All errors will be reverified before installation.'


Step 3: Configure Domains


1. Select **Domains**.

The screenshot shows the 'Configure Domains' form. It has a text box explaining: 'Elastic Runtime hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.' Below this, there are two input fields: 'System Domain *' with the value 'sys.example.com' and 'Apps Domain *' with the value 'apps.example.com'. A blue 'Save' button is at the bottom left.

2. Enter the system and application domains.

- The **System Domain** defines your target when you push apps to PAS.
- The **Apps Domain** defines where PAS should serve your apps.

 **Note:** Pivotal recommends that you use the same domain name but different subdomain names for your system and app domains. Doing so allows you to use a single wildcard certificate for the domain while preventing apps from creating routes that overlap with system routes. For example, name your system domain `system.EXAMPLE.com` and your apps domain `apps.EXAMPLE.com`.


 **Note:** You configured wildcard DNS records for these domains in an earlier step.

3. Click **Save**.

Step 4: Configure Networking

1. Select **Networking**.

2. The values you enter in the **Router IPs** and **HAProxy IPs** fields depend on whether you are using HAProxy in your deployment. Use the table below to determine how to complete these fields.

 **Note:** If you choose to assign specific IP addresses in either the **Router IPs** or **HAProxy IPs** field, ensure that these IP addresses are in the subnet that you configured for PAS in Ops Manager.

| Using HAProxy? | Router IPs Field | HAProxy IPs Field |
|----------------|--|--|
| No | <ol style="list-style-type: none"> 1. Choose IP addresses from the subnet you configured in Ops Manager. 2. Enter these IP addresses in the Router IPs field. You should specify more than one IP address for high availability. 3. Configure your load balancer to forward requests for the domains that you have configured for your deployment to these IP addresses. | Leave this field blank. |
| Yes | Leave this field blank. | <ol style="list-style-type: none"> 1. Choose IP addresses from the subnet you configured in Ops Manager. 2. Enter these IP addresses in the HAProxy IPs field. You should specify more than one IP address for high availability. 3. Configure your load balancer to forward requests for the domains you have configured for your deployment to these IP addresses. |

3. (Optional) In **SSH Proxy IPs**, add the IP address for your Diego Brain, which will accept requests to SSH into application containers on port `2222`.

4. (Optional) In **TCP Router IPs**, add the IP address(es) you would like assigned to the TCP Routers. You enable this feature at the bottom of this screen.

Configure security and routing services for your platform. It is usually preferable to use your own load balancer instead of an HAProxy instance as your point-of-entry to the platform.

Router IPs

10.85.10.200

SSH Proxy IPs

10.85.10.201

HAProxy IPs

TCP Router IPs

5. Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate and Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.

- a. Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

Certificates and Private Keys for HAProxy and Router

Add

▼ example-cert

Name *

example-cert

A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

Generate RSA Certificate

▼ example-cert-2

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager.

- b. If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see *Configure Front End* in [Preparing to Deploy Ops Manager on GCP Manually](#).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

- (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Routerfield**, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

☐ TLSv1.0

☐ TLSv1.1

☒ TLSv1.2

- Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

☒ Log client IPs

☐ Disable logging of X-Forwarded-For header only

☐ Disable logging of both source IP and X-Forwarded-For header

To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.

- Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.

Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *



☒ TLS terminated for the first time at infrastructure load balancer

☐ TLS terminated for the first time at HAProxy

☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|--|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to the instances of HAProxy, and HAProxy instance count is > 0 | TLS terminated for the first time at HAProxy. | <p>HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header.</p> <p> Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option.</p> |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | TLS terminated for the first time at the Gorouter. | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p> <p> Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option.</p> |

For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).


10. To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

☒ HAProxy does not request client certificates.

☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.

 **warning:** Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

11. To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- o **Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- o **Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- o **Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

⚠ warning: Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client Certificate Validation** in the **Networking** pane.

12. In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

`ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384`

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.


💡 Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

13. In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:
`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384` If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384`

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

14. Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ **Enable**

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ **Disable**

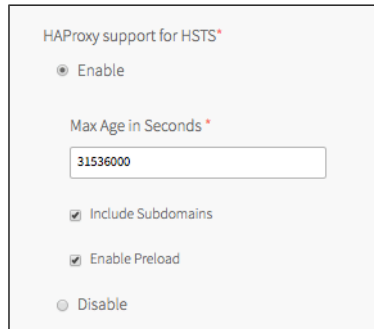
- **Enable HAProxy forwarding of requests to Router over TLS**

| | |
|--------------------------------------|---|
| If you want to: | Encrypt communication between HAProxy and the Gorouter |
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

- **Disable HAProxy forwarding of requests to Router over TLS**

| | |
|--------------------------------------|---|
| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |

15. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field and complete



HAProxy support for HSTS*

☒ Enable

Max Age in Seconds*

31536000

☒ Include Subdomains


☒ Enable Preload

☐ Disable

the following optional configuration steps:

- (Optional) Enter a **Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
- (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
- (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from HAProxy.

- If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

- (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

- (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
- (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
- (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
- By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#)

- (Optional) By default, Gorouter support for the PROXY protocol is disabled. To enable the PROXY protocol, select **Enable support for PROXY protocol in CF Router**. When enabled, client-side load balancers that terminate TLS but do not support HTTP can pass along information from the originating client. Enabling this option may impact Gorouter performance. For more information about enabling the PROXY protocol in Gorouter, see the *HTTP Header Forwarding* sections in the [Securing Traffic in Cloud Foundry](#) topic.
- In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details.
 - If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
- (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

0

500

25. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router*


☒ Enable
 ☐ Disable

26. (Optional) To accommodate larger uploads over connections with high latency, increase the number of seconds in the **Router Timeout to Backends** field.
27. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

28. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
29. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

20

Load Balancer Healthy Threshold *

20

30. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

31. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

32. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.

HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.

HAProxy Trusted CIDRs

33. The **Loggregator Port** defaults to **443** if left blank. Enter a new value to override the default.

Container Network Interface Plugin*



34. For **Container Network Interface Plugin**, ensure **Silk** is selected and review the following fields:

Note: The **External** option exists to support NSX-T integration for vSphere deployments.

- (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to **1454**. Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses **10.255.0.0/16**.

Warning: The overlay network IP range must not conflict with any other IP addresses in your network.

- Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to **1**.
- For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to **100**.
- To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- By default, containers use the same DNS servers as the host. If you want to override the DNS servers to be used in containers, enter a comma-separated list of servers in **DNS Servers**.

Note: If your deployment uses BOSH DNS, which is the default, you cannot use this field to override the DNS servers used in containers.

35. For **DNS Search Domains**, enter DNS search domains for your containers as a comma-separated list. DNS on your containers appends these names to its host names, to resolve them into full domain names.

36. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is **120**. You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

DNS Search Domains

example.com, myapps.com

DNS search domains to be used in containers. A comma-separated list can be specified.

37. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:

- a. Select **Enable TCP Routing**.
- b. For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. These are the same ports that you configured in the [Pre-Deployment Steps](#) of the *Enabling TCP Routing* topic.
 - To support multiple TCP routes, Pivotal recommends allocating multiple ports.
 - To allocate a list of ports rather than a range:
 1. Enter a single port in the **TCP Routing Ports** field.
 2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time
 ☒ Enable TCP Routing

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

- c. Return to the top of the **Networking** screen. In **TCP Router IPs** field, make sure you have entered IP addresses within your subnet CIDR block. These will be the same IP addresses you configured your load balancer with in [Pre-Deployment Steps](#), unless you configured DNS to resolve the TCP domain name directly to an IP you've chosen for the TCP router. You can enter multiple values as a comma-delimited list or as a range. For example, `10.254.0.1, 10.254.0.2` or `10.254.0.1-10.254.0.2`.
- d. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) [↗](#) topic.

38. Click **Save**.

Step 5: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC

☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888


Docker Images Disk-Cleanup Scheduling on Cell VMs*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) *


10240


- The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.
- The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
- If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
- If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.


- To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting](#) in *HTTP Routing*.

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

 **Warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

7. You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
8. Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
9. Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
10. Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.

 **Note:** In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

11. (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs*

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

12. By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.

13. Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
14. You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is seconds and the maximum configurable timeout is seconds.
15. Click **Save**.

Step 6: Configure Application Developer Controls

1. Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *

Staging Timeout (Seconds) *

☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.
4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.

5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.

Note: If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of seconds you specify in this field.
9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 7: Review Application Security Groups

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type ☐ in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 8: Configure UAA

1. Select **UAA**.
2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

3. Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN`.



Note: The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN`.

- If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
M
U
H
M
-----END CERTIFICATE-----

[Change](#)

SAML Service Provider Key Password

Secret

Password.

- (Optional) To override the default value, enter a custom SAML Entity ID in the **SAML Entity ID Override** field. By default, the SAML Entity ID is `http://login.YOUR-SYSTEM-DOMAIN` where `YOUR-SYSTEM-DOMAIN` is set in the **Domains > System Domain** field.
- For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
- (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line Interface (cf CLI) login access and refresh. Most deployments use the defaults.

Apps Manager Access Token Lifetime (in seconds) *

Apps Manager Refresh Token Lifetime (in seconds) *

Cloud Foundry CLI Access Token Lifetime (in seconds) *

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

Global Login Session Max Timeout (in seconds) *


Global Login Session Idle Timeout (in seconds) *

Customize Username Label (on login page) *

Customize Password Label (on login page) *

Proxy IPs Regular Expression *

8. (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:
 - **Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - **Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan
9. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
10. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Gorouter or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
11. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#) for help.

Internal Database Configuration

When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane. See the [Configure Internal Databases](#) section for details.

1. Select **Internal MySQL**.

Choose the location of your UAA database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use AWS RDS)

 **Note:** If you configure your system databases as external in the **Databases** pane, selecting Internal MySQL in the **UAA** pane has no effect.

2. Click **Save**.
3. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

1. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)

☒ External (preferred if, for example, you use AWS RDS)

Hostname *


TCP Port *

Username *


Password *

2. For **Hostname**, enter the hostname of the database server.
3. For **TCP Port**, enter the port of the database server.
4. For **User Account and Authentication database username**, specify a unique username that can access this specific database on the database server.
5. For **User Account and Authentication database password**, specify a password for the provided username.
6. Click **Save**.

Step 9: Configure CredHub

 **Note:** Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

1. Select **CredHub**.
2. Choose the location of your CredHub database. PAS includes this CredHub database for services to store their service instance credentials.

 **Note:** You cannot choose **Internal** for the CredHub database if you choose **External** for your System Databases. See [Configure System](#)

Databases below.

Configure the CredHub Server

Choose the location of your CredHub database *

- ☒ Internal MySQL (preferred for complete high-availability)
- ☐ External (preferred if, for example, you use Google Cloud SQL)

If you chose **External**, enter the following:

- **Hostname.** This is the IP address of your database server.
- **TCP Port.** This is the port of your database server, such as `3306`.
- **Username.** This is a unique username that can access your CredHub database on the database server.
- **Password.** This is the password for the provided username.
- **Database CA Certificate.** This certificate is used when encrypting traffic to and from the database.

3. Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys



Name *

Name of the encryption key.

Provider*

Key *

☐ Primary

- **Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- **Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- **Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- **Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.



Note: For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

4. (Optional) To configure CredHub to use an HSM, complete the following fields:

- **HSM Provider Partition.** This is the name of the HSM provider partition.
- **HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- **HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#) in the

Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

5. If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.

6. Click **Save**.

7. Select the **Resource Config** pane.

8. Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.

9. Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).

Step 10: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *


2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.

3. Click **Save**.

Step 11: Configure System Databases

You can configure PAS to use an internal MySQL database provided with PCF, or you can configure an external database provider for the databases required by PAS.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. Contact Pivotal Support for help. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration

If you want to use internal databases for your deployment, perform the following steps:

1. Select **Databases**.

2. Select one of the **Internal Databases** options:

- **Internal Databases - MySQL - Percona XtraDB Cluster** uses [Percona Server](#) with TLS encryption between server cluster nodes.
- **Internal Databases - MySQL - MariaDB Galera Cluster** uses [MariaDB](#) with cluster nodes communicating over plaintext.

⚠ warning: Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

3. Click **Save**.

Then proceed to [Step 12: \(Optional\) Configure Internal MySQL](#) to configure high availability for your internal MySQL databases.

External Database Configuration

⚠ warning: Protect whichever database you use in your deployment with a password.

To create your Pivotal Application Service (PAS) databases, follow the procedure below.

💡 Note: Exact configurations depend on your database provider. The following procedure uses AWS RDS as an example.

1. Add the `ubuntu` account key pair from your IaaS deployment to your local SSH profile so you can access the Ops Manager VM. For example, in AWS, you add a key pair created in AWS:

```
$ ssh-add aws-keypair.pem
```

2. SSH in to your Ops Manager using the Ops Manager FQDN and the username `ubuntu`:

```
$ ssh ubuntu@OPS-MANAGER-FQDN
```

3. Log in to your MySQL database instance using the appropriate hostname and user login values configured in your IaaS account. For example, to log in to your AWS RDS instance, run the following MySQL command:


```
$ mysql --host=RDSHOSTNAME --user=RDSUSERNAME --password=RDSPASSWORD
```

4. Run the following MySQL commands to create databases for the PAS components that require a relational database:


```
CREATE database ccd;
CREATE database notifications;
CREATE database autoscale;
CREATE database app_usage_service;
CREATE database routing;
CREATE database diego;
CREATE database account;
CREATE database nfsvolume;
CREATE database networkpolicyserver;
CREATE database silk;
CREATE database locket;
CREATE database uaa;
CREATE database credhub;
```

💡 Note: The command `CREATE database credhub;` is optional if you have no CredHub instances. By default, CredHub has `0` instances.

5. Type `exit` to quit the MySQL client, and `exit` again to close your connection to the Ops Manager VM.
6. In PAS, select **Databases**.
7. Select the **External Databases** option.


 **Note:** If you configure databases as external, you cannot configure an internal database in the **UAA** pane.

8. For **Hostname**, enter the hostname of the database server.
9. For **TCP Port**, enter the port of the database server.
10. Each component that requires a relational database has two corresponding fields: one for the database username and one for the database password. For each set of fields, specify a unique username that can access this specific database on the database server and a password for the provided username.

 **Note:** Ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.


11. Click **Save**.

Step 12: (Optional) Configure Internal MySQL

 **Note:** You only need to configure this section if you have selected one of the **Internal Databases - MySQL** options in the **Databases** section.

To use internal MySQL in High Availability configuration, you define a load balancer rule that lets PAS components send queries a single hostname backed by two redundant proxies. Each proxy then directs query traffic to three MySQL server nodes.

1. Allocate an internal load balancer rule to balance traffic between two static IP addresses. The static IP addresses cannot be within the range that that you have reserved for PAS.
The load balancer rule is separate from the software provided by Pivotal, and you need to define it within your infrastructure.
 - **Make your idle time out long enough to not interrupt long-running queries.** When queries take a long time, the load balancer can time out and interrupt the query.
For example, [AWS's Elastic Load Balancer](#) has a default idle timeout of 60 seconds, so queries that take longer than this duration sever the MySQL connection and return an error.
 - **Configure a healthcheck or monitor, using TCP against port 1936.** This defaults to TCP port `1936`, to maintain backwards compatibility with previous releases. This port is not configurable. Unauthenticated healthchecks against port 3306 may cause the service to become unavailable and require manual intervention to fix.
 - **Configure the load balancer to route traffic for TCP port 3306 to the IPs of all proxy instances on TCP port 3306.**
 - Record the hostname of the load balancer rule and the two static IP addresses.

 **warning:** You must configure a load balancer to achieve complete high availability.

2. From the PAS tile in Ops Manager, Select **Internal MySQL**.
3. In the **MySQL Proxy IPs** field, enter the static IP addresses used by the internal MySQL load balancer rule.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.


A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.

The automated backups functionality works with any S3-compatible file store that can receive your backup files.

MySQL Proxy IPs

MySQL Service Hostname

4. For **MySQL Service Hostname**, enter the IP address or hostname for your load balancer. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.
5. In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
6. In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.
7. (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
8. To prohibit the creation of command line history files on the MySQL nodes, disable the **Allow Command History** checkbox.
9. To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

10. For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the default value is 10 seconds.

Replication canary time period *

30

Replication canary read delay *

20

E-mail address (required) *

Fill in your desired email address

☒ Allow Command History

Cluster Probe Timeout

11. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.
12. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.
 - a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.

13. Enter values for the following fields:
 - **Load Balancer Healthy Threshold**: Specifies the amount of time, in seconds, to wait until declaring the MySQL Proxy instance started. This allows an external load balancer time to register the instance as healthy.
 - **Load Balancer Unhealthy Threshold**: Specifies the amount of time, in seconds, that the MySQL Proxy continues to accept connections before shutting down. During this period, the Healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.
14. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.
15. Click **Save**.

For more information on how to monitor the node health of your MySQL Proxy instances, see [Using the MySQL Proxy](#).

Step 13: Configure File Storage

For production-level PCF deployments on OpenStack, the recommended selection is **External S3-Compatible**.

For more factors to consider when selecting file storage, see [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#).

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External S3 or Ceph Filestore

To use an external S3-compatible filestore for PAS file storage, perform the following steps:

1. In the PAS tile, select **File Storage**.
2. Select the **External S3-Compatible Filestore** option and complete the following fields:
 - Enter the `https://` **URL Endpoint** for your region.
For example, in the **us-west-2** region, enter `https://s3-us-west-2.amazonaws.com/`.
 - If you use an AWS instance profile to manage role information for your filestore, select the **S3 AWS with Instance Profile** checkbox. For more information, see [AWS Identity and Access Management](#) in the AWS documentation.

The screenshot shows a configuration form for S3. At the top, the checkbox 'S3 AWS with Instance Profile' is checked. Below it, there are two text input fields: 'Access Key (required if not using S3 AWS with Instance Profile)' and 'Secret Key (required if not using S3 AWS with Instance Profile)'. The 'Secret Key' field has a 'Secret' label and a 'Cancel' button below it.

- Alternatively, enter the **Access Key** and **Secret Key** of the `pcf-user` you created when configuring AWS for PCF. If you select the **S3 AWS with Instance Profile** checkbox and also enter an **Access Key** and **Secret Key**, the instance profile will overrule the Access Key and Secret Key.
- From the **S3 Signature Version** dropdown, select **V4 Signature**. For more information about S4 signatures, see [Signing AWS API Requests](#) in the AWS documentation.
- For **Region**, enter the region in which your S3 buckets are located. `us-west-2` is an example of an acceptable value for this field.
- Select **Server-side Encryption** to encrypt the contents of your S3 filestore. This option is only available for AWS S3.
- (Optional) If you selected **Server-side Encryption**, you can also specify a **KMS Key ID**. PAS uses the KMS key to encrypt files uploaded to the blobstore. If you do not provide a KMS Key ID, PAS uses the default AWS key. For more information, see [Protecting Data Using Server-Side Encryption with AWS KMS-Managed Keys \(SSE-KMS\)](#).
- Enter names for your S3 buckets:

| Ops Manager Field | Value | Description |
|------------------------|-----------------------|---|
| Buildpacks Bucket Name | pcf-buildpacks-bucket | This S3 bucket stores app buildpacks. |
| Droplets Bucket Name | pcf-droplets-bucket | This S3 bucket stores app droplets. Pivotal recommends that you use a unique bucket name for droplets, but you can also use the same name as above. |
| Packages Bucket Name | pcf-packages-bucket | This S3 bucket stores app packages. Pivotal recommends that you use a unique bucket name for packages, but you can also use the same name as above. |
| Resources Bucket Name | pcf-resources-bucket | This S3 bucket stores app resources. Pivotal recommends that you use a unique bucket name for app resources, but you can also use the same name as above. |

- Configure the following depending on whether your S3 buckets have versioning enabled:
 - **Versioned S3 buckets:** Enable the **Use versioning for backup and restore** checkbox to archive each bucket to a version.
 - **Unversioned S3 buckets:** Disable the **Use versioning for backup and restore** checkbox, and enter a backup bucket name for each active bucket. The backup bucket name must be different from the name of the active bucket it backs up.

☐ Use versioning for backup and restore. (All of the above buckets must have versioning enabled and use the V4 S3 Signature Version).

If versioning is not enabled or supported, you can configure separate buckets below for backups. More information at <https://docs.pivotal.io/pivotalcf/2-1/customizing/backup-restore/backup-pcf-bbr.html>.

Backup Region

Backup Buildpacks Bucket Name

Backup Droplets Bucket Name

Backup Packages Bucket Name

For more information about setting up external S3 blobstores, see the [Backup and Restore with External Blobstores](#) topic in the Cloud Foundry documentation.

3. Click **Save**.

Note: For more information regarding AWS S3 Signatures, see the [Authenticating Requests](#) topic in the AWS documentation.

Step 14: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

Note: The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

- ☒ No
☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging


☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration


Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.

 **Note:** The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.

 **Note:** Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 15: (Optional) Customize Apps Manager

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

Add

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑
- ▶ Docs 🗑
- ▶ Tools 🗑

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

4. Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
5. Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
6. Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
7. Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
8. The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
9. The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 16: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret

Save

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

Note: If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 17: (Optional) Configure App Autoscaler

To use App Autoscaler, you must create an instance of the service and bind it to an app. To create an instance of App Autoscaler and bind it to an app, see [Set Up App Autoscaler](#) in the *Scaling an Application Using App Autoscaler* topic.

- Click **App Autoscaler**.

Configure the App Autoscaler

Autoscaler Instance Count (min: 1) *

Autoscaler API Instance Count (min: 1) *

Metric Collection Interval (min: 60, max: 3600) (min: 60, max: 3600) *

Scaling Interval (min: 15, max: 120) (min: 15, max: 120) *

☐ Verbose Logging

☐ Disable API Connection Pooling

☒ Enable Notifications

- Review the following settings:

- Autoscaler Instance Count:** How many instances of the App Autoscaler service you want to deploy. The default value is `3`. For high availability, set this number to `3` or higher. You should set the instance count to an odd number to avoid split-brain scenarios during leadership elections. Larger environments may require more instances than the default number.
- Autoscaler API Instance Count:** How many instances of the App Autoscaler API you want to deploy. The default value is `1`. Larger environments may require more instances than the default number.
- Metric Collection Interval:** How many seconds of data collection you want App Autoscaler to evaluate when making scaling decisions. The minimum interval is 60 seconds, and the maximum interval is 3600 seconds. The default value is `120`. Increase this number if the metrics you use in your scaling rules are emitted less frequently than the existing Metric Collection Interval.
- Scaling Interval:** How frequently App Autoscaler evaluates an app for scaling. The minimum interval is 15 seconds, and the maximum interval is 120 seconds. The default value is `35`.
- Verbose Logging** (checkbox): Enables verbose logging for App Autoscaler. Verbose logging is disabled by default. Select this checkbox to see more detailed logs. Verbose logs show specific reasons why App Autoscaler scaled the app, including information about minimum and maximum instance limits, App Autoscaler's status. For more information about App Autoscaler logs, see [App Autoscaler Events and Notifications](#).
- Disable API Connection Pooling:** API connection pooling increases performance by reducing the cost associated with establishing new connections. If you do not want to keep connections open for reuse, select this option.

3. Click **Save**.

Step 18: Configure Cloud Controller

1. Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
 ☒ Disable

Save

2. Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

3. CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

4. Click **Save**.

Step 19: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

1. Select **Smoke Tests**.
2. If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

- ☐ Temporary space within the system organization (This is deleted after smoke tests finish.)
- ☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.

Step 20: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

Note: Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.

Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.

Whitelist for non-RFC-1918 Private Networks *

allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.

CF CLI Connection Timeout

15

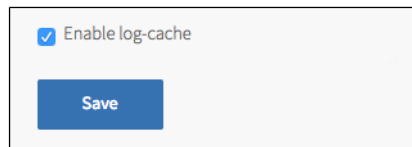
2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PASTopic*.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

⚠ warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 21: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

💡 Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.

- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

💡 Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.

- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.
- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

Step 22: Enable Traffic to Private Subnet

Unless you are using your own load balancer, you must enable traffic flow to the OpenStack private subnet as follows. Give each HAProxy a way of routing traffic into the private subnet by providing public IP addresses as floating IP addresses.

1. Click **Resource Config**.

Resource Config

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|-------------------------------|--------------|----------------------|---|----------------|-------------------------------------|
| Consul | 1 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| NATS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| File Storage | Automatic: 1 | Automatic: 100 GB | Automatic: medium.mem (cpu: 1, ram: 6 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Proxy | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| MySQL Server | 1 | Automatic: 100 GB | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 64 GB) | | <input checked="" type="checkbox"/> |
| Backup Prepare Node | Automatic: 1 | Automatic: 200 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego BBS | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| UAA | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller | 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| HAProxy | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Router | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-web-elb | <input checked="" type="checkbox"/> |
| MySQL Monitor | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Clock Global | Automatic: 1 | None | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB) | | <input checked="" type="checkbox"/> |
| Cloud Controller Worker | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego Brain | 1 | Automatic: 1 GB | Automatic: small (cpu: 1, ram: 2 GB, disk: 8 GB) | pcf-ssh-elb | <input checked="" type="checkbox"/> |
| Diego Cell | 1 | None | Automatic: xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB) | | <input checked="" type="checkbox"/> |
| Loggregator Trafficcontroller | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Adapter | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Syslog Scheduler | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Doppler Server | 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| TCP Router | 0 | Automatic: 1 GB | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | pcf-tcp-elb | <input checked="" type="checkbox"/> |
| CredHub | Automatic: 0 | None | Automatic: large (cpu: 2, ram: 8 GB, disk: 16 GB) | | <input checked="" type="checkbox"/> |

Save

2. Enter one or more IP addresses in **Floating IPs** for each HAProxy.

3. (Optional) If you have enabled the TCP Routing feature, enter one or more IP addresses in **Floating IPs** column for each TCP Router.

4. Click **Save**.

Step 23: (Optional) Scale Down and Disable Resources

Note: The **Resource Config** pane has fewer VMs if you are installing the [Small Footprint Runtime](#).

Note: The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to **3** instances and scale the **Control** VM to **2** instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by navigating to the **Resource Config** section and using the dropdowns under **Instances** for each job.

By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding system-provided resources in Ops Manager to reduce costs and administrative overhead.

To disable specific VMs in Ops Manager, do the following:

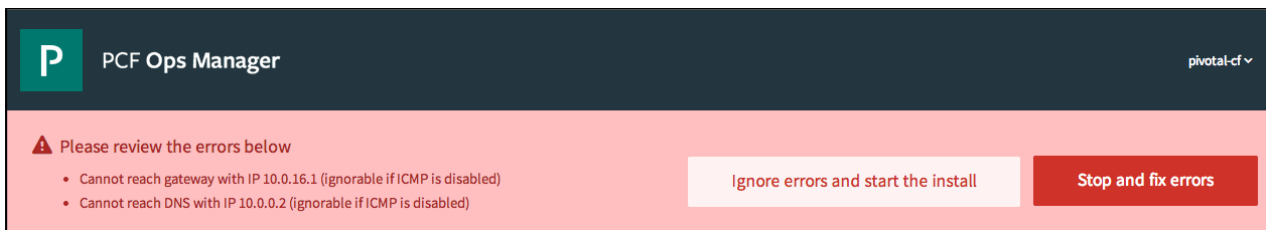
1. Click **Resource Config**.
2. If you configured PAS to use an external S3-compatible filestore, enter **0** in **Instances** in the **File Storage** field.
3. If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:

- MySQL Proxy: Enter in **Instances**.
- MySQL Server: Enter in **Instances**.
- MySQL Monitor: Enter in **Instances**.

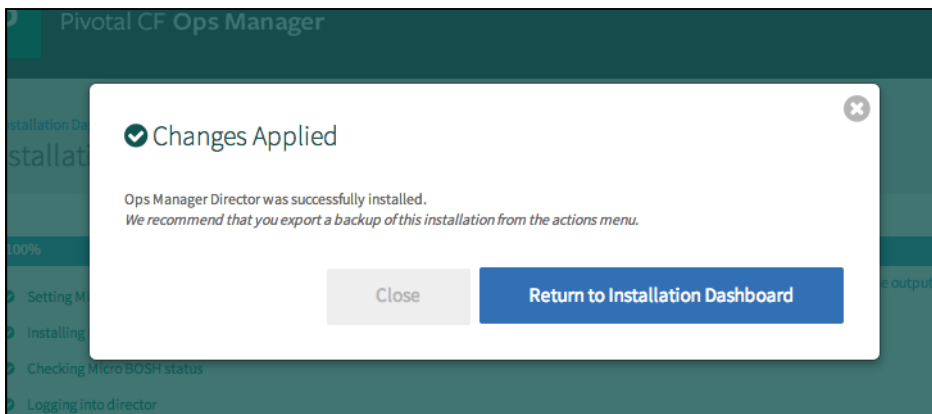
- If you disabled TCP routing, enter **Instances** in the **TCP Router** field.
- If you are not using HAProxy, enter **Instances** in the **HAProxy** field.
- Click **Save**.

Step 24: Complete PAS Installation

- Click the **Installation Dashboard** link to return to the Installation Dashboard.
- Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.



- PAS installs. The image shows the **Changes Applied** message that Ops Manager displays when the installation process successfully completes.



Return to [Installing Pivotal Cloud Foundry on OpenStack](#).

PCF on vSphere Requirements

Page last updated:

This guide describes how to install [Pivotal Cloud Foundry](#) (PCF) on vSphere.

If you experience a problem while following the steps below, refer to the [Known Issues](#) topics or to [Diagnosing Problems in PCF](#).

General Requirements

The following are general requirements for deploying and managing a PCF deployment with Ops Manager and Pivotal Application Service (PAS):

- A wildcard DNS record that points to your router or load balancer. Alternatively, you can use a service such as xip.io. For example, `203.0.113.0.xip.io`.
 - PAS gives each application its own hostname in your app domain.
 - With a wildcard DNS record, every hostname in your domain resolves to the IP address of your router or load balancer, and you do not need to configure an A record for each app hostname. For example, if you create a DNS record `*.example.com` pointing to your load balancer or router, every application deployed to the `example.com` domain resolves to the IP address of your router.
- At least one wildcard TLS certificate that matches the DNS record you set up above, `*.example.com`.
- Sufficient IP allocation:
 - One static IP address for either HAProxy or one of your gorouters
 - One static IP address for each job in the Ops Manager tile. See the Resource Config pane for each tile for a full list.
 - One static IP address for each job listed below:
 - Consul
 - NATS
 - File Storage
 - MySQL Proxy
 - MySQL Server
 - Backup Prepare Node
 - HAProxy
 - Router
 - MySQL Monitor
 - Diego Brain
 - TCP Router
 - One IP for each VM instance created by the service.
 - An additional IP address for each compilation worker. So the formula for total IPs needed is

$$\text{IPs needed} = \text{static IPs} + \text{VM instances} + \text{compilation workers}$$



Note: Pivotal recommends that you allocate at least 36 dynamic IP addresses when deploying Ops Manager and PAS. BOSH requires additional dynamic IP addresses during installation to compile and deploy VMs, install PAS, and connect to services.


- One or more NTP servers if not already provided by your IaaS.
- (**Recommended**) A network without DHCP available for deploying the PAS VMs.




Note: If you have DHCP, refer to the [Troubleshooting Guide](#) to avoid issues with your installation.

- (**Optional**) External storage. When you deploy PCF, you can select internal file storage or external file storage, either network-accessible or IaaS-provided, as an option in the PAS tile. Pivotal recommends using external storage whenever possible. See [Configure File Storage](#) for a discussion of how file storage location affects platform performance and stability during upgrades.
- (**Optional**) External databases. When you deploy PCF, you can select internal or external databases for the BOSH Director and for PAS. Pivotal recommends using external databases in production deployments. An external database must be configured to use the UTC timezone.
- (**Optional**) External user stores. When you deploy PCF, you can select a SAML user store for Ops Manager or a SAML or LDAP user store for PAS, to integrate existing user accounts.
- The most recent version of the [Cloud Foundry Command Line Interface](#) (cf CLI).

vSphere Requirements

 **Note:** If you are using the Cisco Nexus 1000v Switch, refer to the [Using the Cisco Nexus 1000v Switch with Ops Manager](#) topic for more information.

 **Note:** When installing Ops Manager on a vSphere environment with multiple ESXi hosts, you must use network-attached or shared storage devices. Local storage devices do not support sharing across multiple ESXi hosts.

Minimum Resource Requirements for PCF Deployment with Pivotal Application Service

The following are the minimum resource requirements for maintaining a [Pivotal Cloud Foundry](#) (PCF) deployment with Ops Manager and Pivotal Application Service (PAS) on vSphere:

- vSphere v6.7*, v6.5, v6.0, or v5.5
- Disk space: 2 TB recommended
- Memory: 120 GB
- Two public IP addresses: One for PAS and one for Ops Manager
- vCPU cores: 80
- Overall CPU: 28 GHz
- vSphere editions: standard and above
- Ops Manager must have HTTPS access to vCenter and ESX hosts on TCP port 443.
- A configured vSphere cluster:
 - If you enable vSphere DRS (Distributed Resource Scheduler) for the cluster, you must set the Automation level to **Partially automated** or **Fully automated**. If you set the Automation level to **Manual**, the BOSH automated installation will fail with a `power_on_vm` error when BOSH attempts to create virtual machines (VMs).
 - Disable hardware virtualization if your vSphere hosts do not support VT-X/EPT. If you are unsure whether the VM hosts support VT-x/EPT, you should disable this setting. If you leave this setting enabled and the VM hosts do not support VT-x/EPT, then each VM requires manual intervention in vCenter to continue powering on without the Intel virtualized VT-x/EPT. Refer to the vCenter help topic at [Configuring Virtual Machines > Setting Virtual Processors and Memory > Set Advanced Processor Options](#) for more information.
- If you configure an external load balancer, an HTTP keepalive connection timeout greater than five seconds

* Use Ops Manager v2.2.5 or later to deploy PCF on vSphere v6.7.

 **Note:** If you are deploying PCF behind a firewall, see the [Preparing Your Firewall for Deploying Pivotal Cloud Foundry](#) topic.

Minimum Resource Requirements for PCF Deployment with Small Footprint PAS

The following are the minimum resource requirements for maintaining a PCF deployment with Ops Manager and Small Footprint PAS on vSphere:

- 1 vSphere cluster/1 AZ
- 2 resource pools: 1 for NSX-T components and 1 for PAS or PKS
- 3 hosts minimum for vSphere HA (4 hosts for vSphere VSAN)
- Shared storage/VSAN
- 1 NSX Manager
- 3 NSX controllers
- 4 large edge VMs in a cluster
- PCF: Ops Manager, the BOSH Director, and Small Footprint PAS

Instance Number and Scaling Requirements

By default, PAS deploys the number of VM instances required to run a highly available configuration of PCF. If you are deploying a test or sandbox PCF that does not require HA, then you can scale down the number of instances in your deployment.

For information about the number of instances required to run a minimal, non-HA PCF deployment, see [Scaling PAS](#).

vSphere Service Account Requirements


Ops Manager requires read/write permissions to the datacenter level of the [vSphere Inventory Hierarchy](#) to successfully install. Pivotal recommends defining a custom role for the service account that has all privileges for all objects in the datacenter, including propagating privileges to children.

For a complete list of the minimum required vSphere privileges, see the [vSphere Service Account Requirements](#) topic.

Since Ops Manager passes all required credentials through to BOSH, you only need one service account with the required vSphere privileges to complete the installation. Setting up separate service accounts for Ops Manager and BOSH is not necessary or recommended.

 **Note:** You can also apply the default [VMware Administrator System Role](#) to the service account to achieve the appropriate permission level.

vSphere Security Documents

- [vSphere Security guide \(PDF\)](#) 
This guide contains best practices for securing and managing a vSphere installation.


Step 1: Install Ops Manager

Complete the following procedures to install Ops Manager on vSphere:

1. [Deploying Ops Manager to vSphere](#)
2. [Configuring BOSH Director on vSphere](#)

(Optional) Step 2: Install the IPsec Add-on

The PCF IPsec add-on secures network traffic within a PCF deployment and provides internal system protection if a malicious actor breaches your firewall. See the [Securing Data in Transit with the IPsec Add-on](#) topic for installation instructions.

 **Note:** You must install the PCF IPsec add-on before installing any other tiles to enable the IPsec functionality. Pivotal recommends installing IPsec immediately after Ops Manager, and before installing the PAS tile.

(Optional) Step 3: Install the NSX-T Tile

The NSX-T tile provides a single network for containers, VMs, and other entities. It enables NSX to enforce C2C policy and operators to configure additional policies through NSX Manager.

- You must install the NSX-T tile after you install or upgrade the BOSH Director tile.
- You must install the NSX-T tile before you install or upgrade the PAS tile.

See the [NSX-T Container Plug-In for Kubernetes and Cloud Foundry - Installation and Administration Guide](#) for more information.

Step 4: Install PAS


To install PAS on vSphere, perform the procedures in the [Deploying PAS on vSphere](#) topic.

Step 5: Create New User Accounts

Once you have successfully deployed PCF, add users to your account. Refer to the [Creating New PAS User Accounts](#) topic for more information.

Step 6: Target Your Deployment

Use the Cloud Foundry Command Line Interface (cf CLI) to target your deployment. If you have not installed the cf CLI, follow the instructions in [Installing the cf CLI](#). For more information about the cf CLI, see [Getting Started with the cf CLI](#).

 **Note:** To obtain the UAA admin name and password, refer to PAS **Credentials** in Ops Manager. You can also use the user that you created in Apps Manager, or create another user with the `create-user` command.

Additional Configuration

See the following topics for additional configuration information:

- [Deploying PAS with NSX-T Networking](#)
- [Provisioning a Virtual Disk in vSphere](#)
- [Using the Cisco Nexus 1000v Switch with Ops Manager](#)
- [Using BOSH Resurrector and vSphere HA](#)
- [Configuring SSL Termination for vSphere Deployments](#)
- [Availability Zones in vSphere](#)
- [Updating NSX Security Group and Load Balancer Information](#)

vSphere Service Account Requirements

Page last updated:

This topic describes the minimum privileges required by the vSphere BOSH CPI. A vSphere admin must grant the following privileges to the vSphere service account that Pivotal Cloud Foundry (PCF) uses to manage vSphere resources.

The PCF account needs privileges at both the vCenter server level and the Datacenter level. See [Hierarchical Inheritance of Permissions](#) in the VMware documentation for how permission levels and inheritance work in vSphere.

vCenter-Level Privileges

Ops Manager assigns custom attributes to the virtual machines (VMs) it deploys to identify BOSH releases and job index information about each VM. vCenter APIs require vCenter server level access to manage these custom attributes.

The following table summarizes the privileges that a PCF account requires at the vCenter Server instance level. Some of these privileges are inherited, and others must be granted by a vCenter admin:

| Object | Privilege (UI) | Privilege (API) |
|------------------------|--------------------------|---------------------------|
| Role | Read-only | System.Anonymous |
| | | System.Read |
| | | System.View |
| Global | Manage custom attributes | Global.ManageCustomFields |
| | Register Extensions | Extension.Register |
| Profile-Driven Storage | Profile-driven Storage | StorageProfile.Update |
| | | StorageProfile.View |

Datacenter-Level Privileges

The following privileges must be set at the data center level:

| Object | Privilege (UI) | Privilege (API) |
|-----------|---------------------------|--------------------------|
| Datastore | Low level file operations | Datastore.FileManagement |
| Network | Assign network | Network.Assign |

Folder and Datastore-Level Privileges

You must grant the following privileges on any entities in a datacenter where you will deploy PCF:

Datastore Object

| Privilege (UI) | Privilege (API) |
|------------------------------|-------------------------------------|
| Allocate space | Datastore.AllocateSpace |
| Browse datastore | Datastore.Browse |
| Remove file | Datastore.DeleteFile |
| Update virtual machine files | Datastore.UpdateVirtualMachineFiles |

Folder Object

Ops Manager creates a folder for VMs, stemcells, and persistent disks during installation. The folder contents change frequently as Ops Manager applies

changes.

| Privilege (UI) | Privilege (API) |
|----------------|-----------------|
| Delete folder | Folder.Delete |
| Create folder | Folder.Create |
| Move folder | Folder.Move |
| Rename folder | Folder.Rename |

Inventory Service Object

| Privilege (UI) | Privilege (API) |
|--------------------------------------|------------------------------------|
| vSphere Tagging > Create vSphere Tag | InventoryService.Tagging.CreateTag |
| vSphere Tagging > Delete vSphere Tag | InventoryService.Tagging.EditTag |
| vSphere Tagging > Edit vSphere Tag | InventoryService.Tagging.DeleteTag |

Resource Object

When using [vAppImport](#) to clone a VM, BOSH requires the resource migration privileges to create a new, powered-off VM based on a given stemcell. BOSH migrates the VM to the destination datastore, where Ops Manager deploys the VM and powers it on.

| Privilege (UI) | Privilege (API) |
|---|-------------------------|
| Assign virtual machine to resource pool | Resource.AssignVMToPool |
| Migrate powered off virtual machine | Resource.ColdMigrate |
| Migrate powered on virtual machine | Resource.HotMigrate |

Virtual Machine Object

Configuration

| Privilege (UI) | Privilege (API) |
|-----------------------------|---------------------------------------|
| Add existing disk | VirtualMachine.Config.AddExistingDisk |
| Add new disk | VirtualMachine.Config.AddNewDisk |
| Add or remove device | VirtualMachine.Config.AddRemoveDevice |
| Advanced | VirtualMachine.Config.AdvancedConfig |
| Change CPU count | VirtualMachine.Config.CPUCount |
| Change resource | VirtualMachine.Config.Resource |
| Configure managedBy | VirtualMachine.Config.ManagedBy |
| Disk change tracking | VirtualMachine.Config.ChangeTracking |
| Disk lease | VirtualMachine.Config.DiskLease |
| Display connection settings | VirtualMachine.Config.MksControl |
| Extend virtual disk | VirtualMachine.Config.DiskExtend |
| Memory | VirtualMachine.Config.Memory |
| Modify device settings | VirtualMachine.Config.EditDevice |
| Raw device | VirtualMachine.Config.RawDevice |
| Reload from path | VirtualMachine.Config.ReloadFromPath |
| Remove disk | VirtualMachine.Config.RemoveDisk |
| Rename | VirtualMachine.Config.Rename |
| Reset guest information | VirtualMachine.Config.ResetGuestInfo |

| | |
|----------------------------------|--|
| Set annotation | VirtualMachine.Config.Annotation |
| Settings | VirtualMachine.Config.Settings |
| Swapfile placement | VirtualMachine.Config.SwapPlacement |
| Unlock virtual machine | VirtualMachine.Config.Unlock |
| Upgrade virtual machine hardware | VirtualMachine.Config.UpgradeVirtualHardware |

Guest Operations

| Privilege (UI) | Privilege (API) |
|-----------------------------------|--|
| Guest Operation Program Execution | VirtualMachine.GuestOperations.Execute |
| Guest Operation Modifications | VirtualMachine.GuestOperations.Modify |
| Guest Operation Queries | VirtualMachine.GuestOperations.Query |

Interaction

| Privilege (UI) | Privilege (API) |
|--|--|
| Answer question | VirtualMachine.Interact.AnswerQuestion |
| Configure CD media | VirtualMachine.Interact.SetCDMedia |
| Device connection | VirtualMachine.Interact.DeviceConnection |
| Guest operating system management by VIX API | VirtualMachine.Interact.GuestControl |
| Power off | VirtualMachine.Interact.PowerOff |
| Power on | VirtualMachine.Interact.PowerOn |
| Reset | VirtualMachine.Interact.Reset |
| Suspend | VirtualMachine.Interact.Suspend |
| VMware Tools install | VirtualMachine.Interact.ToolsInstall |

Inventory

| Privilege (UI) | Privilege (API) |
|----------------------|---|
| Create from existing | VirtualMachine.Inventory.CreateFromExisting |
| Create new | VirtualMachine.Inventory.Create |
| Move | VirtualMachine.Inventory.Move |
| Remove | VirtualMachine.Inventory.Delete |

Provisioning

When cloning a stemcell, BOSH sets custom specifications, such as hostnames and network configurations, based on the stemcell operating system.

The VM download privilege allows BOSH to modify files within a VM, including links between VMs and persistent disks. When vMotion migrates disks in vSphere, BOSH uses these links to maintain the connections between VMs and their persistent disks.

| Privilege (UI) | Privilege (API) |
|------------------------------------|--|
| Allow disk access | VirtualMachine.Provisioning.DiskRandomAccess |
| Allow read-only disk access | VirtualMachine.Provisioning.DiskRandomRead |
| Allow virtual machine download | VirtualMachine.Provisioning.GetVmFiles |
| Allow virtual machine files upload | VirtualMachine.Provisioning.PutVmFiles |
| Clone template | VirtualMachine.Provisioning.CloneTemplate |
| Clone virtual machine | VirtualMachine.Provisioning.Clone |
| Customize | VirtualMachine.Provisioning.Customize |

| | |
|------------------------------------|---|
| Deploy template | VirtualMachine.Provisioning.DeployTemplate |
| Mark as template | VirtualMachine.Provisioning.MarkAsTemplate |
| Mark as virtual machine | VirtualMachine.Provisioning.MarkAsVM |
| Modify customization specification | VirtualMachine.Provisioning.ModifyCustSpecs |
| Promote disks | VirtualMachine.Provisioning.PromoteDisks |
| Read customization specifications | VirtualMachine.Provisioning.ReadCustSpecs |

Snapshot Management

Before Ops Manager deploys a new VM, it uses a snapshot to clone the stemcell image to the destination.

| Privilege (UI) | Privilege (API) |
|-----------------|---------------------------------------|
| Create snapshot | VirtualMachine.State.CreateSnapshot |
| Remove snapshot | VirtualMachine.State.RemoveSnapshot |
| Rename snapshot | VirtualMachine.State.RenameSnapshot |
| Revert snapshot | VirtualMachine.State.RevertToSnapshot |

vApp Object

These privileges must be set at the resource pool level. `VApp.ApplicationConfig` is required when attaching or detaching persistent disks.

| Privilege (UI) | Privilege (API) |
|--------------------------------|------------------------|
| Import | VApp.Import |
| vApp application configuration | VApp.ApplicationConfig |

Deploying Ops Manager on vSphere

Page last updated:

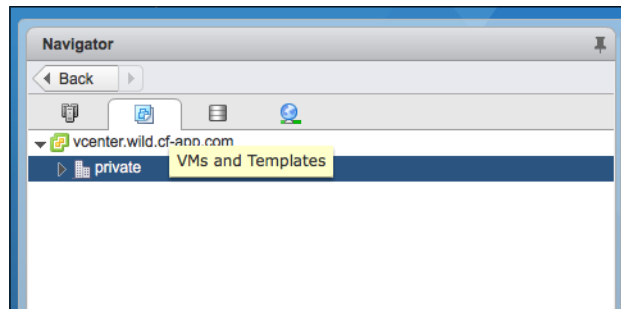
This topic provides instructions for deploying Ops Manager on VMware vSphere.

Warning: If you are installing Pivotal Container Service (PKS) on vSphere with NSX-T integration, follow the instructions in [Deploying Ops Manager with NSX-T for PKS](#) instead of performing the steps provided in this topic.

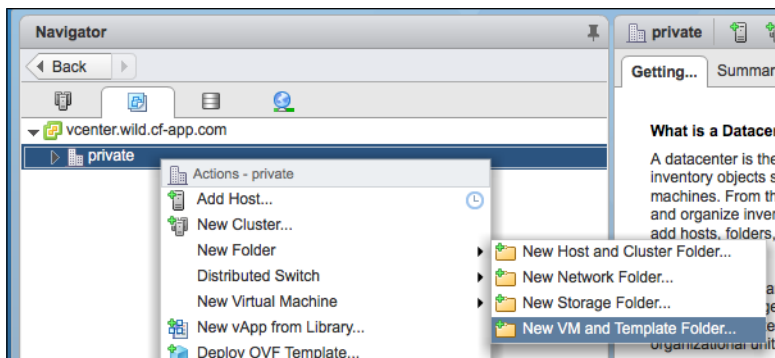
Note: The instructions in this topic are based on vSphere 6.5.

Deploy Ops Manager

1. Download Pivotal Cloud Foundry Ops Manager for vSphere from [Pivotal Network](#).
2. Log in to vCenter.

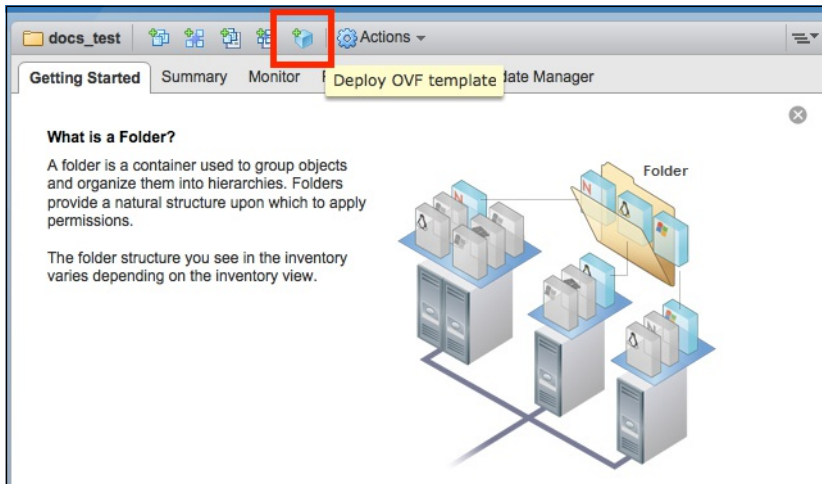


3. In the **Navigator**, click the **VMs and Templates** tab.
4. Right click your datacenter.
 - a. Select **New Folder > New VM and Template Folder**.



- b. Name the folder `pivotal_cf`.
 - c. Click **Ok**.
5. Click your newly created folder.
 6. Click the **Deploy OVF Template** icon and complete the following steps:

Note: The vSphere Web Client requires Flash. If the **Deploy OVF Template** button is unresponsive, ensure that you have Flash enabled in your browser and reload the page.



a. Select template

- i. Click **Browse** and select the `.ova` file that you downloaded from Pivotal Network.
- ii. Click **Next**.

b. Select name and location

- i. Name the virtual machine and click **Next**.

Note: The selected folder is the one that you created.

c. Select a resource

- i. Select the resource that you want to use to launch the VM and click **Next**.

Note: Hardware virtualization must be off if your vSphere host does not support VT-x/EPT.

d. Review Details

- i. Verify the template details and click **Next**.

e. Select storage

- i. Select a disk format. For information about disk formats, see [Provisioning a Virtual Disk](#).

warning: Ops Manager requires a Director VM with at least 8 GB memory.

- ii. Select a storage destination.
- iii. Click **Next**.

f. Select networks

- i. Select a network from the drop down list and click **Next**.

g. Customize template

- i. In the **Admin Password** field, enter a default password for the account with the username `ubuntu`. Alternatively, you can enter a pre-existing SSH key value in the **Public SSH Key** field.

Note: You must specify a default password, an SSH key, or both. If you do not have either of these fields configured, Ops Manager will not boot up.

- ii. Complete the remaining network information and passwords for the Ops Manager VM admin user.

Note: Record this network information. The IP Address will be the location of the Ops Manager interface.

- iii. Click **Next**.

h. Ready to complete

- i. Review the configuration data and click **Finish**.
7. With the VM selected, click **Actions > Power > Power On**. Once the VM boots, the interface is available at the IP address that you specified.



Note: It is normal to experience a brief delay before the interface is accessible while the web server and VM start up.

8. Create a DNS entry for the IP address that you used for Ops Manager. You must use this fully qualified domain name when you log in to Ops Manager as described in the [Set Up Ops Manager](#) section of *Configuring BOSH Director on vSphere*.

Next Steps

After you complete this procedure, follow the instructions in [Configuring BOSH Director on vSphere](#).

[Return to the Installing Pivotal Cloud Foundry Guide](#) [↗](#)

Configuring BOSH Director on vSphere

Page last updated:

This topic describes how to configure the BOSH Director tile for VMware vSphere. You can also perform the procedures in this topic using the Ops Manager API. For more information, see [Using the Ops Manager API](#).

⚠ warning: If you are installing Pivotal Container Service (PKS) on vSphere with NSX-T integration, follow the instructions in [Configuring BOSH Director with NSX-T for PKS](#) instead of performing the steps provided in this topic.

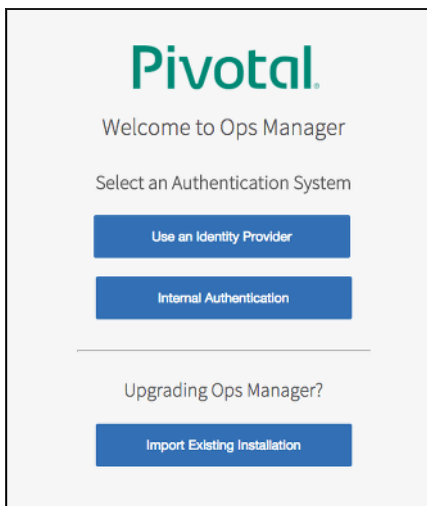
Prerequisites

Before you begin this procedure, you must complete all steps in [Deploying Ops Manager on vSphere](#).

💡 Note: Pivotal strongly recommends installing PAS and PKS on separate instances of Ops Manager for security reasons. For more information, see [PAS and PKS Deployments with Ops Manager](#).

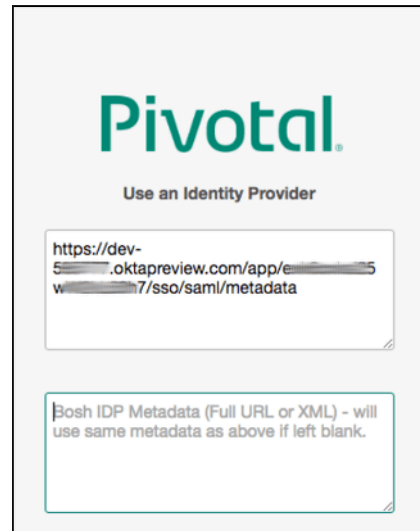
Step 1: Set Up Ops Manager

1. In a web browser, navigate to the fully qualified domain of your Ops Manager.
2. When Ops Manager starts for the first time, you must choose one of the following:
 - [Use an Identity Provider](#): If you choose **Use an Identity Provider**, an external identity server maintains your user database.
 - [Internal Authentication](#): If you choose **Internal Authentication**, Ops Manager maintains your user database.



Use an Identity Provider

1. Log in to your IdP console and download the IdP metadata XML. Optionally, if your IdP supports metadata URL, you can copy the metadata URL instead of the XML.



2. Copy the IdP metadata XML or URL to the Ops Manager **Use an Identity Provider** login page.

Note: The same IdP metadata URL or XML is applied for the BOSH Director. If you use a separate IdP for BOSH, copy the metadata XML or URL from that IdP and enter it into the BOSH IdP Metadata text box in the Ops Manager login page.

3. Enter values for the fields listed below. Failure to provide values in these fields results in a `500` error.

Note: These attributes are case-sensitive.

- **SAML admin group:** Enter the name of the SAML group that contains all Ops Manager administrators.
- **SAML groups attribute:** Enter the groups attribute tag name with which you configured the SAML server.

4. Enter your **Decryption passphrase**. Read the **End User License Agreement**, and select the checkbox to accept the terms.

5. Your Ops Manager login page appears. Enter your username and password. Click **Login**.

6. Download your SAML Service Provider metadata (SAML Relying Party metadata) by navigating to the following URLs:

- **6a.** Ops Manager SAML service provider metadata: `https://OPS-MAN-FQDN:443/uaa/saml/metadata`
- **6b.** BOSH Director SAML service provider metadata: `https://BOSH-IP-ADDRESS:8443/saml/metadata`

Note: To retrieve your `BOSH-IP-ADDRESS`, navigate to the **BOSH Director** tile > **Status** tab. Record the **BOSH Director** IP address.

7. Configure your IdP with your SAML Service Provider metadata. Import the Ops Manager SAML provider metadata from Step 6a above to your IdP. If your IdP does not support importing, provide the values below.

- **Single sign on URL:** `https://OPS-MAN-FQDN:443/uaa/saml/SSO/alias/OPS-MAN-FQDN`
- **Audience URI (SP Entity ID):** `https://OP-MAN-FQDN:443/uaa`
- **Name ID:** Email Address
- SAML authentication requests are always signed

8. Import the BOSH Director SAML provider metadata from Step 6b to your IdP. If the IdP does not support an import, provide the values below.

- **Single sign on URL:** `https://BOSH-IP:8443/saml/SSO/alias/BOSH-IP`
- **Audience URI (SP Entity ID):** `https://BOSH-IP:8443`
- **Name ID:** Email Address
- SAML authentication requests are always signed

9. Return to the **BOSH Director** tile, and continue with the configuration steps below.

Use Internal Authentication

1. When redirected to the **Internal Authentication** page, you must complete the following steps:

- Enter a **Username**, **Password**, and **Password confirmation** to create an Admin user.
- Enter a **Decryption passphrase** and the **Decryption passphrase confirmation**. This passphrase encrypts the Ops Manager datastore, and is not

recoverable.

- If you are using an **HTTP proxy** or **HTTPS proxy**, follow the instructions in [Configuring Proxy Settings for the BOSH CPI](#).
- Read the **End User License Agreement**, and select the checkbox to accept the terms.
- Click **Setup Authentication**.

Step 2: vCenter Configs Page

1. Log in to Ops Manager with the Admin username and password that you created in the previous step.
2. Click the **BOSH Director** tile.
3. Select **vCenter Config**. Configure the one or more vCenters that host your PCF foundation. The following image shows the **vCenter Config** pane.

✓ vCenter Configs

✓ Director Config

✓ Create Availability Zones

✓ Create Networks

✓ Assign AZs and Networks

✓ Security

✓ Syslog

✓ Resource Config

vCenter Config

Add vCenter Config

Name*

first-vcenter

vCenter Host*

10.87.41.6

vCenter Username*

opsmgr@vsphere.local

vCenter Password*

Change

Datacenter Name*

six

Virtual Disk Type*

thin

Ephemeral Datastore Names (comma delimited)*

freenas-smurfs

NOTE: Removing an Ephemeral Datastore after an initial deploy can result in a system outage and/or data loss.

Persistent Datastore Names (comma delimited)*

freenas-smurfs

NOTE: Removing a Persis

n a system outage and/or data loss.

☒ Standard vCenter
 ☐ NSX Networking

NSX Mode*

☒ NSX-V
 ☐ NSX-T

NSX Address*

NSX Username*

NSX Password*

NSX CA Cert

VM Folder*

concourse-bulldog_specs_vms

Template Folder*

concourse-bulldog_specs_templates


Disk path Folder*

concourse-bulldog_specs_disk

Save

4. Complete the fields on the vCenter Config pane as follows:


- **Name:** A name that you provide for your vCenter configuration. This field is used to identify the datacenter configuration in Ops Manager if you are configuring multiple datacenters.
- **vCenter Host:** The hostname of the vCenter that manages ESXi/vSphere.
- **vCenter Username:** A vCenter username with create and delete privileges for virtual machines (VMs) and folders.
- **vCenter Password:** The password for the vCenter user specified above.
- **Datacenter Name:** The name of the datacenter as it appears in vCenter.
- **Virtual Disk Type:** The Virtual Disk Type to provision for all VMs. For guidance about the virtual disk type to select, see [Provisioning a Virtual Disk in vSphere](#).

 **Note:** The following fields do not allow whitespace. Including whitespace characters in datastore or datastore folder names causes an error.

- **Ephemeral Datastore Names (comma delimited):** The names of the datastores that store ephemeral VM disks deployed by Ops Manager.
- **Persistent Datastore Names (comma delimited):** The names of the datastores that store persistent VM disks deployed by Ops Manager.
- **VM Folder:** The vSphere datacenter folder where Ops Manager places VMs. This defaults to `pcf_vms`.
- **Template Folder:** The vSphere datacenter folder where Ops Manager places VMs. This defaults to `pcf_templates`.
- **Disk path Folder:** The vSphere datastore folder where Ops Manager creates attached disk images. This defaults to `pcf_disk`. You must not nest this folder.

5. Select a network configuration from one of the following:

- **Standard vCenter Networking:** This is the default option when upgrading Ops Manager.
- **NSX Networking:** Select this option to enable VMware NSX Network Virtualization. Configure NSX networking by entering the following information:
 - **NSX Mode:** Select either **NSX-V** or **NSX-T**.


 **Note:** If you want to configure NSX Networking for PKS, you must select **NSX-T**. For more information about NSX Networking for PKS, see the [Configure vCenter for PKS](#) section of *Configuring BOSH Director with NSX-T for PKS*.

- **NSX Address:** The address of the NSX manager.
- **NSX Username:** The username to connect to the NSX manager.
- **NSX Password:** The password for the username specified above.
- **NSX CA Cert:** A CA certificate in PEM format that authenticates to the NSX server. If the NSX Manager generated a self-signed certificate, use the following command to retrieve the CA certificate using OpenSSL:

```
openssl s_client -showcerts -connect NSX-MANAGER-ADDRESS:443 < /dev/null 2> /dev/null | openssl x509
```

Where `NSX-MANAGER-ADDRESS` is the address of the NSX manager.

6. Click **Save**.

 **Note:** After your initial deployment, you cannot edit the VM Folder, Template Folder, and Disk path Folder names.

7. (Optional) Click **Add vCenter Config** toward the top of the form to configure additional vCenters. Once you click **Save**, your multiple vCenter Configs are listed in the **vCenter Configs** pane. For more information about multiple vCenter configs, see [Managing Multiple Data Centers](#).

Step 3: Director Config Page

1. Select **Director Config**.

Director Config

NTP Servers (comma delimited)*

JMX Provider IP Address

Bosh HM Forwarder IP Address

☐ Enable VM Resurrecter Plugin

☐ Enable Post Deploy Scripts

☐ Recreate all VMs


This will force BOSH to recreate all VMs on the next deploy. Persistent disk will be preserved

☐ Enable bosh deploy retries


This will attempt to re-deploy a failed deployment up to 5 times.

☐ Keep Unreachable Director VMs


- In the **NTP Servers (comma delimited)** field, enter your NTP server addresses.

 **Note:** The NTP server configuration only updates after VM recreation. Ensure that you select the **Recreate all VMs** checkbox if you modify the value of this field.


- Leave the **JMX Provider IP Address** field blank.

 **Note:** Starting in PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. If you continue to use PCF JMX Bridge to consume these component metrics outside of the Firehose, you may receive duplicate data. To prevent this, leave the **JMX Provider IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#) in the PCF v2.0 Release Notes.

- Leave the **Bosh HM Forwarder IP Address** field blank.

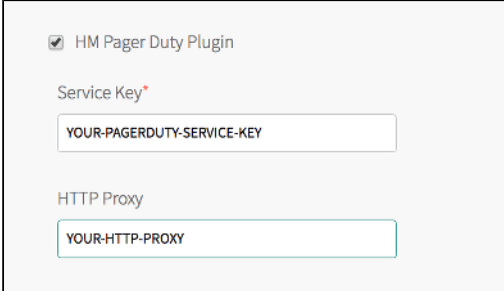
 **Note:** Starting in PCF v2.0, BOSH-reported component metrics are available in the Loggregator Firehose by default. If you continue to use the BOSH HM Forwarder to consume these component metrics, you may receive duplicate data. To prevent this, leave the **Bosh HM Forwarder IP Address** field blank. For additional guidance, see [BOSH System Metrics Available in Loggregator Firehose](#) in the PCF v2.0 Release Notes.

- Select the **Enable VM Resurrecter Plugin** to enable Ops Manager Resurrector functionality and increase your runtime availability. If you intend to install PAS, see [Using BOSH Resurrector and vSphere HA](#) for more information about the Resurrector plugin.
- Select **Enable Post Deploy Scripts** to run a post-deploy script after deployment. This script allows the job to execute additional commands against a deployment.

 **Note:** You must enable post-deploy scripts to install PKS.

- Select **Recreate all VMs** to force BOSH to recreate all VMs on the next deploy. This process does not destroy any persistent disk data.
- Select **Enable bosh deploy retries** to instruct Ops Manager to retry failed BOSH operations up to five times.
- (Optional) Disable **Allow Legacy Agents** if all of your tiles have stemcells v3468 or later. Disabling the field will allow Ops Manager to implement TLS secure communications.

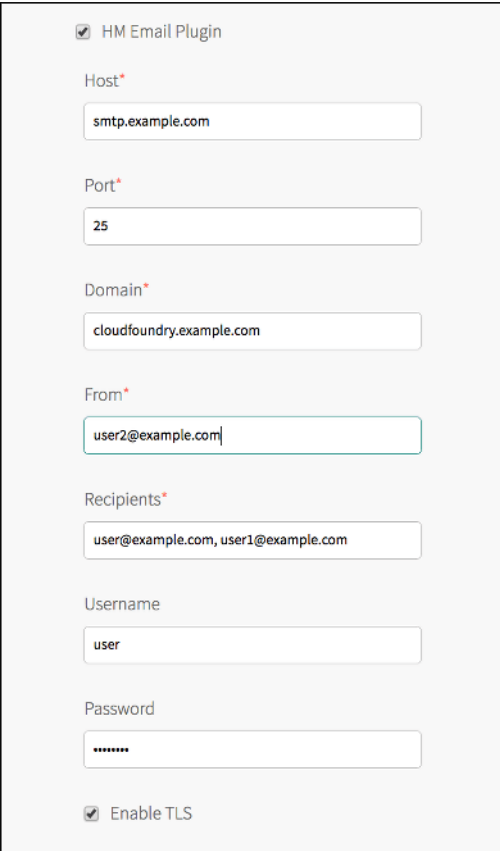
10. Select **Keep Unreachable Director VMs** if you want to preserve BOSH Director VMs after a failed deployment for troubleshooting purposes.



☒ HM Pager Duty Plugin
 Service Key*
 YOUR-PAGERDUTY-SERVICE-KEY
 HTTP Proxy
 YOUR-HTTP-PROXY

11. Select **HM Pager Duty Plugin** to enable Health Monitor integration with PagerDuty.

- **Service Key:** Enter your API service key from PagerDuty.
- **HTTP Proxy:** Enter an HTTP proxy for use with PagerDuty.



☒ HM Email Plugin
 Host*
 smtp.example.com
 Port*
 25
 Domain*
 cloudfoundry.example.com
 From*
 user2@example.com
 Recipients*
 user@example.com, user1@example.com
 Username
 user
 Password

☒ Enable TLS

12. Select **HM Email Plugin** to enable Health Monitor integration with email.

- **Host:** Enter your email hostname.
- **Port:** Enter your email port number.
- **Domain:** Enter your domain.
- **From:** Enter the address for the sender.
- **Recipients:** Enter comma-separated addresses of intended recipients.
- **Username:** Enter the username for your email server.
- **Password:** Enter the password for your email server.
- **Enable TLS:** Select this checkbox to enable Transport Layer Security.

13. For **CredHub Encryption Provider**, you can choose whether BOSH CredHub stores its encryption key internally on the BOSH Director and CredHub VM, or in an external hardware security module (HSM). The HSM option is more secure.

Before configuring an HSM encryption provider in the **Director Config** pane, you must follow the procedures and collect information described in [Preparing CredHub HSMs for Configuration](#).

Note: After you deploy Ops Manager with an HSM encryption provider, you cannot change BOSH CredHub to store encryption keys internally.

CredHub Encryption Provider

☒ Internal
 ☐ Luna HSM

Encryption Key Name*

Provider Partition*

Provider Partition Password*

Provider Client Certificate*

Provider Client Certificate Private Key*

HSM Host Address*


HSM Port Address*

Partition Serial Number*

HSM Certificate*

- **Internal:** Select this option for internal CredHub key storage. This option is selected by default and requires no additional configuration.
- **Luna HSM:** Select this option to use a SafeNet Luna HSM as your permanent CredHub encryption provider, and fill in the following fields:
 1. **Encryption Key Name:** Any name to identify the key that the HSM uses to encrypt and decrypt the CredHub data. Changing this key name after you deploy Ops Manager can cause service downtime.
 2. **Provider Partition:** The partition that stores your encryption key. Changing this partition after you deploy Ops Manager could cause service downtime. For this value and the ones below, use values gathered in [Preparing CredHub HSMs for Configuration](#).
 3. **Provider Partition Password**
 4. **Provider Client Certificate:** The certificate that validates the identity of the HSM when CredHub connects as a client.
 5. **Provider Client Certificate Private Key**
 6. **HSM Host Address**
 7. **HSM Port Address:** If you do not know your port address, enter `1792`.
 8. **Partition Serial Number**
 9. **HSM Certificate:** The certificate that the HSM presents to CredHub to establish a two-way mTLS connection.

14. Select a **Blobstore Location** to either configure the blobstore as an internal server or an external endpoint. Because the internal server is unscalable and less secure, Pivotal recommends that you configure an external blobstore.

 **Note:** After you deploy Ops Manager, you cannot change the blobstore location.

Blobstore Location

☒ Internal
☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature
☐ V4 Signature

Region*

☐ GCS Blobstore


Bucket Name*

Storage Class*


Regional

Service Account Key*


- o **Internal:** Select this option to use an internal blobstore. Ops Manager creates a new VM for blob storage. No additional configuration is required.
- o **S3 Compatible Blobstore:** Select this option to use an external S3-compatible endpoint. Follow the procedures in [Sign up for Amazon S3](#) and [Creating a Bucket](#) in the AWS documentation. When you have created an S3 bucket, complete the following steps:
 1. **S3 Endpoint:** Navigate to the [Regions and Endpoints](#) topic in the AWS documentation.
 - a. Locate the endpoint for your region in the **Amazon Simple Storage Service (S3)** table and construct a URL using your region's endpoint. For example, if you are using the `us-west-2` region, the URL you create would be `https://s3-us-west-2.amazonaws.com`. Enter this URL into the **S3 Endpoint** field.
 - b. On a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
 - c. Copy the custom public CA certificate you used to sign the S3 endpoint into `/etc/ssl/certs` on the Ops Manager VM.
 - d. On the Ops Manager VM, run `sudo update-ca-certificates -f -v` to import the custom CA certificate into the Ops Manager VM truststore.


 **Note:** You must also add this custom CA certificate into the **Trusted Certificates** field in the **Security** page. See [Security Page](#) for instructions.

2. **Bucket Name:** Enter the name of the S3 bucket.
3. **Access Key** and **Secret Key:** Enter the keys you generated when creating your S3 bucket.
4. Select **V2 Signature** or **V4 Signature**. If you select **V4 Signature**, enter your **Region**.

 **Note:** AWS recommends using Signature Version 4. For more information about AWS S3 Signatures, see [Authenticating Requests](#) in the AWS documentation.

- **Enable TLS:** Select this checkbox to enable TLS.

 **Note:** If you are using Linux stemcells, make sure you have configured [Linux stemcell v3586.16 or later](#) for all tiles before enabling TLS.

 **Note:** If you are using PAS for Windows 2016, make sure you have configured [Windows stemcell v1709.10 or later](#) for all tiles before enabling TLS.

- **GCS Blobstore:** Select this option to use an external GCS endpoint. To create a GCS bucket, you must have a GCS account. Follow the procedures in [Creating Storage Buckets](#) in the GCS documentation to create a GCS bucket. When you have created a GCS bucket, complete the following steps:
 1. **Bucket Name:** Enter the name of your GCS bucket.
 2. **Storage Class:** Select the storage class for your GCS bucket. See [Storage Classes](#) in the GCP documentation for more information.
 3. **Service Account Key:** Follow the steps in the [Set up an IAM Service Account](#) section of *Preparing to Deploy Ops Manager on GCP Manually* to download a JSON file with a private key. Enter the contents of the JSON file into the field.

15. Select a **Database Location**. By default, Ops Manager deploys and manages an **Internal** database for you. If you choose to use an **External MySQL Database**, complete the associated fields with information obtained from your external MySQL Database provider: **Host**, **Port**, **Username**,

Database Location

☒ Internal

☐ External MySQL Database

Host*

Port*

Username*

Password*

Database*

Password, and Database.

In addition, if you

selected the **Enable TLS for Director Database** checkbox, you can complete the following optional fields:

- **Enable TLS:** Select this checkbox enables TLS communication between the BOSH Director and the database.
- **TLS CA:** Enter the Certificate Authority for the TLS Certificate.
- **TLS Certificate:** Enter the client certificate for mutual TLS connections to the database.
- **TLS Private Key:** Enter the client private key for mutual TLS connections to the database.
- **Advanced DB Connection Options:** If you would like to provide additional options for the database, use this field to provide a JSON-formatted options string.

16. (Optional) **Director Workers:** Set the number of workers available to execute Director tasks. This field defaults to [5](#).

17. (Optional) **Max Threads:** Enter the number of operations the BOSH Director can perform simultaneously. For vSphere, the default value is [32](#). Leave the field blank to use this default value. Pivotal recommends that you use the default value unless doing so results in rate limiting or errors on your IaaS.

18. (Optional) **Director Hostname:** Enter a valid hostname to add a custom URL for your BOSH Director. You can also use this field to configure a load

balancer in front of your BOSH Director. For more information, see [How to Set Up a Load Balancer in Front of Operations Manager Director](#) in the Pivotal Support documentation.

⚠ warning: In Ops Manager v2.2.7 and earlier, if you change the **Director Hostname** after your initial deployment, VMs become unavailable. This causes PCF downtime. To restore VM availability, enable **Recreate All VMs** and redeploy. This issue is resolved in [Ops Manager v2.2.8](#) and later.

19. (Optional) Enter your list of comma-separated **Excluded Recursors** to declare which IP addresses and ports should not be used by the DNS server.
20. (Optional) To disable BOSH DNS, select the **Disable BOSH DNS server for troubleshooting purposes** checkbox. For more information about the BOSH DNS service discovery mechanism, see [BOSH DNS Enabled by Default](#) in the Ops Manager v2.2 Release Notes.

⚡ Breaking Change: Do not disable BOSH DNS without consulting Pivotal Support.

💡 Note: If you plan to deploy PKS, do not disable BOSH DNS. If PAS and PKS run on the same instance of Ops Manager, you cannot use the opt-out feature of BOSH DNS for your PAS without breaking PKS. To opt out of BOSH DNS in your PAS deployment, install the tile on a separate instance of Ops Manager.

21. (Optional) **Custom SSH Banner:** Enter text to set a custom banner that users see when logging in to the Director using SSH.

☐ Disable BOSH DNS server for troubleshooting purposes

Custom SSH Banner

22. (Optional) Enter your comma-separated custom **Identification Tags**. For example, `iaas:foundation1, hello:world`. You can use the tags to identify your foundation when viewing VMs or disks from your IaaS.
23. Click **Save**.

💡 Note: After your initial deployment, you cannot edit the Blobstore and Database locations.

Step 4: Create Availability Zones Page

An Ops Manager availability zone (AZ) corresponds to your vCenter clusters and resource pools.

Multiple AZs allow you to provide high-availability and load balancing to your applications. When you run more than one instance of an application, Ops Manager balances those instances across all of the AZs assigned to the application.

Pivotal recommends that you use at least three AZs for a highly available installation of your chosen runtime.

1. Select **Create Availability Zones** to navigate to the pane.

Create Availability Zones

Availability Zones

Clusters and resource pools to which you will deploy Pivotal products

Add

▼ first-az

Name*

first-az

A unique name for this availability zone

IaaS Configuration*

first-vcenter

Clusters

Add Cluster

Cluster

hinterlands-1

Resource Pool

bulldog

▶ second-az

Save

2. Use the following steps to create one or more AZs for your applications to use:

- Click **Add**.
- Enter a unique **Name** for the AZ.
- Select a vCenter config name from the **IaaS Configuration** dropdown to associate your AZ with a vCenter. If you have only one vCenter config or if you are creating your first AZ, **IaaS Configuration** defaults to the first vCenter and cannot be configured.
- Enter the name of an existing vCenter **Cluster** to use as an AZ.
- **(Optional)** Enter the name of a **Resource Pool** in the vCenter cluster that you specified above. The jobs running in this AZ share the CPU and memory resources defined by the pool.
- **(Optional)** Click **Add Cluster** to create another set of **Cluster** and **Resource Pool** fields. You can add multiple clusters. Click the trash icon to delete a cluster. The first cluster cannot be deleted.

 **Note:** For the PAS runtime, see [Availability Zones in vSphere](#) for additional information.

3. Click **Save**.

Step 5: Create Networks Page

1. Select **Create Networks**.

Create Networks

Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future. Contact Pivotal support for help completing such a change.

Verification Settings

☐ Enable ICMP checks

Networks

One or many IP ranges upon which your products will be deployed

▼ infrastructure

Name*

infrastructure

Subnets*

vSphere Network Name*

pcf-virt-net/pcf-infrastructure-subnet

CIDR*

192.168.101.0/24

Reserved IP Ranges*

192.168.101.1-192.168.101.9

DNS*

192.168.101.2

Gateway*

192.168.101.1

Availability Zones*

☒ default*

Add Network

Add Subnet

2. Select **Enable ICMP checks** to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.

3. Depending on the runtime that you are deploying, do one of the following:

a. For PAS, use the following steps to create one or more Ops Manager networks:

- Click **Add Network**.
- Enter a unique **Name** for the network.
- Click **Add Subnet** to create one or more subnets for the network.
- Enter the full path and **vSphere Network Name** as it displays in vCenter. For example, enter `YOUR-DIRECTORY-NAME/YOUR-NETWORK-NAME`. If your vSphere Network Name contains a forward slash character, replace the forward slash with the URL-encoded forward slash character `%2F`.
- For **CIDR**, enter a valid CIDR block in which to deploy VMs. For example, enter `192.0.2.0/24`.
- For **Reserved IP Ranges**, enter any IP addresses from the **CIDR** that you want to blacklist from the installation. Ops Manager will not deploy VMs to any address in this range.
- Enter your **DNS** and **Gateway** IP addresses.
- Select which **Availability Zones** to use with the network.

b. For PKS, create the following Ops Manager networks:

- `infrastructure`: This network is for Ops Manager, the BOSH Director, the PKS broker, and the PKS API.
- `pkcs`: If you have a large deployment with multiple tiles, you can choose to deploy the PKS broker and PKS API to a separate network

© Copyright Pivotal Software Inc, 2013-2019

767

2.2


named `main`. See the table below for more information.

- `services`: Network for creating the master and worker VMs for Kubernetes clusters. The CIDR should not conflict with the pod overlay network `10.200.0.0/16` or the reserved Kubernetes services CIDR of `10.100.200.0/24`.


Use the values from the following table as a guide when you create each network, replacing the IP addresses with ranges that are available in your vSphere environment:

| Infrastructure Network | Field | Configuration |
|-------------------------|----------------------|---|
| | Name | <code>infrastructure</code> |
| | vSphere Network Name | <code>pcf-virt-net/pcf-infrastructure-subnet</code> |
| | CIDR | <code>192.168.101.0/26</code> |
| | Reserved IP Ranges | <code>192.168.101.1–192.168.101.9</code> |
| | DNS | <code>192.168.101.2</code> |
| | Gateway | <code>192.168.101.1</code> |
| Main Network (Optional) | Field | Configuration |
| | Name | <code>pks</code> |
| | vSphere Network Name | <code>pcf-virt-net/pcf-pks-subnet</code> |
| | CIDR | <code>192.168.16.0/26</code> |
| | Reserved IP Ranges | <code>192.168.16.1–192.168.16.9</code> |
| | DNS | <code>192.168.16.2</code> |
| | Gateway | <code>192.168.16.1</code> |
| Service Network | Field | Configuration |
| | Name | <code>services</code> |
| | vSphere Network Name | <code>pcf-virt-net/pcf-services-subnet</code> |
| | CIDR | <code>192.168.20.0/22</code> |
| | Reserved IP Ranges | <code>192.168.20.1–192.168.20.9</code> |
| | DNS | <code>192.168.20.2</code> |
| | Gateway | <code>192.168.20.1</code> |

4. Click **Save**.

 **Note:** Multiple networks allow you to place vCenter on a private network and the rest of your deployment on a public network. Isolating vCenter in this manner denies access to it from outside sources and reduces possible security vulnerabilities.

 **Note:** If you use the Cisco Nexus 1000v Switch, see to [Using the Cisco Nexus 1000v Switch with Ops Manager](#) for more information.

 **Note:** After you deploy Ops Manager, you add subnets with overlapping Availability Zones to expand your network. For more information about configuring additional subnets, see [Expanding Your Network with Additional Subnets](#).

Step 6: Assign AZs and Networks Page

1. Select **Assign AZs and Networks**.

Assign AZs and Networks

The BOSH Director is a single instance.

Choose the availability zone in which to place that instance. It is highly recommended that you backup this VM on a regular basis to preserve settings.

Singleton Availability Zone

AZ-MGMT

Network

infrastructure

Save

2. Use the dropdown to select a **Singleton Availability Zone**. The BOSH Director installs in this Availability Zone.
3. Use the dropdown to select a **Network** for your BOSH Director.
4. Click **Save**.

Step 7: Security Page

Security

Trusted Certificates

-----BEGIN CERTIFICATE-----

THE

-----END CERTIFICATE-----

These certificates enable BOSH-deployed components to trust a custom root certificate.

Generate VM passwords or use single password for all VMs

☒ Generate passwords
 ☐ Use default BOSH password



Save

1. Select **Security**.
2. In **Trusted Certificates**, enter your custom certificate authority (CA) certificates to insert into your organization's certificate trust chain. This feature enables all BOSH-deployed components in your deployment to trust custom root certificates.

To enter multiple certificates, paste your certificates one after the other. For example, format your certificates like the following:


```
-----BEGIN CERTIFICATE-----
ABCDEF12345678ABCDEF12345678ABCDEF12345678AB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BCDEF12345678ABCDEF12345678ABCDEF12345678ABB
EFGH12345678ABCDEF12345678ABCDEF12345678ABCDEF
GH12345678ABCDEF12345678ABCDEF12345678...
```

```
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
CDEFGH12345678ABCDEFGH12345678ABCDEFGH12345678ABBB  
EFGH12345678ABCDEFGH12345678ABCDEFGH12345678ABCDEF  
GH12345678ABCDEFGH12345678ABCDEFGH12345678...  
-----END CERTIFICATE-----
```

 **Note:** If you want to use Docker Registries for running app instances in Docker containers, enter the certificate for your private Docker Registry in this field. See [Using Docker Registries](#)  for more information on running app instances in PAS using Docker Registries.

3. Choose **Generate passwords** or **Use default BOSH password**. Pivotal recommends that you use the **Generate passwords** option for greater security.
4. Click **Save**. To view your saved Director password, click the **Credentials** tab.

Step 8: Syslog Page

 **Note:** BOSH Director logs contain sensitive information that should be considered privileged. For example, these logs may contain cloud provider credentials. If you choose to forward logs to an external syslog endpoint, use TLS encryption to prevent information from being intercepted by a third party.

1. Select **Syslog**.

Syslog

Do you want to configure Syslog for Bosh Director?

☐ No
 ☒ Yes

Address*

The address or host for the syslog server

Port*

Transport Protocol*

TCP

☐ Enable TLS

Permitted Peer*

SSL Certificate*

Save

- (Optional) Select **Yes** to send BOSH Director system logs to a remote server.
- In the **Address** field, enter the IP address or DNS name for the remote server.
- In the **Port** field, enter the port number that the remote server listens on.
- In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
- (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
 - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
 - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
- Click **Save**.

Step 9: Resource Config Page


- Select **Resource Config**.


Resource Config


| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE |
|------------------------|--------------|----------------------|---|
| Ops Manager Director | Automatic: 1 | Automatic: 50 GB | Automatic: medium.disk (cpu: 2, ram: 4 GB |
| Master Compilation Job | Automatic: 4 | None | Automatic: large.cpu (cpu: 4, ram: 4 GB, di |

Save

- Adjust any values as necessary for your deployment. Under the **Instances**, **Persistent Disk Type**, and **VM Type** fields, choose **Automatic** from the dropdown to allocate the recommended resources for the job. If the **Persistent Disk Type** field reads **None**, the job does not require persistent disk space.

 **Note:** Ops Manager requires a Director VM with at least 8 GB memory.

 **Note:** If you set a field to **Automatic** and the recommended resource allocation changes in a future version, Ops Manager automatically uses the updated recommended allocation.

 **Note:** If you install PAS for Windows, provision your **Master Compilation Job** with at least 128 GB of disk space.

- Click **Save**.

Step 10: (Optional) Add Custom VM Extensions

Use the Ops Manager API to add custom properties to your VMs such as associated security groups and load balancers. For more information, see [Managing Custom VM Extensions](#).

Step 11: Complete the BOSH Director Installation

- Click the **Installation Dashboard** link to return to the Installation Dashboard.
- Click **Apply Changes** on the right navigation.

Next Steps

After you complete this procedure, follow the instructions for the runtime that you intend to install.

- To install PAS, see [Deploying PAS on vSphere](#).
- To install PKS, see [Installing PKS on vSphere](#).

For more information about PCF runtimes, see [Installing Runtimes](#).

Deploying PAS on vSphere

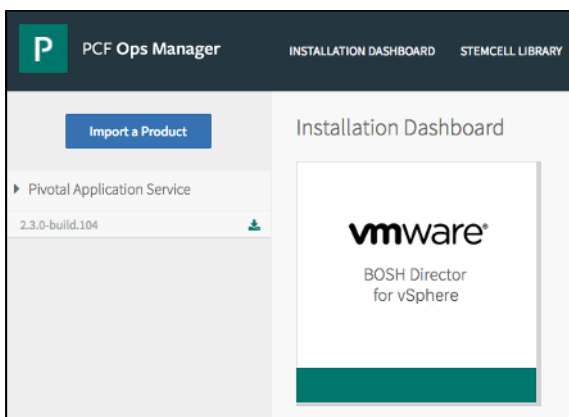
Page last updated:

This topic describes how to configure the Pivotal Application Service (PAS) components that you need to run [Pivotal Cloud Foundry](#) (PCF) for VMware vSphere.

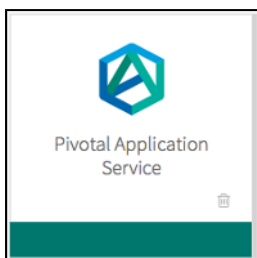
Note: If you plan to install the IPsec add-on, you must do so before installing any other tiles. For more information, see [Installing the IPsec Add-on for PCF](#).

Step 1: Add PAS to Ops Manager

1. Log in to [Pivotal Network](#) and download PAS.
2. From the **Releases** dropdown, select the release you want to install and choose one of the following:
 - Click PAS to download the PAS `.pivotal` file.
 - Click PCF Small Footprint PAS to download the Small Footprint Runtime `.pivotal` file. For more information, see [Getting Started with Small Footprint Runtime](#).
3. Click **Import a Product**. Select the PAS `.pivotal` file that you downloaded from Pivotal Network and click **Open**. After the import completes, PAS appears as an available product.
4. Hover over PAS and click **Add**.



5. Click the PAS tile in the Installation Dashboard.



Step 2: Assign Availability Zones and Networks

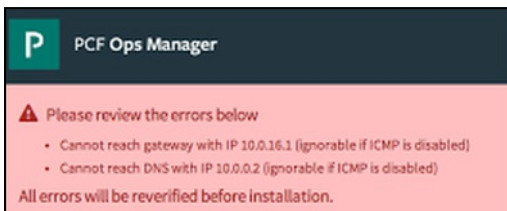
1. Select **Assign AZs and Networks**. These are the Availability Zones that you create when configuring BOSH Director. For more information, see [Create Availability Zone Page](#) in *Configuring BOSH Director on vSphere*.
2. **(vSphere Only):** Under **Place singleton jobs**, select an Availability Zone. Ops Manager runs any job with a single instance in this Availability Zone.
3. **(vSphere Only):** Under **Balance other jobs**, select one or more Availability Zones. Ops Manager balances instances of jobs with more than one instance across the Availability Zones that you specify.

- From the **Network** dropdown, choose the network where you want to run PAS.

The screenshot shows the 'Pivotal Application Service' settings interface. At the top, there's a navigation bar with 'Settings', 'Status', 'Credentials', and 'Logs'. Below this, a sidebar on the left lists various configuration categories, each with a green checkmark: 'Assign AZs and Networks' (highlighted), 'Domains', 'Networking', 'Application Containers', 'Application Developer Controls', 'Application Security Groups', 'Authentication and Enterprise SSO', and 'Databases'. The main content area is titled 'AZ and Network Assignments'. It contains two sections: 'Place singleton jobs in' with a radio button selected for 'first-az', and 'Balance other jobs in' with a checkbox selected for 'first-az'. Below these is a 'Network' dropdown menu currently showing 'first-network'. A blue 'Save' button is positioned at the bottom right of the configuration area.

- Click **Save**.

Note: When you save this form, a verification error displays because the PCF security group blocks ICMP. You can ignore this error.



Step 3: Configure Domains

- Select **Domains**.

The screenshot shows the 'Domains' configuration page. At the top, a text block explains: 'Application Service hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.' Below this, there are two input fields: 'System Domain' and 'Apps Domain'. Both fields contain the text 'sys.metallicseaweed.cf-app.com'. A blue 'Save' button is located at the bottom left of the form.

- Enter the system and application domains.
 - The **System Domain** defines your target when you push apps to PAS.
 - The **Apps Domain** defines where PAS should serve your apps.

Note: Pivotal recommends that you use the same domain name but different subdomain names for your system and app domains.

Doing so allows you to use a single wildcard certificate for the domain while preventing apps from creating routes that overlap with system routes. For example, name your system domain `system.EXAMPLE.com` and your apps domain `apps.EXAMPLE.com`.

3. Click **Save**.

Step 4: Configure Networking

1. Select **Networking**.
2. The values you enter in the **Router IPs** and **HAProxy IPs** fields depend on whether you are using HAProxy in your deployment. Use the table below to determine how to complete these fields.



Note: If you choose to assign specific IP addresses in either the **Router IPs** or **HAProxy IPs** field, ensure that these IP addresses are in the subnet that you configured for PAS in Ops Manager.

| Using HAProxy? | Router IPs Field | HAProxy IPs Field |
|----------------|--|--|
| No | <ol style="list-style-type: none"> 1. Choose IP addresses from the subnet you configured in Ops Manager. 2. Enter these IP addresses in the Router IPs field. You should specify more than one IP address for high availability. 3. Configure your load balancer to forward requests for the domains that you have configured for your deployment to these IP addresses. | Leave this field blank. |
| Yes | Leave this field blank. | <ol style="list-style-type: none"> 1. Choose IP addresses from the subnet you configured in Ops Manager. 2. Enter these IP addresses in the HAProxy IPs field. You should specify more than one IP address for high availability. 3. Configure your load balancer to forward requests for the domains you have configured for your deployment to these IP addresses. |

3. (Optional) In **SSH Proxy IPs**, add the IP address for your Diego Brain, which will accept requests to SSH into application containers on port `2222`.
4. (Optional) In **TCP Router IPs**, add the IP addresses you want assigned to the TCP Routers. You enable this feature at the bottom of this screen.

Configure security and routing services for your platform. It is usually preferable to use your own load balancer instead of an HAProxy instance as your point-of-entry to the platform.

Router IPs

10.85.10.200



SSH Proxy IPs

10.85.10.201

HAProxy IPs

TCP Router IPs

5. Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate** and **Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.

- a. Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

Certificates and Private Keys for HAProxy and Router

Add

▼ example-cert

Name *

example-cert

A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

Generate RSA Certificate

▼ example-cert-2

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *

-----BEGIN CERTIFICATE-----

MIIE...

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIIE...

-----END RSA PRIVATE KEY-----

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager.

- b. If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see *Configure Front End* in [Preparing to Deploy Ops Manager on GCP Manually](#).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

6. (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Router** field, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

- ☐ TLSv1.0
- ☐ TLSv1.1
- ☒ TLSv1.2

- Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

- ☒ Log client IPs
- ☐ Disable logging of X-Forwarded-For header only
- ☐ Disable logging of both source IP and X-Forwarded-For header

To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.

- Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.



Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

- ☒ TLS terminated for the first time at infrastructure load balancer
- ☐ TLS terminated for the first time at HAProxy
- ☐ TLS terminated for the first time at the Router

The following table

indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|---|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to | TLS terminated for | HAProxy sets the XFCC header with the client certificate received in the TLS handshake. The Gorouter forwards the header. |

| | | |
|--|--|---|
| <ul style="list-style-type: none"> the instances of HAProxy, and HAProxy instance count is > 0 | the first time at HAProxy. |  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |
| <ul style="list-style-type: none"> The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | TLS terminated for the first time at the Gorouter. | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. |


For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).

- To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

- ☒ HAProxy does not request client certificates.
- ☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.


 **warning:** Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

- To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

- ☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.
- ☒ Router requests but does not require client certificates.
- ☐ Router requires client certificates.

- Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

 **warning:** Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client**


Certificate Validation in the Networking pane.

- In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.


 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following:
`DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384` If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

 **Note:** Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

- Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable

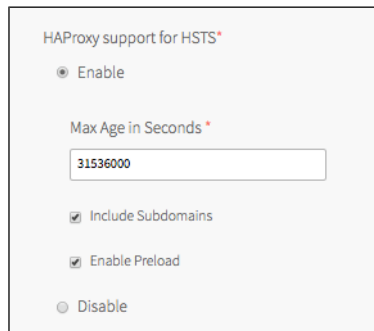
◦ Enable HAProxy forwarding of requests to Router over TLS

| If you want to: | Encrypt communication between HAProxy and the Gorouter |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

◦ Disable HAProxy forwarding of requests to Router over TLS

| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |


15. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field and complete



the following optional configuration steps:

- a. (Optional) **Enter a Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
- b. (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
- c. (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from HAProxy.

16. If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

17. (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

18. (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
19. (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
20. (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
21. By default, the PAS routers handle traffic for applications deployed to an isolation segment created by the PCF Isolation Segment tile. To configure the PAS routers to reject requests for applications within isolation segments, select the **Routers reject requests for Isolation Segments** checkbox.

☐ Routers reject requests for Isolation Segments

Do not enable this option without deploying

routers for each isolation segment. See the following topics for more information:

- [Installing PCF Isolation Segment](#)
- [Sharding Routers for Isolation Segments](#)

22. (Optional) By default, Gorouter support for the PROXY protocol is disabled. To enable the PROXY protocol, select **Enable support for PROXY protocol in CF Router**. When enabled, client-side load balancers that terminate TLS but do not support HTTP can pass along information from the originating client. Enabling this option may impact Gorouter performance. For more information about enabling the PROXY protocol in Gorouter, see the [HTTP Header Forwarding](#) sections in the [Securing Traffic in Cloud Foundry](#) topic.
23. In the **Choose whether to enable route services** section, choose either **Enable route services** or **Disable route services**. Route services are a class of [marketplace services](#) that perform filtering or content transformation on application requests and responses. See the [Route Services](#) topic for details.
 - a. If you enabled route services, you can also configure the **Bypass security checks for route service lookup** field. Pivotal recommends that you do not enable this field because it has potential security concerns. However, you may need to enable it if your load balancer requires mutual TLS from clients. For more information, see [Configuring Route Service Lookup](#).
24. (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

0

500

25. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router*

☒ Enable
 ☐ Disable

26. (Optional) To accommodate larger uploads over connections with high latency, increase the number of seconds in the **Router Timeout to Backends** field.
27. (Optional) Use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| IaaS | Guidance |
|-------|---|
| AWS | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> . |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST. |
| GCP | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout. |

 **Note:** Do not set a frontend idle timeout lower than six seconds.

28. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
29. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

20

Load Balancer Healthy Threshold *

20

30. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

31. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

32. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.

HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.

HAProxy Trusted CIDRs

33. The **Loggregator Port** defaults to **443** if left blank. Enter a new value to override the default.

34. For **Container Network Interface Plugin**, select one of the following:

- **Silk:** This option is the default Container Network Interface (CNI) for PAS.
- **External:** Select this if you are deploying the [VMware NSX-T Container Plug-in for PCF](#).
 - If you select **External**, follow the instructions in [Deploying PAS with NSX-T Networking](#) in addition to the PAS configuration instructions in this topic.

⚠ warning: The NSX-T integration only works for fresh installs of PCF. If your PAS is already deployed and running with Silk as its CNI, you cannot change the CNI plugin to NSX-T.

35. If you selected **Silk** in the previous step, review the following fields:

- (Optional) You can change the value in the **Applications Network Maximum Transmission Unit (MTU)** field. Pivotal recommends setting the MTU value for your application network to **1454**. Some configurations, such as networks that use GRE tunnels, may require a smaller MTU value.
- (Optional) Enter an IP range for the overlay network in the **Overlay Subnet** box. If you do not set a custom range, Ops Manager uses **10.255.0.0/16**.

⚠ warning: The overlay network IP range must not conflict with any other IP addresses in your network.

- Enter a UDP port number in the **VXLAN Tunnel Endpoint Port** box. If you do not set a custom port, Ops Manager uses 4789.
- For **Denied logging interval**, set the per-second rate limit for packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) rules applied across the space, org, or deployment. This field defaults to **1**.
- For **UDP logging interval**, set the per-second rate limit for UDP packets sent and received. This field defaults to **100**.
- To enable logging for app traffic, select **Log traffic for all accepted/denied application packets**. See [Manage Logging for Container-to-Container Networking](#) for more information.
- By default, containers use the same DNS servers as the host. If you want to override the DNS servers to be used in containers, enter a comma-separated list of servers in **DNS Servers**.

💡 Note: If your deployment uses BOSH DNS, which is the default, you cannot use this field to override the DNS servers used in containers.

36. For **DNS Search Domains**, enter DNS search domains for your containers as a comma-separated list. DNS on your containers appends these names to its host names, to resolve them into full domain names.

DNS Search Domains

example.com, myapps.com

DNS search domains to be used in containers. A comma-separated list can be specified.

37. For **Database Connection Timeout**, set the connection timeout for clients of the policy server and silk databases. The default value is `120`. You may need to increase this value if your deployment experiences timeout issues related to Container-to-Container Networking.

38. (Optional) TCP Routing is disabled by default. You should enable this feature if your DNS sends TCP traffic through a load balancer rather than directly to a TCP router. To enable TCP routing:

- a. Select **Enable TCP Routing**.
- b. For **TCP Routing Ports**, enter a single port or a range of ports for the load balancer to forward to. These are the same ports that you configured in the [Pre-Deployment Steps](#) of the *Enabling TCP Routing* topic.
 - To support multiple TCP routes, Pivotal recommends allocating multiple ports.
 - To allocate a list of ports rather than a range:
 1. Enter a single port in the **TCP Routing Ports** field.
 2. After deploying PAS, follow the directions in [Configuring a List of TCP Routing Ports](#) to add TCP routing ports using the cf CLI.

Enable TCP requests to your apps via specific ports on the TCP router. You will want to configure a load balancer to forward these TCP requests to the TCP routers. If you do not have a load balancer, then you can also send traffic directly to the TCP router.*

☐ Select this option if you prefer to enable TCP Routing at a later time

☒ Enable TCP Routing

TCP Routing Ports (one-time configuration, if you want to update this value you can via the CF CLI) *

1024-1123

- c. Return to the top of the **Networking** screen. In **TCP Router IPs** field, make sure you have entered IP addresses within your subnet CIDR block. These will be the same IP addresses you configured your load balancer with in [Pre-Deployment Steps](#), unless you configured DNS to resolve the TCP domain name directly to an IP you've chosen for the TCP router.
- d. (Optional) To disable TCP routing, click **Select this option if you prefer to enable TCP Routing at a later time** For more information, see the [Configuring TCP Routing in PAS](#) [topic](#).

39. Click **Save**.

Step 5: Configure Application Containers

1. Select **Application Containers**.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC

☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888


Docker Images Disk-Cleanup Scheduling on Cell VMs*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) *


10240


- The **Enable Custom Buildpacks** checkbox governs the ability to pass a custom buildpack URL to the `-b` option of the `cf push` command. By default, this ability is enabled, letting developers use custom buildpacks when deploying apps. Disable this option by disabling the checkbox. For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.
- The **Allow SSH access to app containers** checkbox controls SSH access to application instances. Enable the checkbox to permit SSH access across your deployment, and disable it to prevent all SSH access. See the [Application SSH Overview](#) topic for information about SSH access permissions at the space and app scope.
- If you want to enable SSH access for new apps by default in spaces that allow SSH, select **Enable SSH when an app is created**. If you deselect the checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.
- If you want to disable the Garden Root filesystem (GrootFS), deselect the **Enable the GrootFS container image plugin for Garden RunC** checkbox. Pivotal recommends using this plugin, so it is enabled by default. However, some external components are sensitive to dependencies with filesystems such as GrootFS. If you experience issues, such as antivirus or firewall compatibility problems, deselect the checkbox to roll back to the plugin that is built into Garden RunC. For more information about GrootFS, see [Component: Garden](#) and [Container Mechanics](#).

 **Note:** If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.


- To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox.

Verifying app identity using TLS enables encryption between router and app containers and guards against misrouting during control plane failures. For more information about Gorouter route consistency modes, see [Preventing Misrouting](#) in *HTTP Routing*.

 **warning:** TLS routing requires an additional 32 MB of RAM capacity on Diego cells per app instance. It also requires additional CPU capacity on Diego cells. If the total amount of Diego cell memory available is less than 32 MB times the number of running app instances, scale your Diego cells before configuring the Gorouter with TLS.

 **Warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. If the total amount of memory and CPU usage of the Gorouters in your environment are close to the size limit, scale your Gorouters before enabling TLS routing.

- You can configure Pivotal Application Service (PAS) to run app instances in Docker containers by supplying their IP address ranges in the **Private Docker Insecure Registry Whitelist** textbox. See the [Using Docker Registries](#) topic for more information.
- Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
- Enter a number in the **Max Inflight Container Starts** textbox. This number configures the maximum number of started instances across the Diego cells in your deployment. For more information about this feature, see [Setting a Maximum Number of Started Containers](#).
- Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](#) topic.

 **Note:** In a clean install, NFSv3 volume services is enabled by default. In an upgrade, NFSv3 volume services is set to the same setting as it was in the previous deployment.

- (Optional) To configure LDAP for NFSv3 volume services, do the following:

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. *

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

Format of timestamps in Diego logs*

☒ RFC3339 timestamps (e.g. 2018-02-09T00:54:13.479724884Z)

☐ Seconds since the Unix epoch (e.g. 1518137653.479724884)

Save

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account named `volume-services` that belongs to organizational units (OU) named `service-accounts` and `my-company`, and your domain is named `domain`, the fully qualified path looks like the following:

```
CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com
```

- By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.

13. Select the **Format of timestamps in Diego logs**, either **RFC3339 timestamps** or **Seconds since the Unix epoch**. Fresh PAS v2.2 installations default to **RFC3339 timestamps**, while upgrades to PAS v2.2 from previous versions default to **Seconds since the Unix epoch**.
14. You can optionally modify the **Default health check timeout**. The value configured for this field is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy. The default timeout is seconds and the maximum configurable timeout is seconds.
15. Click **Save**.

Step 6: Configure Application Developer Controls

1. Select **Application Developer Controls**.

Configure restrictions and default settings for applications pushed to Application Service.

Maximum File Upload Size (MB) (min: 1024, max: 2048) *

Default App Memory (MB) (min: 64, max: 2048) *

Default App Memory Quota per Org (MB) (min: 10240, max: 102400) *

Maximum Disk Quota per App (MB) (min: 512, max: 20480) *

Default Disk Quota per App (MB) (min: 512, max: 20480) *

Default Service Instances Quota per Org (min: 0, max: 1000) *

Staging Timeout (Seconds) *


☐ Allow Space Developers to manage network policies

☒ Enable Service Discovery for Apps

Save

2. Enter the **Maximum File Upload Size (MB)**. This is the maximum size of an application upload.
3. Enter the **Default App Memory (MB)**. This is the amount of RAM allocated by default to a newly pushed application if no value is specified with the cf CLI.
4. Enter the **Default App Memory Quota per Org**. This is the default memory limit for all applications in an org. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value.

5. Enter the **Maximum Disk Quota per App (MB)**. This is the maximum amount of disk allowed per application.

 **Note:** If you allow developers to push large applications, PAS may have trouble placing them on Cells. Additionally, in the event of a system upgrade or an outage that causes a rolling deploy, larger applications may not successfully re-deploy if there is insufficient disk capacity. Monitor your deployment to ensure your Cells have sufficient disk to run your applications.

6. Enter the **Default Disk Quota per App (MB)**. This is the amount of disk allocated by default to a newly pushed application if no value is specified with the cf CLI.
7. Enter the **Default Service Instances Quota per Org**. The specified limit only applies to the first installation of PAS. After the initial installation, operators can use the cf CLI to change the default value .
8. Enter the **Staging Timeout (Seconds)**. When you stage an application droplet with the Cloud Controller, the server times out after the number of seconds you specify in this field.
9. Select the **Allow Space Developers to manage network policies** checkbox to permit developers to manage their own network policies for their applications.
10. The **Enable Service Discovery for Apps** checkbox, which enables service discovery between applications, is enabled by default. To disable this feature, clear this checkbox. For more information about application service discovery, see the [App Service Discovery](#) section of the *Understanding Container-to-Container Networking* topic.
11. Click **Save**.

Step 7: Review Application Security Group

Setting appropriate [Application Security Groups](#) is critical for a secure deployment. Type ☐ in the box to acknowledge that once the Pivotal Application Service (PAS) deployment completes, you will review and set the appropriate application security groups. See [Restricting App Access to Internal PCF Components](#) for instructions.

Setting appropriate Application Security Groups that control application network policy is the responsibility of the Elastic Runtime administration team. Please refer to the Application Security Groups topic in the Pivotal Cloud Foundry documentation for more detail on completing this activity after the Elastic Runtime deployment completes.

Type X to acknowledge that you understand this message *

Save

Step 8: Configure Authentication and Enterprise SSO

1. Select **Authentication and Enterprise SSO**.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms *

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length *

Minimum Uppercase Characters Required for Password *

Minimum Lowercase Characters Required for Password *

Minimum Numerical Digits Required for Password *

Minimum Special Characters Required for Password *

Maximum Password Entry Attempts Allowed *

2. To authenticate user sign-ons, your deployment can use one of three types of user database: the UAA server's internal user store, an external SAML identity provider, or an external LDAP server.

- To use the internal UAA, select the **Internal** option and follow the instructions in the [Configuring UAA Password Policy](#) topic to configure your password policy.
- To connect to an external identity provider through SAML, scroll down to select the **SAML Identity Provider** option and follow the instructions in the [Configuring PCF for SAML](#) section of the *Configuring Authentication and Enterprise SSO for Pivotal Application Service (PAS)* topic.
- To connect to an external LDAP server, scroll down to select the **LDAP Server** option and follow the instructions in the [Configuring LDAP](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.

3. Click **Save**.

Step 9: Configure UAA

1. Select **UAA**.

2. (Optional) Under **JWT Issuer URI**, enter the URI that UAA uses as the issuer when generating tokens.

JWT Issuer URI

3. Under **SAML Service Provider Credentials**, enter a certificate and private key to be used by UAA as a SAML Service Provider for signing outgoing SAML authentication requests. You can provide an existing certificate and private key from your trusted Certificate Authority or generate a self-signed certificate. The following domain must be associated with the certificate: `*.login.YOUR-SYSTEM-DOMAIN`.



Note: The Pivotal Single Sign-On Service and Pivotal Spring Cloud Services tiles require the `*.login.YOUR-SYSTEM-DOMAIN`.

- If the private key specified under **Service Provider Credentials** is password-protected, enter the password under **SAML Service Provider Key**

SAML Service Provider Credentials *

-----BEGIN CERTIFICATE-----
 M
 U
 H
 M
 -----END CERTIFICATE-----

[Change](#)

SAML Service Provider Key Password

Secret

Password.

- (Optional) To override the default value, enter a custom SAML Entity ID in the **SAML Entity ID Override** field. By default, the SAML Entity ID is `http://login.YOUR-SYSTEM-DOMAIN` where `YOUR-SYSTEM-DOMAIN` is set in the **Domains > System Domain** field.
- For **Signature Algorithm**, choose an algorithm from the dropdown menu to use for signed requests and assertions. The default value is `SHA256`.
- (Optional) In the **Apps Manager Access Token Lifetime**, **Apps Manager Refresh Token Lifetime**, **Cloud Foundry CLI Access Token Lifetime**, and **Cloud Foundry CLI Refresh Token Lifetime** fields, change the lifetimes of tokens granted for Apps Manager and Cloud Foundry Command Line Interface (cf CLI) login access and refresh. Most deployments use the defaults.

Apps Manager Access Token Lifetime (in seconds) *

1209600

Apps Manager Refresh Token Lifetime (in seconds) *

1209600

Cloud Foundry CLI Access Token Lifetime (in seconds) *

7200

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

1209600

Global Login Session Max Timeout (in seconds) *

1800

Global Login Session Idle Timeout (in seconds) *

1800

Customize Username Label (on login page) *

Email

Customize Password Label (on login page) *


Password

Proxy IPs Regular Expression *

10\.\d{1,3}\.\d{1,3}\.\d{1,3}|192\.168\.\d{1,3}

[Save](#)

8. (Optional) In the **Global Login Session Max Timeout** and **Global Login Session Idle Timeout** fields, change the maximum number of seconds before a global login times out. These fields apply to the following:
 - **Default zone sessions:** Sessions in Apps Manager, PCF Metrics, and other web UIs that use the UAA default zones
 - **Identity zone sessions:** Sessions in apps that use a UAA identity zone, such as a Single Sign-On service plan
9. (Optional) Customize the text prompts used for username and password from the cf CLI and Apps Manager login popup by entering values for **Customize Username Label (on login page)** and **Customize Password Label (on login page)**.
10. (Optional) The **Proxy IPs Regular Expression** field contains a pipe-delimited set of regular expressions that UAA considers to be reverse proxy IP addresses. UAA respects the `x-forwarded-for` and `x-forwarded-proto` headers coming from IP addresses that match these regular expressions. To configure UAA to respond properly to Gorouter or HAProxy requests coming from a public IP address, append a regular expression or regular expressions to match the public IP address.
11. You can configure UAA to use an internal MySQL database provided with PCF, or you can configure an external database provider. Follow the procedures in either the [Internal Database Configuration](#) or the [External Database Configuration](#) section below.

 **Note:** If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data before changing the configuration. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information, and contact [Pivotal Support](#) for help.

Internal Database Configuration

When you configure the UAA to use an internal MySQL database, it uses the type of database selected in the **Databases** pane. See the [Configure Internal Databases](#) section for details.

1. Select **Internal MySQL**.

Choose the location of your UAA database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use AWS RDS)

 **Note:** If you configure your system databases as external in the **Databases** pane, selecting Internal MySQL in the **UAA** pane has no effect.

2. Click **Save**.
3. Ensure that you complete the [Configure Internal MySQL](#) step later in this topic to configure high availability for your internal MySQL databases.

External Database Configuration

1. From the **UAA** section in Pivotal Application Service (PAS), select **External**.

Choose the location of your UAA database *

☐ Internal MySQL (preferred for complete high-availability)

☒ External (preferred if, for example, you use AWS RDS)

Hostname *


TCP Port *

Username *


Password *

2. For **Hostname**, enter the hostname of the database server.
3. For **TCP Port**, enter the port of the database server.
4. For **User Account and Authentication database username**, specify a unique username that can access this specific database on the database server.
5. For **User Account and Authentication database password**, specify a password for the provided username.
6. Click **Save**.

Step 10: Configure CredHub

 **Note:** Enabling CredHub is not required. However, you cannot leave the fields under **Encryption Keys** blank. If you do not intend to use CredHub, enter any text in the **Name** and **Key** fields as placeholder values.

1. Select **CredHub**.
2. Choose the location of your CredHub database. PAS includes this CredHub database for services to store their service instance credentials.

 **Note:** You cannot choose **Internal** for the CredHub database if you choose **External** for your System Databases. See [Configure System Databases](#) below.

Configure the CredHub Server

Choose the location of your CredHub database *

☒ Internal MySQL (preferred for complete high-availability)

☐ External (preferred if, for example, you use Google Cloud SQL)

If you chose **External**, enter the following:

- **Hostname.** This is the IP address of your database server.
- **TCP Port.** This is the port of your database server, such as `3306`.
- **Username.** This is a unique username that can access your CredHub database on the database server.
- **Password.** This is the password for the provided username.
- **Database CA Certificate.** This certificate is used when encrypting traffic to and from the database.

3. Under **Encryption Keys**, specify one or more keys to use for encrypting and decrypting the values stored in the CredHub database.

Encryption Keys

Name *

Name of the encryption key.

Provider*


Internal

Key *

Secret

☐ Primary

- **Name.** This is the name of the encryption key.
 - If you plan to use internal encryption, enter any key name.
 - If you plan to use an HSM as your encryption provider, enter a key name that already exists on your HSM or a new key name. For each new key name, CredHub generates a key in **HSM Provider Partition** that you configure below.
- **Provider.** This is the provider of the encryption key. If you plan to configure an HSM provider and HSM servers below, select **HSM**. Otherwise, select **Internal**.
- **Key.** If you select internal encryption, this key is used for encrypting all data. The key must be at least 20 characters long.
 - If you selected **Internal** above, enter a randomly generated value under **Key**.
 - If you selected **HSM** above, enter a placeholder value under **Key**. CredHub does not use this key for encryption. However, you cannot leave the **Key** field blank.
- **Primary.** This checkbox is used for marking the key you specified above as the primary encryption key. You must mark one key as **Primary**. Do not mark more than one key as **Primary**.

 **Note:** For information about using additional keys for key rotation, see the [Rotating Runtime CredHub Encryption Keys](#) topic.

4. (Optional) To configure CredHub to use an HSM, complete the following fields:

- **HSM Provider Partition.** This is the name of the HSM provider partition.
- **HSM Provider Partition Password.** This password is used to access the HSM provider partition.
- **HSM Provider Client Certificate.** This is the client certificate for the HSM. For more information, see [Create and Register HSM Clients](#) in the

Preparing CredHub HSMs for Configuration topic.

- In the **HSM Provider Servers** section, click **Add** to add an HSM server. You can add multiple HSM servers. For each HSM server, complete the following fields:
 - **Host Address.** This is the host name or IP address of the HSM server.
 - **Port.** This is the port of the HSM server. If you do not know your port address, enter `1792`.
 - **Partition Serial Number.** This is the serial number of the HSM partition.
 - **HSM Certificate.** This is the certificate for the HSM server. The HSM presents this certificate to CredHub to establish a two-way TLS connection.

5. If your deployment uses any PCF services that support storing service instance credentials in CredHub and you want to enable this feature, select the **Secure Service Instance Credentials** checkbox.
6. Click **Save**.
7. Select the **Resource Config** pane.
8. Under the **Job** column of the **CredHub** row, set the number of instances to `2`. This is the minimum instance count required for high availability.
9. Click **Save**.

For more information about using CredHub for securing service instance credentials, see [Securing Service Instance Credentials with Runtime CredHub](#).

Step 11: Configure System Databases

You can configure PAS to use an internal MySQL database provided with PCF, or you can configure an external database provider for the databases required by PAS.

Note: If you are performing an upgrade, do not modify your existing internal database configuration or you may lose data. You must migrate your existing data first before changing the configuration. Contact Pivotal Support for help. See [Upgrading Pivotal Cloud Foundry](#) for additional upgrade information.

Internal Database Configuration

If you want to use internal databases for your deployment, perform the following steps:

1. Select **Databases**.
2. Select one of the **Internal Databases** options:
 - **Internal Databases - MySQL - Percona XtraDB Cluster** uses [Percona Server](#) with TLS encryption between server cluster nodes.
 - **Internal Databases - MySQL - MariaDB Galera Cluster** uses [MariaDB](#) with cluster nodes communicating over plaintext.

⚠ warning: Changing existing internal databases from **MySQL - MariaDB Galera Cluster** to **MySQL - Percona XtraDB Cluster** migrates the databases after you click **Apply Changes**, causing temporary system downtime. See [Migrate to Internal Percona MySQL](#) for details.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. *

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

3. Click **Save**.

Then proceed to [Step 12: \(Optional\) Configure Internal MySQL](#) to configure high availability for your internal MySQL databases.

External Database Configuration

⚠ warning: Protect whichever database you use in your deployment with a password.

To create your Pivotal Application Service (PAS) databases, follow the procedure below.

💡 Note: Exact configurations depend on your database provider. The following procedure uses AWS RDS as an example.

1. Add the `ubuntu` account key pair from your IaaS deployment to your local SSH profile so you can access the Ops Manager VM. For example, in AWS, you add a key pair created in AWS:

```
$ ssh-add aws-keypair.pem
```

2. SSH in to your Ops Manager using the Ops Manager FQDN and the username `ubuntu`:

```
$ ssh ubuntu@OPS-MANAGER-FQDN
```

3. Log in to your MySQL database instance using the appropriate hostname and user login values configured in your IaaS account. For example, to log in to your AWS RDS instance, run the following MySQL command:

```
$ mysql --host=RDSHOSTNAME --user=RDSUSERNAME --password=RDSPASSWORD
```

4. Run the following MySQL commands to create databases for the PAS components that require a relational database:


```
CREATE database ccdb;
CREATE database notifications;
CREATE database autoscale;
CREATE database app_usage_service;
CREATE database routing;
CREATE database diego;
CREATE database account;
CREATE database nfsvolume;
CREATE database networkpolicyserver;
CREATE database silk;
CREATE database locket;
CREATE database uaa;
CREATE database credhub;
```

💡 Note: The command `CREATE database credhub;` is optional if you have no CredHub instances. By default, CredHub has `0` instances.


5. Type `exit` to quit the MySQL client, and `exit` again to close your connection to the Ops Manager VM.

6. In PAS, select **Databases**.

7. Select the **External Databases** option.


 **Note:** If you configure databases as external, you cannot configure an internal database in the **UAA** pane.

8. For **Hostname**, enter the hostname of the database server.
9. For **TCP Port**, enter the port of the database server.
10. Each component that requires a relational database has two corresponding fields: one for the database username and one for the database password. For each set of fields, specify a unique username that can access this specific database on the database server and a password for the provided username.

 **Note:** Ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.

11. Click **Save**.

Step 12: (Optional) Configure Internal MySQL


 **Note:** You only need to configure this section if you have selected one of the **Internal Databases - MySQL** options in the **Databases** section.

To use internal MySQL in High Availability configuration, you define a load balancer rule that lets PAS components send queries a single hostname backed by two redundant proxies. Each proxy then directs query traffic to three MySQL server nodes.

1. Allocate an internal load balancer rule to balance traffic between two static IP addresses. The static IP addresses cannot be within the range that that you have reserved for PAS.

The load balancer rule is separate from the software provided by Pivotal, and you need to define it within your infrastructure.

- **Make your idle time out long enough to not interrupt long-running queries.** When queries take a long time, the load balancer can time out and interrupt the query.
For example, [AWS's Elastic Load Balancer](#) has a default idle timeout of 60 seconds, so queries that take longer than this duration sever the MySQL connection and return an error.
- **Configure a healthcheck or monitor, using TCP against port 1936.** This defaults to TCP port `1936`, to maintain backwards compatibility with previous releases. This port is not configurable. Unauthenticated healthchecks against port 3306 may cause the service to become unavailable and require manual intervention to fix.
- **Configure the load balancer to route traffic for TCP port 3306 to the IPs of all proxy instances on TCP port 3306.**
- Record the hostname of the load balancer rule and the two static IP addresses.

 **warning:** You must configure a load balancer to achieve complete high availability.

2. From the PAS tile in Ops Manager, Select **Internal MySQL**.
3. In the **MySQL Proxy IPs** field, enter the static IP addresses used by the internal MySQL load balancer rule.

Only configure this section if you selected Internal Databases - MySQL in the previous Databases section.

A proxy tier routes MySQL connections from internal components to healthy cluster nodes. Configure DNS and/or your own load balancer to point to multiple proxy instances for increased availability. TCP healthchecks can be configured against port 1936.


The automated backups functionality works with any S3-compatible file store that can receive your backup files.

MySQL Proxy IPs

MySQL Service Hostname

4. For **MySQL Service Hostname**, enter the IP address or hostname for your load balancer. If you leave this field blank, components are configured with the IP address of the first proxy instance entered above.

5. In the **Replication canary time period** field, leave the default of 30 seconds or modify the value based on the needs of your deployment. Lower numbers cause the canary to run more frequently, which means that the canary reacts more quickly to replication failure but adds load to the database.
6. In the **Replication canary read delay** field, leave the default of 20 seconds or modify the value based on the needs of your deployment. This field configures how long the canary waits, in seconds, before verifying that data is replicating across each MySQL node. Clusters under heavy load can experience a small replication lag as write-sets are committed across the nodes.
7. (**Required**): In the **E-mail address** field, enter the email address where the MySQL service sends alerts when the cluster experiences a replication issue or when a node is not allowed to auto-rejoin the cluster.
8. To prohibit the creation of command line history files on the MySQL nodes, disable the **Allow Command History** checkbox.
9. To allow the admin and roadmin to connect from any remote host, enable the **Allow Remote Admin Access** checkbox. When the checkbox is disabled, admins must `bosh ssh` into each MySQL VM to connect as the MySQL super user.

 **Note:** Network configuration and Application Security Groups restrictions may still limit a client's ability to establish a connection with the databases.

10. For **Cluster Probe Timeout**, enter the maximum amount of time, in seconds, that a new node will search for existing cluster nodes. If left blank, the default value is 10 seconds.

Replication canary time period *

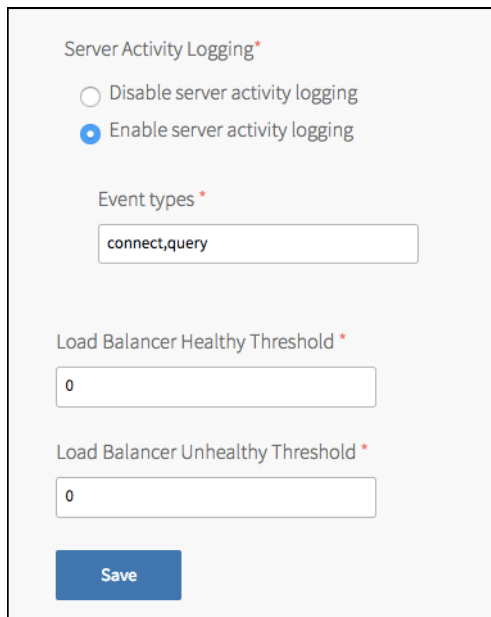
Replication canary read delay *

E-mail address (required) *

☒ Allow Command History

Cluster Probe Timeout

11. For **Max Connections**, enter the maximum number of connections allowed to the database. If left blank, the default value is 1500.
12. If you want to log audit events for internal MySQL, select **Enable server activity logging** under **Server Activity Logging**.
 - a. For the **Event types** field, you can enter the events you want the MySQL service to log. By default, this field includes `connect` and `query`, which tracks who connects to the system and what queries are processed.



The screenshot shows a configuration panel for a MySQL Proxy instance. It includes the following fields and controls:

- Server Activity Logging***: Two radio buttons. The first is "Disable server activity logging" (unselected). The second is "Enable server activity logging" (selected).
- Event types ***: A text input field containing the value "connect,query".
- Load Balancer Healthy Threshold ***: A text input field containing the value "0".
- Load Balancer Unhealthy Threshold ***: A text input field containing the value "0".
- Save**: A blue button at the bottom of the panel.

13. Enter values for the following fields:

- **Load Balancer Healthy Threshold**: Specifies the amount of time, in seconds, to wait until declaring the MySQL Proxy instance started. This allows an external load balancer time to register the instance as healthy.
- **Load Balancer Unhealthy Threshold**: Specifies the amount of time, in seconds, that the MySQL Proxy continues to accept connections before shutting down. During this period, the Healthcheck reports as unhealthy to cause load balancers to fail over to other proxies. You must enter a value greater than or equal to the maximum time it takes your load balancer to consider a proxy instance unhealthy, given repeated failed healthchecks.

14. If you want to enable the MySQL interruptor feature, select the checkbox to **Prevent node auto re-join**. This feature stops all writes to the MySQL database if it notices an inconsistency in the dataset between the nodes. For more information, see the [Interruptor](#) section in the MySQL for PCF documentation.

15. Click **Save**.

For more information on how to monitor the node health of your MySQL Proxy instances, see [Using the MySQL Proxy](#).

Step 13: Configure File Storage

For production-level PCF deployments on vSphere, the recommended selection is **External S3-Compatible** and the use of an external filestore. For more information about production-level PCF deployments on vSphere, see the [Reference Architecture for Pivotal Cloud Foundry on vSphere](#).

For more factors to consider when selecting file storage, see [Considerations for Selecting File Storage in Pivotal Cloud Foundry](#).

Internal Filestore

Internal file storage is only appropriate for small, non-production deployments.

To use the PCF internal filestore, perform the following steps:

1. In the Pivotal Application Service (PAS) tile, select **File Storage**.
2. Select **Internal WebDAV**, and click **Save**.

External S3 or Ceph Filestore

To use an external S3-compatible filestore for PAS file storage, perform the following steps:

1. In the PAS tile, select **File Storage**.

2. Select the **External S3-Compatible Filestore** option and complete the following fields:

- Enter the `https://` **URL Endpoint** for your region.
For example, in the **us-west-2** region, enter `https://s3-us-west-2.amazonaws.com/`.
- If you use an AWS instance profile to manage role information for your filestore, select the **S3 AWS with Instance Profile** checkbox. For more information, see [AWS Identity and Access Management](#) in the AWS documentation.

☒ S3 AWS with Instance Profile

Access Key (required if not using S3 AWS with Instance Profile)

Secret Key (required if not using S3 AWS with Instance Profile)

Secret

[Cancel](#)

- Alternatively, enter the **Access Key** and **Secret Key** of the `pcf-user` you created when configuring AWS for PCF. If you select the **S3 AWS with Instance Profile** checkbox and also enter an **Access Key** and **Secret Key**, the instance profile will overrule the Access Key and Secret Key.
- From the **S3 Signature Version** dropdown, select **V4 Signature**. For more information about S4 signatures, see [Signing AWS API Requests](#) in the AWS documentation.
- For **Region**, enter the region in which your S3 buckets are located. `us-west-2` is an example of an acceptable value for this field.
- Select **Server-side Encryption** to encrypt the contents of your S3 filestore. This option is only available for AWS S3.
- (Optional) If you selected **Server-side Encryption**, you can also specify a **KMS Key ID**. PAS uses the KMS key to encrypt files uploaded to the blobstore. If you do not provide a KMS Key ID, PAS uses the default AWS key. For more information, see [Protecting Data Using Server-Side Encryption with AWS KMS-Managed Keys \(SSE-KMS\)](#).
- Enter names for your S3 buckets:

| Ops Manager Field | Value | Description |
|------------------------|-----------------------|---|
| Buildpacks Bucket Name | pcf-buildpacks-bucket | This S3 bucket stores app buildpacks. |
| Droplets Bucket Name | pcf-droplets-bucket | This S3 bucket stores app droplets. Pivotal recommends that you use a unique bucket name for droplets, but you can also use the same name as above. |
| Packages Bucket Name | pcf-packages-bucket | This S3 bucket stores app packages. Pivotal recommends that you use a unique bucket name for packages, but you can also use the same name as above. |
| Resources Bucket Name | pcf-resources-bucket | This S3 bucket stores app resources. Pivotal recommends that you use a unique bucket name for app resources, but you can also use the same name as above. |

- Configure the following depending on whether your S3 buckets have versioning enabled:
 - Versioned S3 buckets:** Enable the **Use versioning for backup and restore** checkbox to archive each bucket to a version.
 - Unversioned S3 buckets:** Disable the **Use versioning for backup and restore** checkbox, and enter a backup bucket name for each active bucket. The backup bucket name must be different from the name of the active bucket it backs up.

☐ Use versioning for backup and restore.
 (All of the above buckets must have versioning enabled and use the V4 S3 Signature Version).

If versioning is not enabled or supported, you can configure separate buckets below for backups. More information at <https://docs.pivotal.io/pivotalcf/2-1/customizing/backup-restore/backup-pcf-bbr.html>.

Backup Region

Backup Buildpacks Bucket Name


Backup Droplets Bucket Name

Backup Packages Bucket Name

For more information


about setting up external S3 blobstores, see the [Backup and Restore with External Blobstores](#) topic in the Cloud Foundry documentation.

3. Click **Save**.

 **Note:** For more information regarding AWS S3 Signatures, see the [Authenticating Requests](#) topic in the AWS documentation.

Step 14: (Optional) Configure System Logging

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

 **Note:** The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?*

- ☒ No
☐ Yes

Syslog Drain Buffer Size (# of messages) *

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging

☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration

Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.



Note: The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
 - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
 - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.



Note: Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

Step 15: (Optional) Customize Apps Manager

This section describes how to configure **Custom Branding** and **Apps Manager** to customize the appearance and functionality of Apps Manager. For more information about the **Custom Branding** configuration settings, see [Custom Branding Apps Manager](#).

1. Select **Custom Branding**. Use this section to configure the text, colors, and images of the interface that developers see when they log in, create an account, reset their password, or use Apps Manager.

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name

Accent Color

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer

Classification Header/Footer Background Color

Classification Header/Footer Text Color

Classification Header Content

Classification Footer Content

Save

Add

2. Click **Save** to save your settings in this section.
3. Select **Apps Manager**.

Configure Apps Manager

☒ Enable Invitations

☐ Display Marketplace Service Plan Prices

Supported currencies as JSON *

```
{ "usd": "$", "eur": "€" }
```

Product Name

Marketplace Name

Customize Sidebar Links Add

You may configure up to 10 links in the Apps Manager sidebar.

- ▶ Marketplace 🗑️
- ▶ Docs 🗑️
- ▶ Tools 🗑️

Apps Manager Memory Usage (MB) (min: 128)

Invitations Memory Usage (MB) (min: 256)

Apps Manager Polling Interval *

30


Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save

4. Select **Enable Invitations** to enable invitations in Apps Manager. Space Managers can invite new users for a given space, Org Managers can invite new users for a given org, and Admins can invite new users across all orgs and spaces. See the [Inviting New Users](#) section of the *Managing User Roles with Apps Manager* topic for more information.
5. Select **Display Marketplace Service Plan Prices** to display the prices for your services plans in the Marketplace.
6. Enter the **Supported currencies as JSON** to appear in the Marketplace. Use the format `{ "CURRENCY-CODE": "SYMBOL" }`. This defaults to `{ "usd": "$", "eur": "€" }`.
7. Use **Product Name**, **Marketplace Name**, and **Customize Sidebar Links** to configure page names and sidebar links in the **Apps Manager** and **Marketplace** pages.
8. The **Apps Manager Memory Usage (MB)** field sets the memory limit with which to deploy the Apps Manager app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.
9. The **Invitations Memory Usage (MB)** field sets the memory limit with which to deploy the Invitations app. Use this field to increase the memory limit if the app fails to start with an `out of memory` error.

10. The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`. This stops Apps Manager from refreshing data automatically, but users can update displayed data by reloading Apps Manager manually.

11. Click **Save** to save your settings in this section.

Step 16: (Optional) Configure Email Notifications

PAS uses SMTP to send invitations and confirmations to Apps Manager users. You must complete the **Email Notifications** page if you want to enable end-user self-registration.

1. Select **Email Notifications**.

Configure Simple Mail Transfer Protocol for the Notifications application to send email notifications about your deployment. This application is deployed as an errand in Elastic Runtime. If you do not need this service, leave this section blank and disable the Notifications and Notifications UI errands.

From Email

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

[Change](#)

☒ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

SMTP CRAMMD5 secret

2. Enter your reply-to and SMTP email information.

 **Note:** For GCP, you must use port `2525`. Ports `25` and `587` are not allowed on GCP Compute Engine.

3. Verify your authentication requirements with your email administrator and use the **SMTP Authentication Mechanism** dropdown to select `None`, `Plain`, or `CRAMMD5`. If you have no SMTP authentication requirements, select `None`.

- If you selected `CRAMMD5` as your authentication mechanism, enter a secret in the **SMTP CRAMMD5 secret** field.
- Click **Save**.

Note: If you do not configure the SMTP settings using this form, the administrator must create orgs and users using the cf CLI. See [Creating and Managing Users with the cf CLI](#) for more information.

Step 17: (Optional) Configure App Autoscaler

To use App Autoscaler, you must create an instance of the service and bind it to an app. To create an instance of App Autoscaler and bind it to an app, see [Set Up App Autoscaler](#) in the *Scaling an Application Using App Autoscaler* topic.

- Click **App Autoscaler**.

Configure the App Autoscaler

Autoscaler Instance Count (min: 1) *

Autoscaler API Instance Count (min: 1) *

Metric Collection Interval (min: 60, max: 3600) (min: 60, max: 3600) *

Scaling Interval (min: 15, max: 120) (min: 15, max: 120) *

☐ Verbose Logging

☐ Disable API Connection Pooling

☒ Enable Notifications

Save

- Review the following settings:

- Autoscaler Instance Count:** How many instances of the App Autoscaler service you want to deploy. The default value is `3`. For high availability, set this number to `3` or higher. You should set the instance count to an odd number to avoid split-brain scenarios during leadership elections. Larger environments may require more instances than the default number.
- Autoscaler API Instance Count:** How many instances of the App Autoscaler API you want to deploy. The default value is `1`. Larger environments may require more instances than the default number.
- Metric Collection Interval:** How many seconds of data collection you want App Autoscaler to evaluate when making scaling decisions. The minimum interval is 60 seconds, and the maximum interval is 3600 seconds. The default value is `120`. Increase this number if the metrics you use in your scaling rules are emitted less frequently than the existing Metric Collection Interval.
- Scaling Interval:** How frequently App Autoscaler evaluates an app for scaling. The minimum interval is 15 seconds, and the maximum interval is 120 seconds. The default value is `35`.
- Verbose Logging** (checkbox): Enables verbose logging for App Autoscaler. Verbose logging is disabled by default. Select this checkbox to see more detailed logs. Verbose logs show specific reasons why App Autoscaler scaled the app, including information about minimum and maximum instance limits, App Autoscaler's status. For more information about App Autoscaler logs, see [App Autoscaler Events and Notifications](#).
- Disable API Connection Pooling:** API connection pooling increases performance by reducing the cost associated with establishing new connections. If you do not want to keep connections open for reuse, select this option.

3. Click **Save**.

Step 18: Configure Cloud Controller

1. Click **Cloud Controller**.

Configure the Cloud Controller

Cloud Controller DB Encryption Key

Secret

Enabling CF API Rate Limiting will prevent API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval. *

☐ Enable
 ☒ Disable

Save

2. Enter your **Cloud Controller DB Encryption Key** if all of the following are true:

- You deployed Pivotal Application Service (PAS) previously.
- You then stopped PAS or it crashed.
- You are re-deploying PAS with a backup of your Cloud Controller database.

See [Backing Up Pivotal Cloud Foundry](#) for more information.

3. CF API Rate Limiting prevents API consumers from overwhelming the platform API servers. Limits are imposed on a per-user or per-client basis and reset on an hourly interval.

To disable CF API Rate Limiting, select **Disable** under **Enable CF API Rate Limiting**. To enable CF API Rate Limiting, perform the following steps:

- Under **Enable CF API Rate Limiting**, select **Enable**.
- For **General Limit**, enter the number of requests a user or client is allowed to make over an hour interval for all endpoints that do not have a custom limit. The default value is `2000`.
- For **Unauthenticated Limit**, enter the number of requests an unauthenticated client is allowed to make over an hour interval. The default value is `100`.

4. Click **Save**.

Step 19: Configure Smoke Tests

The Smoke Tests errand runs basic functionality tests against your Pivotal Application Service (PAS) deployment after an installation or update. In this section, choose where to run smoke tests. In the **Errands** section, you can choose whether or not to run the Smoke Tests errand.

1. Select **Smoke Tests**.
2. If you have a shared apps domain, select **Temporary space within the system organization**, which creates a temporary space within the `system` organization for running smoke tests and deletes the space afterwards. Otherwise, select **Specified org and space** and complete the fields to specify where you want to run smoke tests.

Specify a Cloud Foundry organization and space where smoke tests can run if in the future you delete your Elastic Runtime deployment domains.

Choose where to deploy applications when running the smoke tests *

- ☐ Temporary space within the system organization (This is deleted after smoke tests finish.)
- ☒ Specified org and space (The org and space must have a domain available for routing.)

Organization *

Space *

Domain *

Save

3. Click **Save**.

Step 20: (Optional) Enable Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

Note: Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.

Cell Memory Capacity (MB) (min: 1)

Cell Disk Capacity (MB) (min: 1)

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Whitelist for Non-RFC-1918 Private Networks

Some private networks require extra configuration so that internal file storage (WebDAV) can communicate with other PCF processes.

The **Whitelist for non-RFC-1918 Private Networks** field is provided for deployments that use a non-RFC 1918 private network. This is typically a private network other than `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.

Most PCF deployments do not require any modifications to this field.

To add your private network to the whitelist, do the following:

1. Select **Advanced Features**.
2. Append a new `allow` rule to the existing contents of the **Whitelist for non-RFC-1918 Private Networks** field.

Whitelist for non-RFC-1918 Private Networks *

allow 10.0.0.0/8;;allow 172.16.0.0/12;;allow .

If your Elastic Runtime deployment is using a private network that is not RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), then you must type in "allow <your-network>;" here. It is important to include the word "allow" and the semi-colon at the end. For example, "allow 172.99.0.0/24;"

Include the word `allow`, the network CIDR range to allow, and a semi-colon (`;`) at the end. For example: `allow 172.99.0.0/24;`

3. Click **Save**.

CF CLI Connection Timeout

The **CF CLI Connection Timeout** field allows you to override the default five second timeout of the Cloud Foundry Command Line Interface (cf CLI) used within your PCF deployment. This timeout affects the cf CLI command used to push PAS errand apps such as Notifications, Autoscaler, and Apps Manager.

Set the value of this field to a higher value, in seconds, if you are experiencing domain name resolution timeouts when pushing errands in PAS.

To modify the value of the **CF CLI Connection Timeout**, perform the following steps:

1. Select **Advanced Features**.

CF CLI Connection Timeout

15

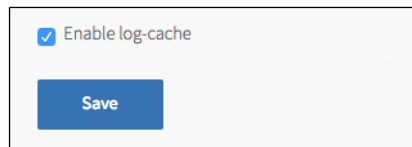
2. Add a value, in seconds, to the **CF CLI Connection Timeout** field.
3. Click **Save**.

Log Cache

Log Cache is an in-memory caching layer for logs and metrics. This Loggregator feature lets users filter and query logs through a CLI or API endpoints. Cached logs are available on demand. For more information about Log Cache, see [Enable Log Cache](#) in the *Configuring Logging in PASTopic*.

To configure the **Enable log-cache** checkbox, do the following:

1. Select **Advanced Features**.



A screenshot of a configuration panel. It contains a checkbox labeled 'Enable log-cache' which is checked. Below the checkbox is a blue button labeled 'Save'.

2. Select or deselect the **Enable log-cache** checkbox.
3. Click **Save**.

Database Connection Limits

You can configure the maximum number of concurrent database connections that diego and container networking components can have. Use the field beginning with **Maximum number of open connections...** for a given component. The placeholder values for each field are the default values.

When there are not enough connections available, such as during a time of heavy load, components may experience degraded performance and sometimes failure. To resolve or prevent this, you can increase and fine-tune database connection limits for the component.

⚠ warning: Decreasing the value of this field for a component may affect the amount of time it takes for it to respond to requests.

Step 21: Configure Errands

Errands are scripts that Ops Manager runs automatically when it installs or uninstalls a product, such as a new version of Pivotal Application Service (PAS). There are two types of errands: *post-deploy errands* run after the product is installed, and *pre-delete errands* run before the product is uninstalled.

By default, Ops Manager always runs all errands.

The PAS tile **Errands** pane lets you change these run rules. For each errand, you can select **On** to run it always or **Off** to never run it.

For more information about how Ops Manager manages errands, see the [Managing Errands in Ops Manager](#) topic.

💡 Note: Several errands, such as App Autoscaler and Notifications, deploy apps that provide services for your deployment. When one of these apps is running, selecting **Off** for the corresponding errand on a subsequent installation does not stop the app.

- **Smoke Test Errand** verifies that your deployment can do the following:
 - Push, scale, and delete apps
 - Create and delete orgs and spaces
- **Usage Service Errand** deploys the Pivotal Usage Service application, which Apps Manager depends on.
- **Apps Manager Errand** deploys Apps Manager, a dashboard for managing apps, services, orgs, users, and spaces. Until you deploy Apps Manager, you must perform these functions through the cf CLI. After Apps Manager has been deployed, Pivotal recommends setting this errand to **Off** for subsequent PAS deployments. For more information about Apps Manager, see the [Getting Started with the Apps Manager](#) topic.
- **Notifications Errand** deploys an API for sending email notifications to your PCF platform users.

💡 Note: The Notifications app requires that you [configure SMTP](#) with a username and password, even if you set the value of **SMTP Authentication Mechanism** to `none`.

- **Notifications UI Errand** deploys a dashboard for users to manage notification subscriptions.
- **App Autoscaler Errand** enables you to configure your apps to automatically scale in response to changes in their usage load. See the [Scaling an Application Using Autoscaler](#) topic for more information.
- **NFS Broker Errand** enables you to use NFS Volume Services by installing the NFS Broker app in PAS. See the [Enabling NFS Volume Services](#) topic for more information.

Step 22: (Optional) Disable Unused Resources

💡 Note: The **Resource Config** pane has fewer VMs if you are installing the [Small Footprint Runtime](#).

Note: The Small Footprint Runtime does not default to a highly available configuration. It defaults to the minimum configuration. If you want to make the Small Footprint Runtime highly available, scale the **Compute**, **Router**, and **Database** VMs to **3** instances and scale the **Control** VM to **2** instances.

Pivotal Application Service (PAS) defaults to a highly available resource configuration. However, you may need to perform additional procedures to make your deployment highly available. See the [Zero Downtime Deployment and Scaling in CF](#) and the [Scaling Instances in PAS](#) topics for more information.

If you do not want a highly available resource configuration, you must scale down your instances manually by navigating to the **Resource Config** section and using the dropdowns under **Instances** for each job.

By default, PAS also uses an internal filestore and internal databases. If you configure PAS to use external resources, you can disable the corresponding system-provided resources in Ops Manager to reduce costs and administrative overhead.

To disable specific VMs in Ops Manager, do the following:

1. Click **Resource Config**.
2. If you configured PAS to use an external S3-compatible filestore, enter **0** in **Instances** in the **File Storage** field.
3. If you selected **External** when configuring the UAA, System, and CredHub databases, edit the following fields:
 - MySQL Proxy: Enter **0** in **Instances**.
 - MySQL Server: Enter **0** in **Instances**.
 - MySQL Monitor: Enter **0** in **Instances**.
4. If you disabled TCP routing, enter **0** **Instances** in the **TCP Router** field.
5. If you are not using HAProxy, enter **0** **Instances** in the **HAProxy** field.
6. Click **Save**.

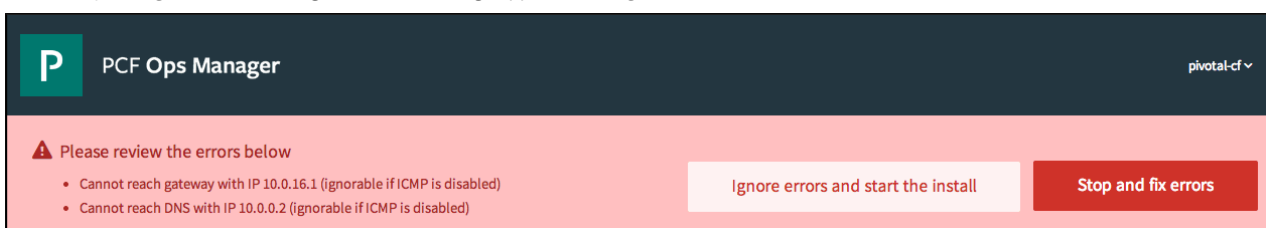
Step 23: Download Stemcell

This step is only required if your Ops Manager does not already have the stemcell version required by PAS. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

1. Open the [Stemcell product page](#) in the Pivotal Network. *Note, you may have to log in.*
2. Download the appropriate stemcell version targeted for your IaaS.
3. Navigate to **Stemcell Library** in the **Installation Dashboard**.
4. Click **Import Stemcell** to import the downloaded stemcell **.tgz** file.
5. When prompted, enable the Ops Manager product checkbox to stage your stemcell.
6. Click **Apply Stemcell to Products**.

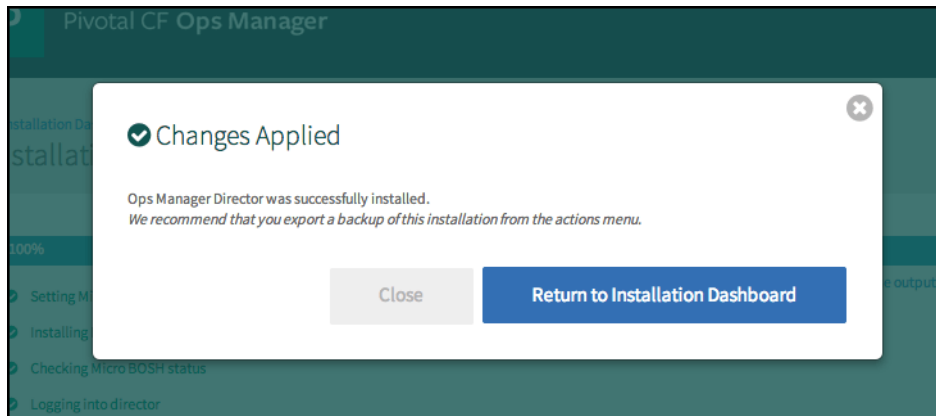
Step 24: Complete the PAS Installation

1. Click the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click **Apply Changes**. If the following ICMP error message appears, click **Ignore errors and start the install**.



The install process generally requires a minimum of 90 minutes to complete. The image shows the Changes Applied window that displays when the

installation process successfully completes.



Deploying PAS with NSX-T Networking

Page last updated:

This topic describes how to install Pivotal Application Service (PAS) on vSphere with NSX-T internal networking, using the VMware NSX-T Container Plug-in for PCF.

Overview

PAS v2.0 uses a Container Network Interface (CNI) plugin to support secure and direct internal communication between containers. This plugin can be:

- The internal Silk plugin that comes packaged with PAS, or
- On vSphere, [VMware NSX-T Container Plug-in for PCF](#), which installs as an Ops Manager tile.

Prerequisites

Before deploying PAS with NSX-T networking, you must have the following:

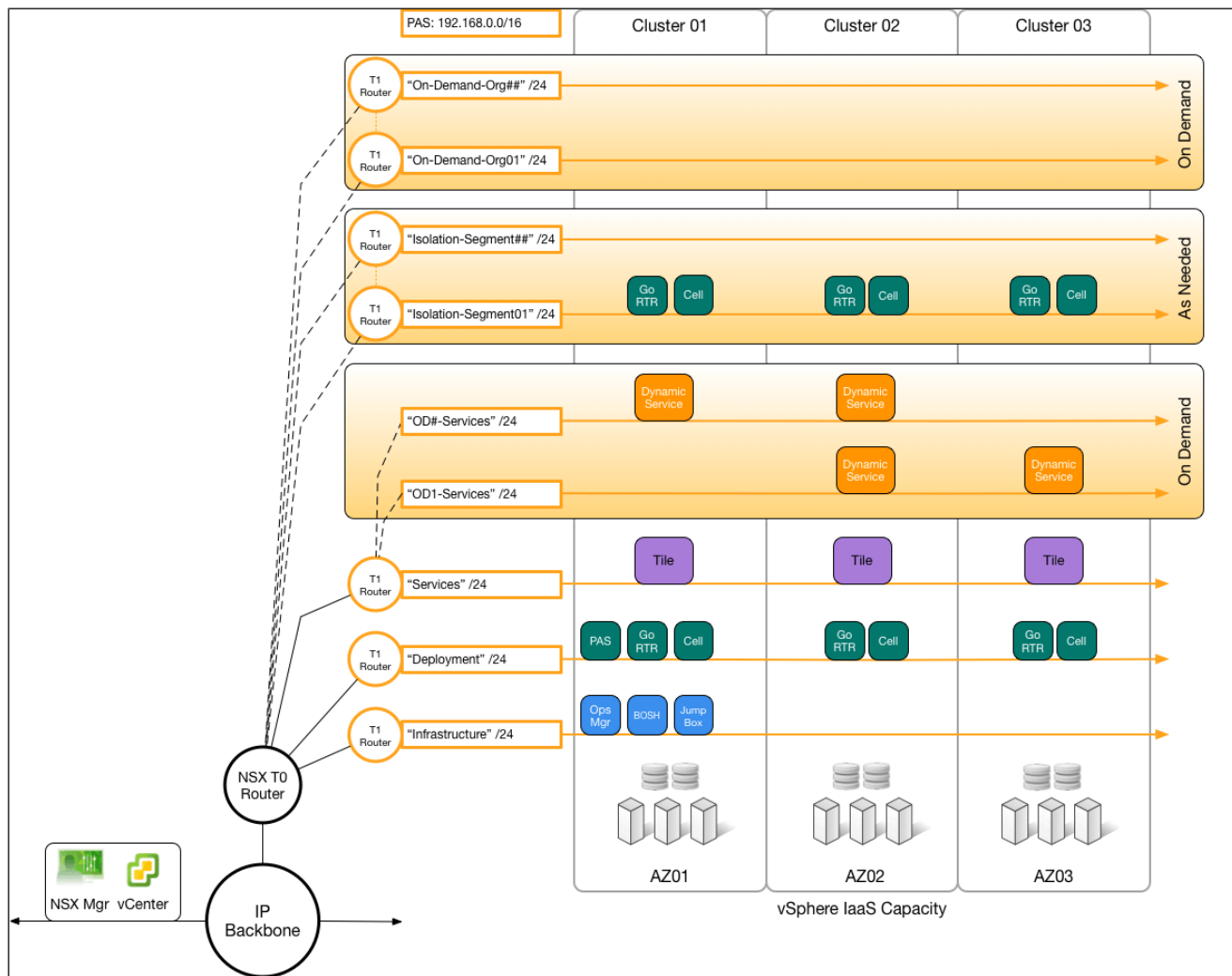
- An NSX-T 2.2 or later environment with NSX-T components installed and configured. See the [NSX-T Cookbook](#) for directions.
- BOSH and Ops Manager v2.3 or later installed and configured on vSphere. See [Deploying Ops Manager on vSphere](#) and [Configuring BOSH Director on vSphere](#).
- The [VMware NSX-T Container Plug-in for PCF tile](#) downloaded from Pivotal Network and imported to the Ops Manager **Installation Dashboard**. See [Adding and Importing Products](#) for how to download and import Pivotal products to the **Installation Dashboard**.
- The [PAS tile](#) downloaded from Pivotal Network and imported to the Ops Manager **Installation Dashboard**. The PAS tile must be in one of the following two states:
 - Not deployed yet; you have not yet run **Apply Changes** on this version of PAS.
 - Deployed previously, with the **Networking** pane > **Container Network Interface Plugin** set to **External**.



Note: Deploying PAS with its Container Network Interface (CNI) set to **Silk** configures Diego cells to use an internally-managed container network. Subsequently switching the CNI interface to **External** NSX-T leads to errors.

Architecture

The following diagram shows how to deploy an NSX-T machine to run PAS across multiple vSphere hardware clusters. NSX-T runs a Tier-0 (T0) router and multiple Tier-1 (T1) routers, each connecting to a network within Pivotal Cloud Foundry. Each vSphere hardware column cluster corresponds to an Availability Zone in PCF:



When a developer pushes an app to a new Org for the first time, the NSX-T plugin triggers NSX-T to create a new T1 router and allocate an address range for the Org, on demand.

Install and Configure PAS and NSX-T

Installing NSX-T to run with PAS requires the following actions, which are described below:

1. [Set up NSX-T to Integrate with PAS](#)
2. [Enable NSX-T Mode in the BOSH Director](#)
3. [Configure PAS for External Container Networking](#)
4. [Install and Configure the NSX-T Tile](#)

Set up NSX-T to Integrate with PAS

1. In vSphere, create logical network switches to correspond to the networks that PCF uses.
 - a. Log into the **NSX Manager Dashboard**.
 - b. Open the **Switching** tab.
 - c. For each of these networks...
 - **Infrastructure** (BOSH and Ops Manager, defined in BOSH Director tile > **Assign AZs and Networks** pane)
 - **Deployment** (PAS, defined in PAS tile > **Assign AZs and Networks** pane)
 - **Services and Dynamic Services** (marketplace services and on-demand services, also defined in the PAS tile)
 - **Isolation Segment** (optional, defined in the Isolation Segment tile > **Assign AZs and Networks** pane)

...do the following:

1. Click **Add New Logical Switch**.
2. Enter a name for the logical switch (e.g. `infrastructure-ls`, `deployment-ls`).

Add New Logical Switch

General Switching Profiles

Name * infrastructure-ls

Description

Transport Zone * tz-overlay

Admin Status ☒ Up

Replication Mode ☒ Hierarchical Two-Tier replication ☐ Head replication

VLAN *

SAVE **CANCEL**

3. Click **Save**.

2. Create T0 network address translation (NAT) rules to facilitate communication between Ops Manager and the BOSH Director.

- a. Create and configure a T0 router and router port for PCF.
- b. In NSX Manager, select your T0 Router and navigate to **Services > NAT**.
- c. Add a rule for destination NAT (DNAT) with:
 - The externally-specified destination IP address of incoming requests
 - The internal network address to translate the external address to

New NAT Rule

Priority 1024

Action * DNAT

Protocol ☒ Any Protocol ☐ Specific Protocol

Source IP

Destination IP * 10.193.253.65

Translated IP * 192.168.1.10

Translated Ports

Status ☒ Enabled

Logging ☐ Disabled

Firewall Bypass ☒ Enabled

SAVE **CANCEL**

- d. Add a rule for source NAT (SNAT) with:

- The range of internal addresses that outgoing traffic may come from

- The external IP address to put in each outgoing packet header, indicating its source

New NAT Rule

Priority

1024

Action *

SNAT

Protocol

☒ Any Protocol
 ☐ Specific Protocol

Source IP

192.168.1.0/24

Destination IP

Translated IP *

10.193.253.66

Status

☒ Enabled

Logging

☐ Disabled

Firewall Bypass

☒ Enabled

SAVE

CANCEL

3. Create T1 Routers for PAS, to connect from the T0 router. For each PCF network, Infrastructure, Deployment, and so on, create a T1 router as follows:

- In the NSX Manager UI, navigate to **Routing > Routers**
- Click **Add > Tier-1 Router**.
- Configure the router. For example, the Infrastructure network router configuration might look like:

New Tier-1 Router

Tier-1 Router

Advanced

Name *

infrastructure-t1

Description

Tier-0 Router

router-t0

Failover Mode

☒ Preemptive
 ☐ Non-Preemptive

Edge Cluster

edge-cluster-01

Edge Cluster Members ⓘ

Preferred Member ⓘ

SAVE

CANCEL

4. Create T1 router ports for PAS. For each T1 router you created, add a **New Router Port** as follows, to allow traffic in and out:

- In the NSX Manager UI, select the T1 router.
- In **Configuration > Router Ports**, add a new router port.
- For **Logical Switch**, enter the name of the logical switch you defined for the network in **Add New Logical Switch**, above.

New Router Port

Name *

Description

Logical Switch

[OR Create a New Switch](#)

Logical Switch Port

☒ Attach to new switch port

☐ Attach to existing switch port

IP Address/mask *

Relay Service

SAVE

CANCEL

5. Advertise the routes of the T1 routers to the T0 router, so the T0 router can correctly route incoming requests based on their destination IP address:

- Select your T1 Router and navigate to **Routing > Route Advertisement**.
- Under **Edit Route Advertisement Configuration**, enable route advertisement by setting **Status** to **Enabled**.
- Set **Advertise All NSX Connected Routes** to **Yes**.
- If you are using NSX-T Load Balancers to route traffic, set **Advertise All LB VIP Routes** and **Advertise All LB SNAT IP Routes** to **Yes**.

Edit Route Advertisement Configuration

Status

☒ Enabled

Advertise All NSX Connected Routes

☒ Yes

Advertise All NAT Routes

☐ No

Advertise All Static Routes

☐ No

Advertise All LB VIP Routes

☒ Yes

Advertise All LB SNAT IP Routes

☒ Yes

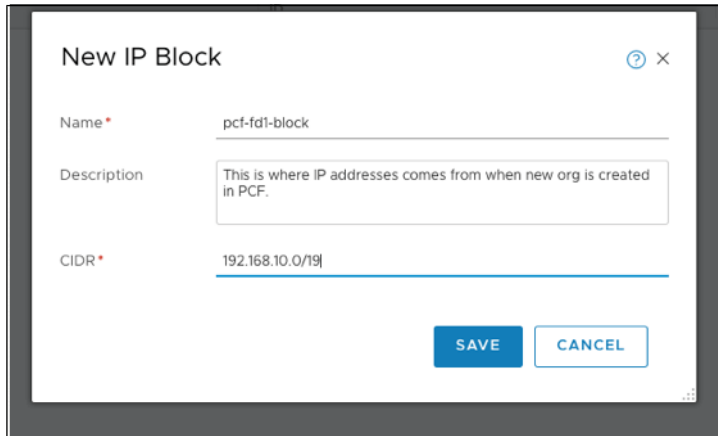
CANCEL

SAVE

6. Allocate an IP Block for PAS Orgs.

- From NSX Manager, navigate to **DDI > IPAM > New IP block**.

- b. Enter a description, such as `This is where IP addresses come from when a new Org is created in PAS.`
- c. Enter a CIDR to allocate an address block large enough to accommodate all PAS apps.

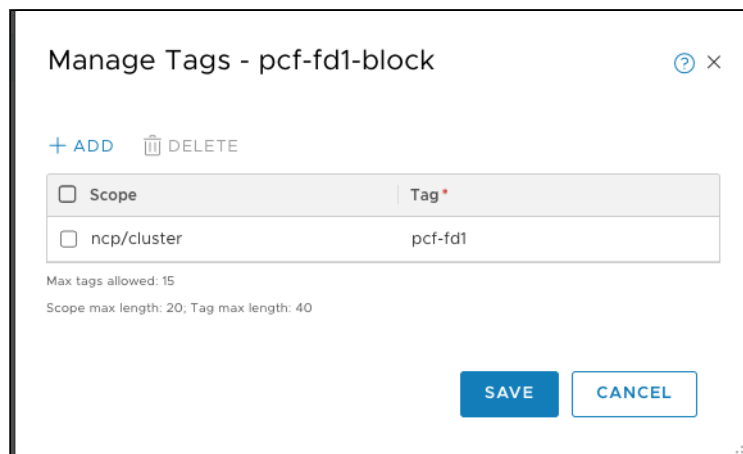


New IP Block ⓘ ×

Name *

Description

CIDR *



Manage Tags - pcf-fd1-block ⓘ ×

[+ ADD](#) [DELETE](#)

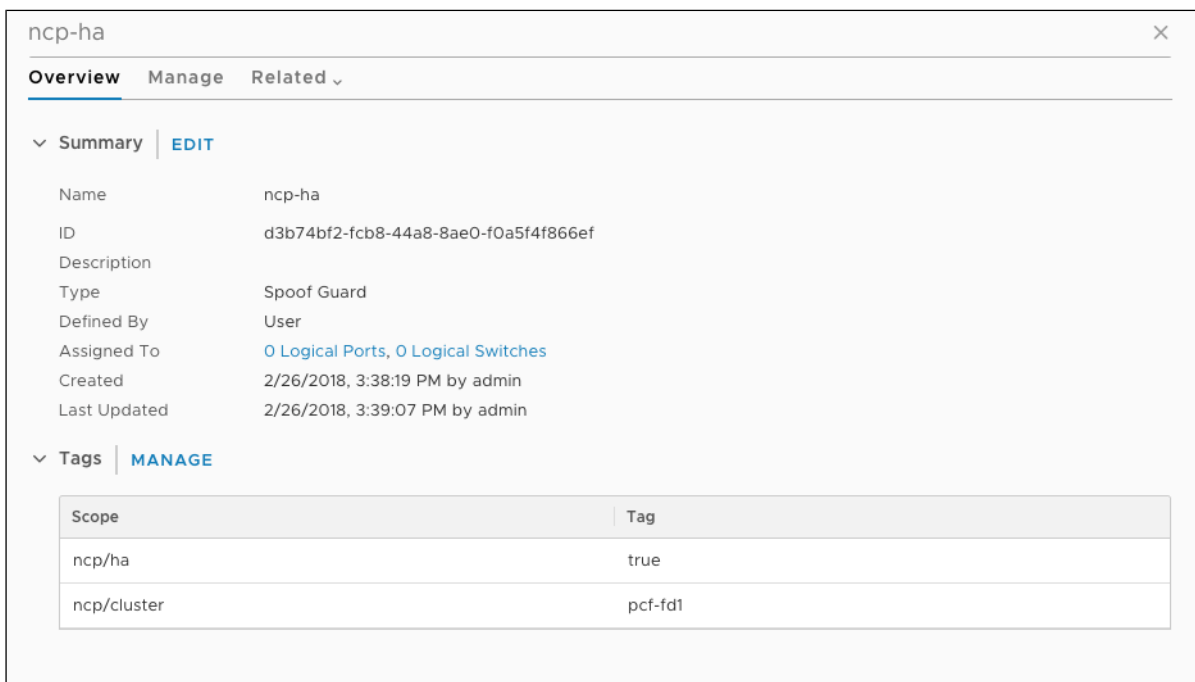
| <input type="checkbox"/> Scope | Tag * |
|--------------------------------------|---------|
| <input type="checkbox"/> ncp/cluster | pcf-fd1 |

Max tags allowed: 15
Scope max length: 20; Tag max length: 40

- d. Add a tag to the newly-created IP block.

7. Create a new switching profile with the following fields and tags:

- **Name:** `ncp-ha`
- **Type:** `Spoof Guard`
- **Tags:** Add a tag with **Scope** `ncp/ha`, **Tag** `True`
- **Tags:** Add a second tag with the **Scope** and **Tag** name of the T0 router tag you defined above.



ncp-ha ×

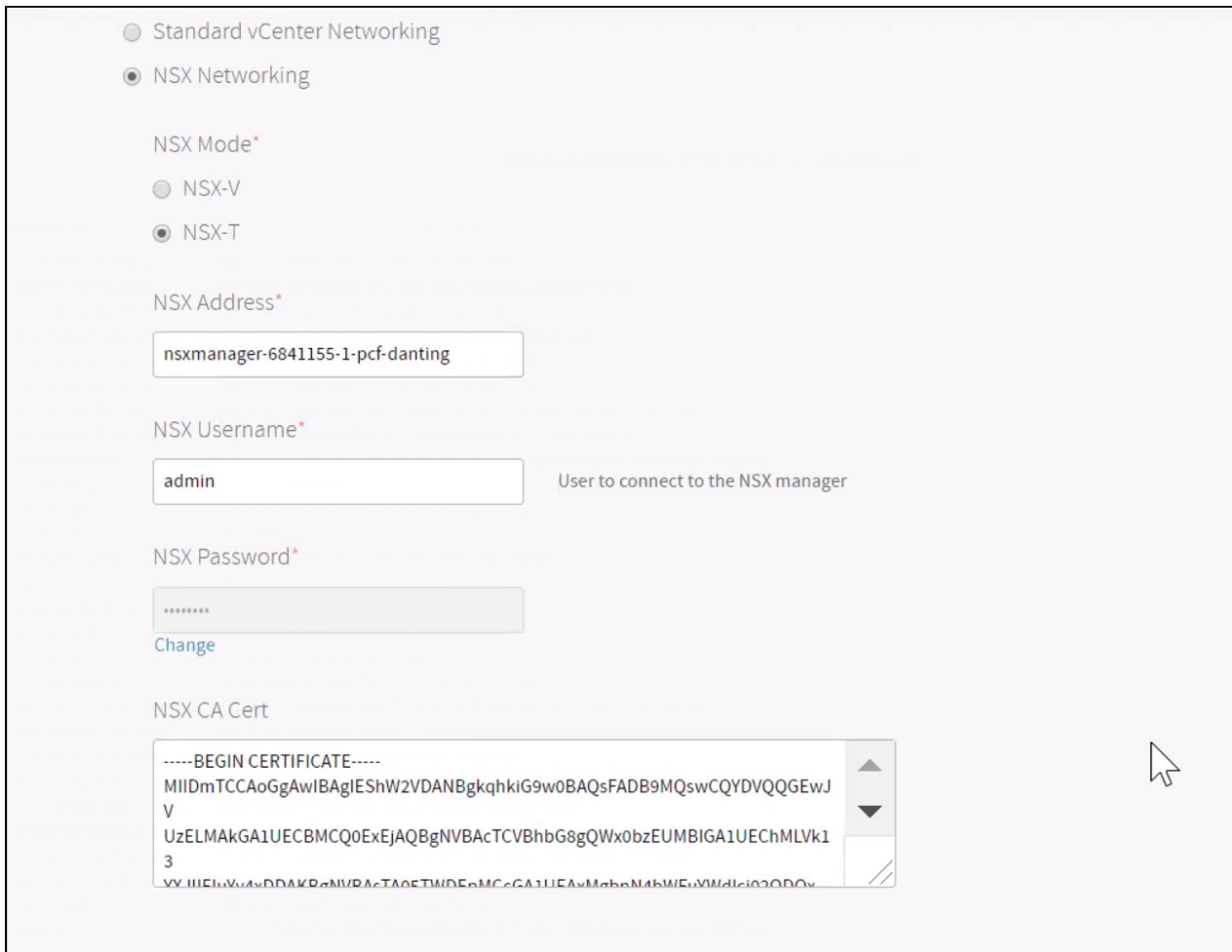
Overview Manage Related ▾

▼ Summary | [EDIT](#)

| | |
|--------------|---|
| Name | ncp-ha |
| ID | d3b74bf2-fcb8-44a8-8ae0-f0a5f4f866ef |
| Description | |
| Type | Spoof Guard |
| Defined By | User |
| Assigned To | 0 Logical Ports, 0 Logical Switches |
| Created | 2/26/2018, 3:38:19 PM by admin |
| Last Updated | 2/26/2018, 3:39:07 PM by admin |

▼ Tags | [MANAGE](#)

| Scope | Tag |
|-------------|---------|
| ncp/ha | true |
| ncp/cluster | pcf-fd1 |



Standard vCenter Networking

☒ NSX Networking

NSX Mode*

☐ NSX-V

☒ NSX-T

NSX Address*

nsxmanager-6841155-1-pcf-danting

NSX Username*

admin

User to connect to the NSX manager

NSX Password*


[Change](#)

NSX CA Cert

```
-----BEGIN CERTIFICATE-----
MIIDmTCCAAoGgAwIBAgIEShW2VDANBgkqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJ
V
UzELMAkGA1UECBMCQ0ExEjAQBgNVBACTCVBhbG8gQWx0bzEUMBIGA1UEChMLVk1
3
XYJUElEwYw4wDQAKRgNVBACTA0STWDEoMCcGA1UEFyMm90bWdldi03ODQw
-----END CERTIFICATE-----
```

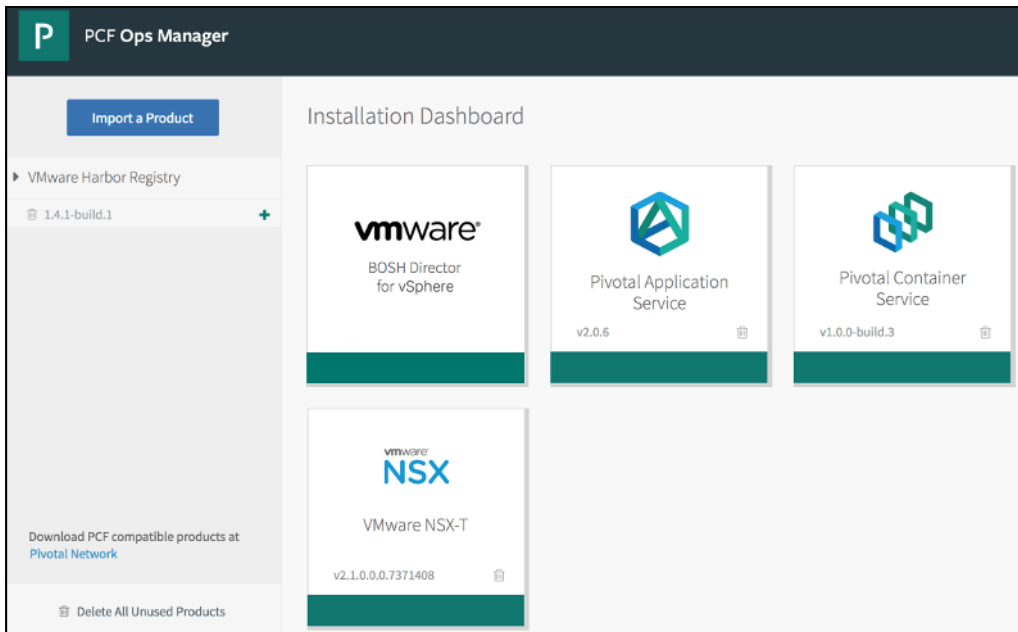
3. Configure NSX networking by entering the following:

- **NSX Mode:** Select **NSX-T**.
- **NSX Address:** Enter the address of the NSX Manager.
- **NSX Username:** Enter the username to connect to the NSX Manager.
- **NSX Password:** The password for the username specified above.
- **NSX CA Cert:** A CA certificate in PEM format that authenticates to the NSX server. If the NSX Manager generated a self-signed certificate, you can retrieve the CA certificate using OpenSSL with the command `openssl s_client -host NSX-ADDRESS -port 443 -prexit -showcerts`.

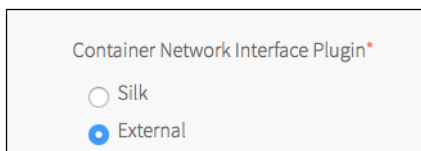
 **Note:** To update NSX security group and load balancer information, see the [Updating NSX Security Group and Load Balancer Information](#) topic.

Configure PAS for External Container Networking

1. If you have not already done so, download the PAS tile from [Pivotal Network](#) and import it to the **Installation Dashboard**. See [Adding and Importing Products](#) for directions.

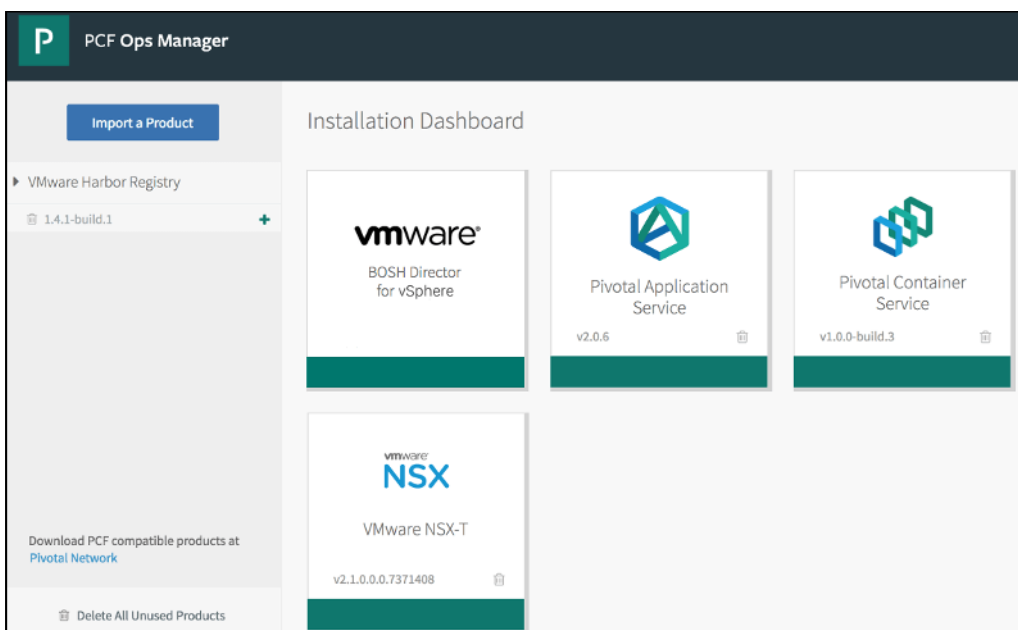


2. Configure PAS, following the directions in [Deploying PAS on vSphere](#). When you configure **Networking**, select **External** under **Container Networking Interface Plugin**.



Install and Configure the NSX-T tile

1. If you have not already done so, download the VMware NSX-T tile from [Pivotal Network](#) and import it to the **Installation Dashboard**. See [Adding and Importing Products](#) for directions.



2. Click the **VMware NSX-T** tile to open its **Settings** tab, and configure the **NSX Manager** pane as follows:
 - **NSX Manager Address:** NSX Manager host address or IP address
 - **Use Client Certificates or Username/Password:** Select **Basic Authentication with Username and Password** and enter **NSX Manager Admin Username** and **Admin Password** credentials in the fields underneath.
 - **NSX Manager CA Cert:** Obtain this certificate from NSX Manager as follows:

1. `ssh` into NSX Manager using the admin account that you created when you deployed NSX Manager.
2. From the NSX Manager command line, run `get certificate api` to retrieve the certificate.

The screenshot shows the VMware NSX-T Installation Dashboard. The top navigation bar includes 'Installation Dashboard', 'Settings', 'Status', 'Credentials', and 'Logs'. The left sidebar shows a list of components: NSX Manager (checked), NCP (checked), and NSX Node Agent (checked). The main content area is titled 'NSX Manager Configuration'. It contains the following fields and options:

- NSX Manager Address ***: A text input field containing 'nsx-manager.haas-108.pez.pivotal.io'.
- Use Client Certificates or Username/Password for NSX Manager Authentication ***: Two radio button options. 'Client Certificate Authentication' is unselected, and 'Basic Authentication with Username and Password' is selected.
- NSX Manager Admin Username ***: A text input field containing 'admin'. A label 'Admin username of NSX Manager' is to the right.
- NSX Manager Admin Password ***: A password input field with masked characters '*****'. A 'Change' link is below the field.
- NSX Manager CA Cert**: A text input field containing '-----BEGIN CERTIFICATE-----'.

3. Open and configure the **NCP** (NSX-T Container Plugin) pane as follows:

- **PAS Foundation Name**: The tag string you gave to the `t0 router` in NSX Manager, above.
- **Overlay Transport Zone**: A uniquely identifying string for the **Transport Zone** that you chose when you [created logical switches](#) for each network. This can be the name of the transport zone if no other zones in NSX share the same name, or else the UUID for the transport zone.
- **Tier-0 Router**: A uniquely identifying string for the T0 router. This can be the tag string that you gave the router in NSX Manager if no other T0 routers in NSX share the same name, or else the UUID for the router.
- **Subnet Prefix of Container Networks**: Subnet mask to set the address range size for apps in a single org. Defaults to `24`. This number must be higher than the mask for all PAS orgs in the NSX Manager **New IP Block** pane, to define a each Org's fraction of the total PAS address space.
- **Enable SNAT for Container Network**: Enable this checkbox.

NCP Configuration

PAS Foundation Name *

Overlay Transport Zone *

This string uniquely identifies the NSX overlay transport zone for logical switches for container networking. You can specify the name or the UUID of the transport zone to be used.

Tier-0 Router *

IP Blocks of Container Networks

Subnet Prefix of Container Networks *

☒ Enable SNAT for Container Networks

IP Pools used to provide External (NAT) IP Addresses to Org Networks

Top Firewall Section Marker

Bottom Firewall Section Marker

☐ Log Dropped Application Traffic

☐ Enable Debug Level for NCP Logging

Save

- In the **NSX Node Agent** pane, enable the **Enable Debug Level of Logging for NSX Node Agent** checkbox.



NSX Node Agent Configuration

☒ Enable Debug Level of Logging for NSX Node Agent

Save

- Click **Save** and return to the **Installation Dashboard**.
- After you have configured both the **PAS** tile and the **VMware NSX-T** tile, click **Apply Changes** to deploy PAS with NSX-T networking.

Automation

- [Concourse Pipelines: Configure NSX-T for PAS](#) : This sample Concourse pipeline provides jobs setup switches, routers, an IP block, and an IP pool to be used by PAS.
- [PyNSXT](#) : This is a Python library that can be used as a CLI to run commands against a VMWare NSX-T installation. It exposes operations for working with logical switches, logical routers, and pools. It uses version 2.1 of NSX-T for the swagger client.

vSphere Virtual Disk Types

Page last updated:

When you create a virtual machine in VMware vSphere, vSphere creates a new virtual hard drive for that virtual machine. The virtual hard drive is contained in a virtual machine disk (VMDK). The disk format you choose for the new virtual hard drive can have a significant impact on performance.

You can choose one of three formats when creating a virtual hard drive:

- Thin Provisioned
- Thick Provisioned Lazy Zeroed
- Thick Provisioned Eager Zeroed

Thin Provisioned

Advantages:

- Fastest to provision
- Allows disk space to be overcommitted to VMs

Disadvantages:

- Slowest performance due to metadata allocation overhead and additional overhead during initial write operations
- Overcommitment of storage can lead to application disruption or downtime if resources are actually used
- Does not support clustering features

When vSphere creates a thin provisioned disk, it only writes a small amount of metadata to the datastore. It does not allocate or zero out any disk space. At write time, vSphere first updates the allocation metadata for the VMDK, then zeros out the block or blocks, then finally writes the data. Because of this overhead, thin provisioned VMDKs have the lowest performance of the three disk formats.

Thin provisioning allows you to overcommit disk spaces to VMs on a datastore. For example, you could put 10 VMs, each with a 50 GB VMDK attached to it, on a single 100 GB datastore, as long as the sum total of all data written by the VMs never exceeded 100 GB. Thin provisioning allows administrators to use space on datastores that would otherwise be unavailable if using thick provisioning, possibly reducing costs and administrative overhead.

Thick Provisioned Lazy Zeroed

Advantages:

- Faster to provision than Thick Provisioned Eager Zeroed
- Better performance than Thin Provisioned

Disadvantages:

- Slightly slower to provision than Thin Provisioned
- Slower performance than Thick Provisioned Eager Zero
- Does not support clustering features

When vSphere creates a thick provisioned lazy zeroed disk, it allocates the maximum size of the disk to the VMDK, but does nothing else. At the initial access to each block, vSphere first zeros out the block, then writes the data. Performance of a thick provisioned lazy zeroed disk is not as good a thick provisioned eager zero disk because of this added overhead.

Thick Provisioned Eager Zeroed

Advantages:

- Best performance
- Overwriting allocated disk space with zeros reduces possible security risks
- Supports clustering features such as Microsoft Cluster Server (MSCS) and VMware Fault Tolerance

Disadvantages:

- Longest time to provision

When vSphere creates a thick provisioned eager zeroed disk, it allocates the maximum size of the disk to the VMDK, then zeros out all of that space.

Example: If you create an 80 GB thick provisioned eager zeroed VMDK, vSphere allocates 80 GB and writes 80 GB of zeros.

By overwriting all data in the allocated space with zeros, thick provisioned eager zeroed eliminates the possibility of reading any residual data from the disk, thereby reducing possible security risks.

Thick provisioned eager zeroed VMDKs have the best performance. When a write operation occurs to a thick provisioned eager zeroed disk, vSphere writes to the disk, with none of the additional overhead required by thin provisioned or thick provisioned lazy zeroed formats.

Using the Cisco Nexus 1000v Switch with Ops Manager

Page last updated:

Refer to the procedure in this topic to use Ops Manager with the Cisco Nexus 1000v Switch. First, configure Ops Manager through Step 4 in [Configuring BOSH Director on vSphere](#). Then configure your network according to the following steps.

1. From your [Pivotal Cloud Foundry](#) (PCF) Ops Manager **Installation Dashboard**, click the **BOSH Director** tile.
2. Select **Create Networks**.
3. Click the network name to configure the network settings. This is **default** if you have not changed the name.

Installation Dashboard

Ops Manager Director

Settings Status Credentials

- ✓ vCenter Config
- ✓ Director Config
- ✓ Create Availability Zones
- ✓ **Create Networks**
- ✓ Assign AZs and Networks
- ✓ Security
- ✓ Resource Config

Create Networks

Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future. Contact Pivotal support for help completing such a change.

Verification Settings

☒ Enable ICMP checks

Networks

One or many IP ranges upon which your products will be deployed

▼ default

Name*

default

A unique name for this network

Subnets

vSphere Network Name*

CIDR*

Reserved IP Ranges

DNS*

Gateway*

Availability Zones*

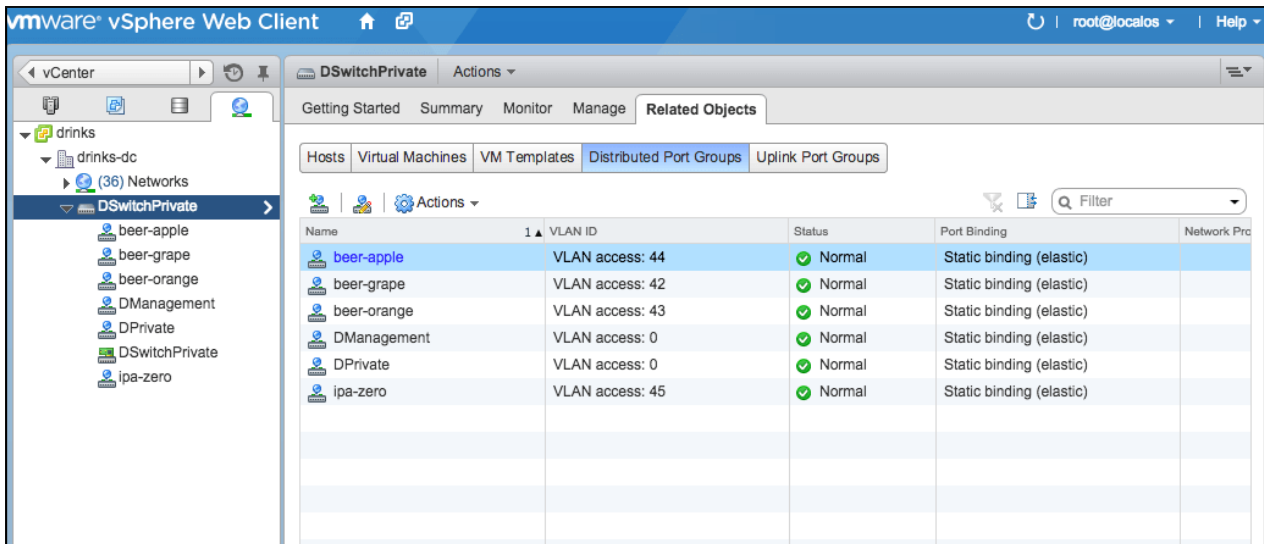
☐ first-az

Save

Add Network

Add Subnet

4. Find the folder name and port group name for the switch, as you configured them in vCenter. For the example vSphere environment pictured below, a user might want to use the switch configured on the `beer-apple` port group, which is in the `drinks-dc` folder.



5. In the **vSphere Network Name** field, instead of entering your network name, enter the folder name and port group name for the switch, as you configured them in vCenter. For the example vSphere environment pictured above, you would enter `drinks-dc/beer-apple` to use the switch configured on the `beer-apple` port group.

[Installation Dashboard](#)

Ops Manager Director

Settings
Status
Credentials

✓ vCenter Config

✓ Director Config

✓ Create Availability Zones

✓ Create Networks

✓ Assign AZs and Networks

✓ Security

✓ Resource Config

Create Networks

Warning: Pivotal recommends keeping the IP settings throughout the life of your installation. Ops Manager may prevent you from changing them in the future. Contact Pivotal support for help completing such a change.

Verification Settings

☒ Enable ICMP checks

Networks

One or many IP ranges upon which your products will be deployed

▼ YOUR_NETWORK_NAME

Name*

YOUR_NETWORK_NAME

Subnets

vSphere Network Name*

drinks-dc/beer-apple

The name of the network as it appears in vCenter

CIDR*

Reserved IP Ranges

DNS*

Gateway*

Availability Zones*

☐ first-az

Add Network

Add Subnet

Save

6. Click **Save**.

7. Return to [Configuring BOSH Director on vSphere](#) to complete the Ops Manager installation.

Using BOSH Resurrector and vSphere HA

Page last updated:

This topic describes the BOSH Resurrector and vSphere High Availability (HA), as well as how to enable them for your Pivotal Cloud Foundry (PCF) deployment.

Pivotal recommends BOSH Resurrector, vSphere HA, and a highly-available storage solution to protect the VMs in your deployment.

BOSH Resurrector

The following sections describe the BOSH Resurrector and how to enable it.

About BOSH Resurrector

The BOSH Resurrector increases Pivotal Application Service (PAS) availability in the following ways:

- Reacts to hardware failure and network disruptions by recreating virtual machines on active, stable hosts
- Detects operating system failures by continuously monitoring virtual machines and recreating them as required
- Continuously monitors the BOSH Agent running on each virtual machine and recreates the VMs as required

The BOSH Resurrector continuously monitors the status of all virtual machines in an PAS deployment. The Resurrector also monitors the BOSH Agent on each VM. If either the VM or the BOSH Agent fail, the Resurrector recreates the virtual machine on another active host.

BOSH Resurrector Limitations

The following limitations apply to using the BOSH Resurrector:

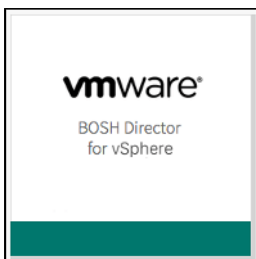
- The Resurrector does not monitor or protect the Ops Manager VM or the BOSH Director VM.
- The Resurrector might not be able to resolve issues caused by the loss of an entire host.
- The Resurrector does not monitor or protect data storage.

To mitigate these limitations, Pivotal recommends vSphere HA. For more information, see [vSphere HA](#) below.

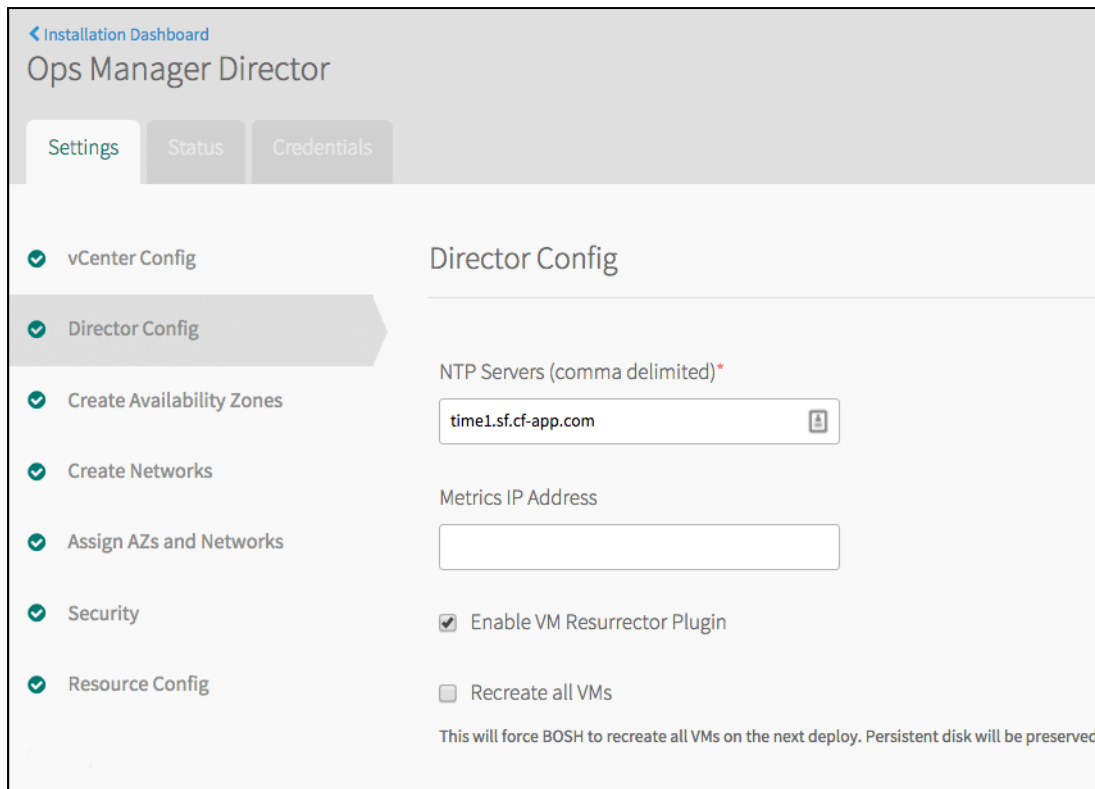
Enable BOSH Resurrector

To enable the BOSH Resurrector:

1. Log into the Ops Manager web interface.
2. On the Product Dashboard, select **BOSH Director**.



3. In the left navigation menu, select **Director Config**.



4. Select **Enable VM Resurrector Plugin** and click **Save**.

vSphere HA

The following sections describe vSphere HA and how to enable it.

About vSphere HA

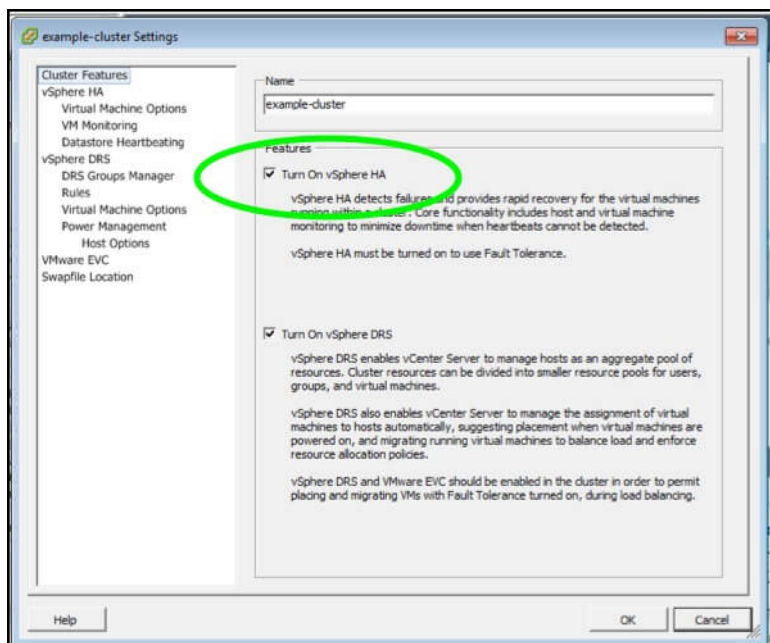
In the event of a host failure, vSphere HA restarts but does not recreate VMs on alternate ESXi hosts in the same cluster. A host failure could result from a sudden power off, crash due to hardware fault, or the vSphere host becoming disconnected from the network. BOSH Resurrector cannot recover from a host failure.

For more information, see [vSphere High Availability](#) in the BOSH documentation.

Enable vSphere HA

Follow the steps below to enable vSphere High Availability:

1. Launch the vSphere Management Console.
2. Right-click the cluster that contains the [Pivotal Cloud Foundry](#) deployment and select **Edit Settings**.
3. Select the **Turn on vSphere High Availability** checkbox.



4. Click **OK** to enable vSphere High Availability on the cluster.

Configuring Pivotal Cloud Foundry SSL Termination for vSphere Deployments

Page last updated:


To use SSL termination in [Pivotal Cloud Foundry](#) (PCF), you must configure the Pivotal-deployed HAProxy load balancer or your own load balancer.

Pivotal recommends that you use HAProxy in lab and test environments only. Production environments should instead use a highly-available customer-provided load balancing solution.

Select an SSL termination method to determine the steps you must take to configure Pivotal Application Service (PAS).

Using the Pivotal HAProxy Load Balancer

PCF deploys with a single instance of HAProxy for use in lab and test environments. You can use this HAProxy instance for SSL termination and load balancing to the PCF Routers. HAProxy can generate a self-signed certificate if you do not want to obtain a signed certificate from a well-known certificate authority.

 **Note:** Certificates generated in PAS are signed by the Operations Manager Certificate Authority. They are not technically self-signed, but they are referred to as “Self-Signed Certificates” in the Ops Manager GUI and throughout this documentation.

To use the HAProxy load balancer, you must create a wildcard A record in your DNS and configure three fields in the PAS product tile.

1. Create an A record in your DNS that points to the HAProxy IP address. The A record associates the **System Domain** and **Apps Domain** that you configure in the **Domains** section of the PAS tile with the HAProxy IP address.

For example, with `cf.example.com` as the main subdomain for your CF install and an HAProxy IP address `203.0.113.1`, you must create an A record in your DNS that serves `example.com` and points `*.cf` to `203.0.113.1`.

| Name | Type | Data | Domain |
|------|------|-------------|-------------|
| *.cf | A | 203.0.113.1 | example.com |

2. Use the Linux `host` command to test your DNS entry. The `host` command should return your HAProxy IP address.

Example:

```
$ host cf.example.com
cf.example.com has address 203.0.113.1
$ host anything.example.com
anything.cf.example.com has address 203.0.113.1
```

3. From the PCF Ops Manager Dashboard, click on the PAS tile.
4. Select **Networking**.
5. Leave the **Router IPs** field blank. HAProxy assigns the router IPs internally.
6. Enter the IP address for HAProxy in the **HAProxy IPs** field.
7. Provide your SSL certificate in the **SSL Termination Certificate and Private Key** field. See [Providing a Certificate for your SSL Termination Point](#) for details.

[Return to the Getting Started Guide](#)

Using Another Load Balancer

Production environments should use a highly-available customer-provided load balancing solution that does the following:

- Provides SSL termination with wildcard DNS location
- Provides load balancing to each of the PCF Router IPs

- Adds appropriate `x-forwarded-for` and `x-forwarded-proto` HTTP headers


You must register static IP addresses for PCF with your load balancer and configure three fields in the PAS product tile.

1. Register one or more static IP address for PCF with your load balancer.
2. Create an A record in your DNS that points to your load balancer IP address. The A record associates the **System Domain** and **Apps Domain** that you configure in the **Domains** section of the PAS tile with the IP address of your load balancer.

For example, with `cf.example.com` as the main subdomain for your CF install and a load balancer IP address `198.51.100.1`, you must create an A record in your DNS that serves `example.com` and points `*.cf` to `198.51.100.1`.

| Name | Type | Data | Domain |
|------|------|--------------|-------------|
| *.cf | A | 198.51.100.1 | example.com |

3. From the PCF Ops Manager Dashboard, click on the PAS tile.
4. Select **Networking**.
5. In the **Router IPs** field, enter the static IP address for PCF that you have registered with your load balancer.
6. Leave the **HAProxy IPs** field blank.
7. Provide your SSL certificate in the **SSL Termination Certificate and Private Key** field. See [Providing a Certificate for your SSL Termination Point](#) for details.

 **Note:** When adding or removing PCF routers, you must update your load balancing solution configuration with the appropriate IP addresses.

[Return to the Installing Pivotal Cloud Foundry Guide](#) 

Availability Zones in vSphere

Page last updated:

This topic describes availability zones (AZs) in vSphere and an example of how an operator might scale an app across AZs.

Overview

Pivotal defines an AZ as an operator-assigned, functionally-independent segment of network infrastructure. In cases of partial infrastructure failure, a tile distributes and balances all instances of running apps across remaining AZs. Strategic use of Availability Zones contributes to the fault tolerance and high availability of a tile deployment.

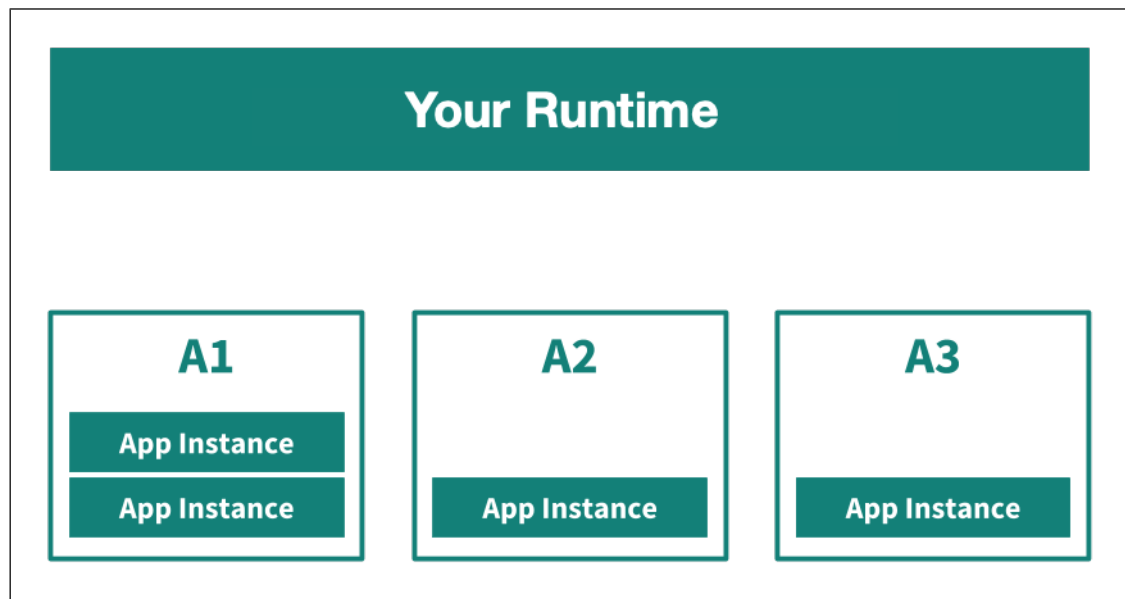
vSphere supports distributing deployments across multiple AZs. For more information, see *Step 4: Create Availability Zones* in [Configuring BOSH Director on vSphere](#).

It is recommended that customers use three Availability Zones to operate a highly available tile deployment.

Balancing Across AZs During Failure: Example Scenario

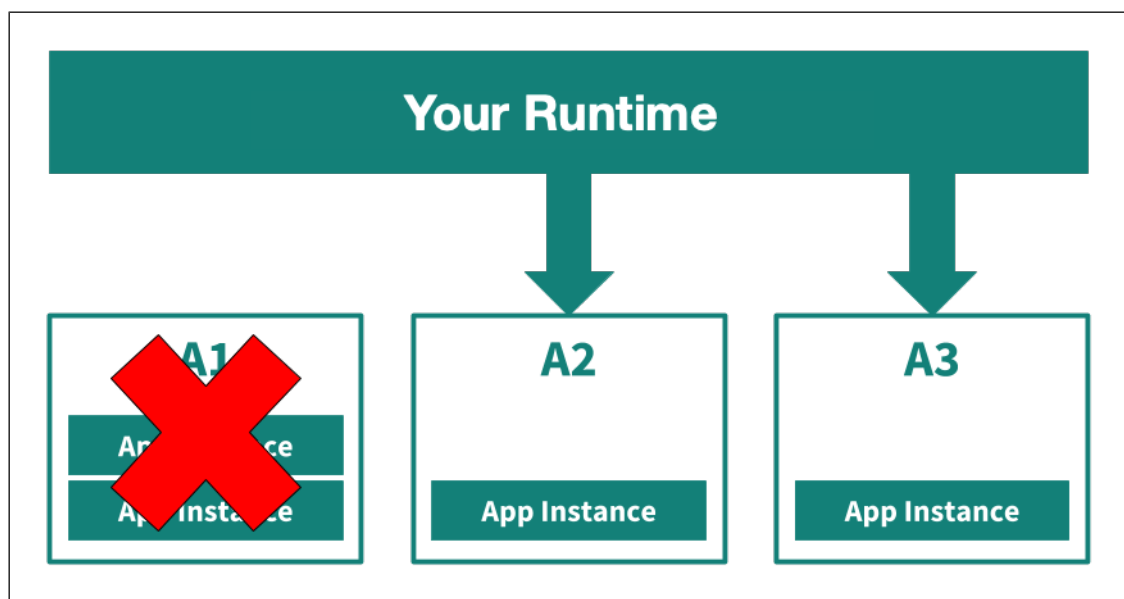
An operator scales an app to four instances in a tile environment distributed across three availability zones: A1, A2, and A3. The environment allocates the instances according to the [Diego Auction](#).

For a visual representation of this scenario, see the following diagram:



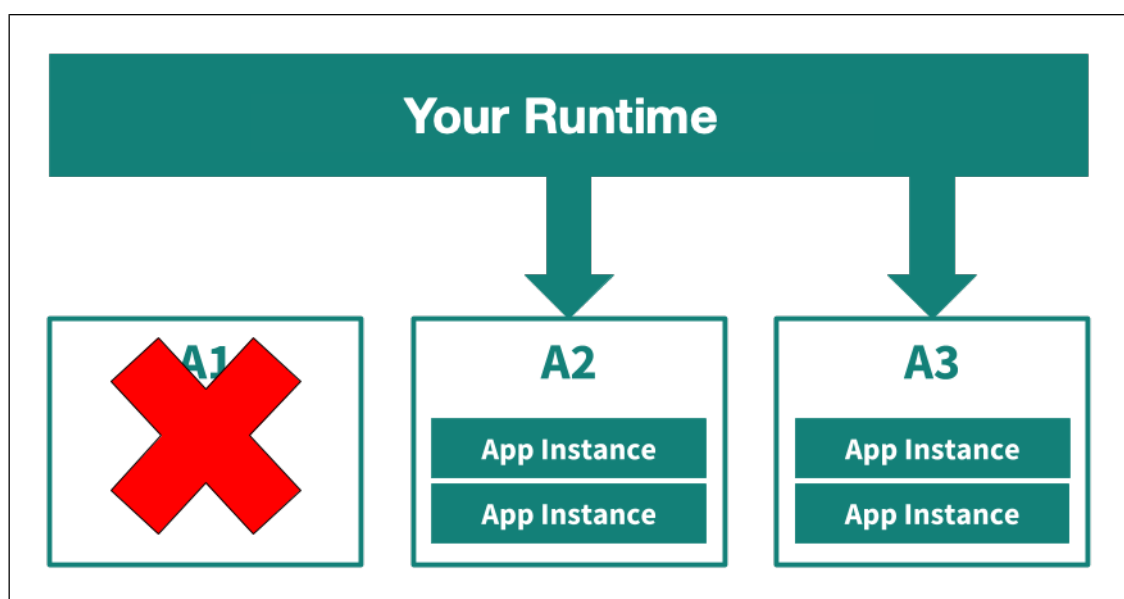
If A1 experiences a power outage or hardware failure, the two app instances running in A1 terminate while the app instances in zones A2 and A3 continue to run.

For a visual representation of this scenario, see the following diagram:



If A1 remains unavailable, the tile balances new instances of the app across the remaining availability zones.

For a visual representation of this scenario, see the following diagram:




Updating NSX Security Group and Load Balancer Information

Page last updated:

This topic describes how to update security group and load balancer information for Pivotal Cloud Foundry (PCF) deployments using NSX-V on vSphere. To update this information, you must use the Ops Manager API.

See the [Ops Manager API documentation](#) for more information about the API.

See [Using Edge Services Gateway on VMware NSX](#) for guidance on how to configure the NSX firewall, load balancing, and NAT/SNAT services for PCF on vSphere installations.

 **Note:** Ops Manager v1.11 supports NSX-V 6.2+.

Authenticate

To use the Ops Manager API, you must authenticate and retrieve a token from the Ops Manager User Account and Authentication (UAA) server. For instructions, see the [Using Ops Manager API](#) topic.

Update Security Group or Load Balancer Information

To update either NSX security group or load balancer information, you use `curl` to make a PUT request against the `api/v0/staged/products/product_guid/jobs/job_guid/resource_config` endpoint.

You must first retrieve the GUID of your PCF deployment, and the GUID of the job whose information you want to update.

Perform the following steps:

1. Retrieve a list of staged products:

```
$ curl 'https://OPS-MAN-FQDN/api/v0/staged/products' \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
[
  {
    "product_version": "1.10.6.0",
    "guid": "p-bosh-dee11e111e111e1e1a",
    "installation_name": "p-bosh",
    "type": "p-bosh"
  },
  {
    "type": "cf",
    "product_version": "1.10.8-build.7",
    "installation_name": "cf-01222ab1111111aaa1a",
    "guid": "cf-01222ab1111111aaa1a"
  }
]
```

Record the GUID of the `cf` product. In the above example, the GUID is `cf-01222ab1111111aaa1a`.

2. Retrieve a list of jobs for your product:

```
$ curl 'https://OPS-MAN-FQDN/api/v0/staged/products/PRODUCT-GUID/jobs' \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
{
  "jobs": [
    {
      "guid": "consul_server-9c37cf48ae7412f2afd1",
      "name": "consul_server"
    },
    {
      "name": "nats",
      "guid": "nats-6af18efdd18d198edee9"
    },
    {
      "name": "nfs_server",
      "guid": "nfs_server-b49b0b2aed247302e0e1"
    },
    ...
  ]
}
```

Record the GUID of the job whose security groups you want to update.


3. You can update either your security group information, load balancer information, or both.

- **Security groups:** To update the security groups for your job, use the following command:

```
$ curl "https://OPS-MAN-FQDN/api/v0/staged/products/PRODUCT-GUID/jobs/JOB-GUID/resource_config" \
-X PUT \
-H "Content-Type: application/json" \
-H "Authorization: Bearer UAA-ACCESS-TOKEN" \
-d '{"instance_type": {"id": "INSTANCE-TYPE"},
  "persistent_disk": {"size_mb": "DISK-SIZE"},
  "nsx_security_groups": ["SECURITY-GROUP1", "SECURITY-GROUP2"]}'
```

Replace the placeholder values as follows:

- **INSTANCE-TYPE** : The instance type for the job. For the default instance type, use `"automatic"`.
- **DISK-SIZE** : The disk size for the job. For the default persistent disk size, use `"automatic"`.

 **Note:** The `persistent_disk` parameter is required to make this API request. For jobs that do not have persistent disks, you must set the value of the parameter to `"automatic"`.


- **SECURITY-GROUP1** , **SECURITY-GROUP2** : The value of the `nsx_security_groups` parameter is a list of the security groups that you want to set for the job. To clear all security groups for a job, pass an empty list with the `[]` value.

- **Load balancers:** To update the load balancers for your job, use the following command:

```
$ curl "https://OPS-MAN-FQDN/api/v0/staged/products/PRODUCT-GUID/jobs/JOB-GUID/resource_config" \
-X PUT \
-H "Content-Type: application/json" \
-H "Authorization: Bearer UAA-ACCESS-TOKEN" \
-d '{"instance_type": {"id": "INSTANCE-TYPE"},
  "persistent_disk": {"size_mb": "DISK-SIZE"},
  "nsx_lbs": [
    {
      "edge_name": "EDGE-NAME",
      "pool_name": "POOL-NAME",
      "security_group": "SECURITY-GROUP",
      "port": "PORT-NUMBER"
    }
  ]
}'
```

Replace the placeholder values as follows:

- **INSTANCE-TYPE** : The instance type for the job. For the default instance type, use `"automatic"`.
- **DISK-SIZE** : The disk size for the job. For the default persistent disk size, use `"automatic"`.

 **Note:** The `persistent_disk` parameter is required to make this API request. For jobs that do not have persistent disks, you must set the value of the parameter to `"automatic"`.

- **EDGE-NAME** : The name of the NSX Edge.
- **POOL-NAME** : The name of the NSX Edge's server pool.
- **SECURITY-GROUP** : The name of the NSX server pool's target security group.
- **PORT** : The name of the port that the VM service is listening on, such as `5000`.

You can configure more than one load balancer for a job by using additional hashes in the `nsx_lbs` array.

4. Navigate to `OPS-MAN-FQDN` in a browser and log in to the Ops Manager Installation Dashboard.
5. Click **Apply Changes** to redeploy.

Installing PCF Isolation Segment

Page last updated:

This topic describes how to install the PCF Isolation Segment tile, which allows operators to isolate deployment workloads into dedicated resource pools called *isolation segments*.

Installing the tile installs a single isolation segment. However, you can install multiple isolation segments using the Replicator tool documented in [Step 4](#).

After installing the tile, you must perform the steps in the [Create an Isolation Segment](#) section of the *Managing Isolation Segments* topic to create the isolation segment in the Cloud Controller Database (CCDB). The topic also includes information about managing an isolation segment.

For more information about how isolation segments work, see [Isolation Segments](#).

Step 1: (Optional) Configure Routing

By default, the Pivotal Application Service (PAS) Router handles traffic for your isolation segment. However, you can deploy a dedicated router for your isolation segment instead. For information about configuring and managing routing for isolation segments, see the [Routing for Isolation Segments](#) topic.

To deploy a dedicated router, perform the following steps:

1. Add a load balancer in front of the PAS Router. The steps to do this depend on your IaaS, but the setup of the load balancer should mirror the setup of the load balancer for the PAS Router that you configured in the PAS tile.
2. Create a wildcard DNS entry for traffic routed to any app in the isolation segment. For example, `*.iso.example.com`.
3. Attach the wildcard DNS entry to the load balancer you created.

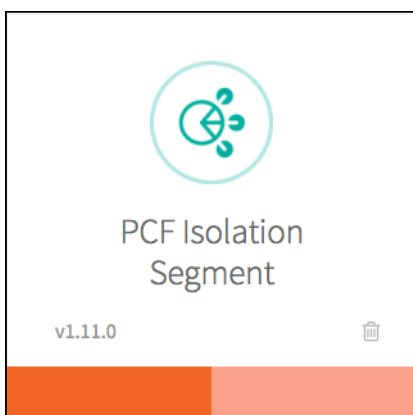
Step 2: Install the Tile

Perform the following steps to install the PCF Isolation Segment tile:

1. Download the product file from [Pivotal Network](#).
2. Navigate to `YOUR-OPSMAN-FQDN` in a browser to log in to the Ops Manager Installation Dashboard.
3. Click **Import a Product** and select the downloaded product file.
4. Under **PCF Isolation Segment** in the left column, click the plus sign.

Step 3: Configure the Tile

Click the orange **PCF Isolation Segment** tile to start the configuration process.



Assign AZs and Networks

Perform the following steps to configure the PCF Isolation Segment tile:

1. Click **Assign AZs and Networks**.

2. Select an availability zone for your singleton jobs, and one or more availability zones to balance other jobs in.
3. Select a network. This network does not need to be the same network where you deployed PAS. For most deployments, operators should create unique networks in which to deploy the Isolation Segment tile. These networks should maintain network reachability with the Diego components so that the cells can reach the Diego Brain and Diego Database VMs.
4. Click **Save**.

Networking

Perform the following steps to configure the PCF Isolation Segment tile:

1. Click **Networking**.

2. (Optional): Under **Router IPs**, enter one or more static IP addresses for the routers that handle this isolation segment. These IP addresses must be within the subnet CIDR block that you defined in the Ops Manager network configuration for your Isolation Segment. If you have a load balancer, configure it to point to these IP addresses.

Note: Entering the static IP addresses is not necessary for deployments running on a public IaaS such as AWS, GCP, or Azure because PCF users specify the IaaS load balancer in the **Resource Config** section of the **PCF Isolation Segment** tile.

- If you want to use HAProxy for this isolation segment, enter at least one address in the **HAProxy IPs** field. You should specify more than one IP address for high availability. Then configure your load balancer to forward requests for the domains you have set up for your deployment to these IP addresses. For more information, see [Configuring SSL/TLS Termination at HAProxy](#).

Note: If you rely on HAProxy for a feature in Pivotal Application Service (PAS) and you want isolated networking for this isolation segment, you may want to deploy the HAProxy provided by the Isolation Segment tile.

- Under **Certificates and Private Key for HAProxy and Router**, you must provide at least one **Certificate and Private Key** name and certificate keypair for HAProxy and Gorouter. The HAProxy and Gorouter are enabled to receive TLS communication by default. You can configure multiple certificates for HAProxy and Gorouter.
 - Click the **Add** button to add a name for the certificate chain and its private keypair. This certificate is the default used by Gorouter and HAProxy.

Certificates and Private Keys for HAProxy and Router

example-cert

Name *

example-cert

A human-readable name describing the use of this certificate.

Certificate and Private Key for HAProxy and Router *

```
-----BEGIN CERTIFICATE-----
MIIE...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```

[Generate RSA Certificate](#)

example-cert-2

Name *

example-cert-2

Certificate and Private Key for HAProxy and Router *

```
-----BEGIN CERTIFICATE-----
MIIE...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```

You can either provide a certificate signed by a Certificate Authority (CA) or click on the **Generate RSA Certificate** link to generate a self-signed certificate in Ops Manager.

- If you want to configure multiple certificates for HAProxy and Gorouter, click the **Add** button and fill in the appropriate fields for each additional certificate keypair.

For details about generating certificates in Ops Manager for your wildcard system domains, see the [Providing a Certificate for Your SSL/TLS Termination Point](#) topic.

Note: If you configured Ops Manager Front End without a certificate, you can use this new certificate to complete Ops Manager configuration. To configure your Ops Manager Front End certificate, see *Configure Front End* in [Preparing to Deploy Ops Manager on GCP Manually](#).

Note: Ensure that you add any certificates that you generate in this pane to your infrastructure load balancer.

- (Optional) When validating client requests using mutual TLS, the Gorouter trusts multiple certificate authorities (CAs) by default. If you want to

configure the Gorouter and HAProxy to trust additional CAs, enter your CA certificates under **Certificate Authorities Trusted by Router and HAProxy**. All CA certificates should be appended together into a single collection of PEM-encoded entries.

Certificate Authorities Trusted by Router and HAProxy

In addition to well-known, public CAs, and those trusted via the BOSH trusted certificates collection, these certificates can be used to validate the certificates from incoming client requests. All CA certificates should be appended together into a single collection of PEM-encoded entries.

- In the **Minimum version of TLS supported by HAProxy and Routerfield**, select the minimum version of TLS to use in HAProxy and Gorouter communications. HAProxy and Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

Minimum version of TLS supported by HAProxy and Router*

☐ TLSv1.0
☐ TLSv1.1
☒ TLSv1.2

- Configure **Logging of Client IPs in CF Router**. The **Log client IPs** option is set by default. To comply with the General Data Protection Regulation (GDPR), select one of the following options to disable logging of client IP addresses:

- If your load balancer exposes its own source IP address, disable logging of the `X-Forwarded-For` HTTP header only.
- If your load balancer exposes the source IP of the originating client, disable logging of both the source IP address and the `X-Forwarded-For` HTTP header.

Logging of Client IPs in CF Router*

☒ Log client IPs
☐ Disable logging of X-Forwarded-For header only
☐ Disable logging of both source IP and X-Forwarded-For header

To comply with GDPR, select one of the options to disable logging of client IPs. If the source IP exposed by your load balancer is its own, choose to disable logging of XFF header only. If the source IP exposed by your load balancer is that of the downstream client, choose to disable logging of the source IP also.



- Under **Configure support for the X-Forwarded-Client-Cert header**, configure PCF handles `x-forwarded-client-cert` (XFCC) HTTP headers based on where TLS is terminated for the first time in your deployment.

Configure support for the X-Forwarded-Client-Cert header. This header can be used by applications to verify the requester via mutual TLS. The option you should select depends upon where you will be terminating the TLS connection for the first time. *

☒ TLS terminated for the first time at infrastructure load balancer
☐ TLS terminated for the first time at HAProxy
☐ TLS terminated for the first time at the Router

The following table indicates which option to choose based on your deployment layout.

| If your deployment is configured as follows: | Then select the following option: | Additional notes: |
|--|--|---|
| <ul style="list-style-type: none"> The Load Balancer is terminating TLS, and Load balancer is configured to put the client certificate from a mutual authentication TLS handshake into the X-Forwarded-Client-Cert HTTP header | TLS terminated for the first time at infrastructure load balancer (default). | Both HAProxy and the Gorouter forward the XFCC header when included in the request. |
| | | HAProxy sets the XFCC header with the client certificate received in the |

| | | |
|--|---|--|
| <ul style="list-style-type: none"> ◦ The Load Balancer is configured to pass through the TLS handshake via TCP to the instances of HAProxy, and ◦ HAProxy instance count is > 0 | <p>TLS terminated for the first time at HAProxy.</p> | <p>TLS handshake. The Gorouter forwards the header.</p> <div>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. </div> |
| <ul style="list-style-type: none"> ◦ The Load Balancer is configured to pass through the TLS handshake via TCP to instances of the Gorouter | <p>TLS terminated for the first time at the Gorouter.</p> | <p>The Gorouter strips the XFCC header if it is included in the request and forwards the client certificate received in the TLS handshake in a new XFCC header.</p> <p>If you have deployed instances of HAProxy, app traffic bypasses those instances in this configuration. If you have also configured your load balancer to route requests for ssh directly to the Diego Brain, consider reducing HAProxy instances to 0.</p> <div>  Breaking Change: In the Router behavior for Client Certificates field, you cannot select the Router does not request client certificates option. </div> |

For a description of the behavior of each configuration option, see [Forward Client Certificate to Applications](#).


9. To configure HAProxy to handle client certificates, select one of the following options in the **HAProxy behavior for Client Certificate Validation** field.

HAProxy behavior for Client Certificate Validation*

☒ HAProxy does not request client certificates.

☐ HAProxy requests but does not require client certificates. This option is necessary if you want to enable mTLS for applications and TLS is terminated for the first time at HAProxy

- **HAProxy does not request client certificates.** This option requires mutual authentication, which makes it incompatible with XFCC option **TLS terminated for the first time at HAProxy**. HAProxy does not request client certificates, so the client does not provide them and no validation occurs. This is the default configuration.
- **HAProxy requests but does not require client certificates.** The HAProxy requests client certificates in TLS handshakes, validates them when presented, but does not require them.

 **warning:** Upon upgrade, PAS will fail to receive requests if your load balancer is configured to present a client certificate in the TLS handshake with HAProxy but HAProxy has not been configured with the certificate authority used to sign it. To mitigate this issue, select **HAProxy does not request client certificates** in the **Networking** pane or configure the HAProxy with the appropriate CA.

10. To configure Gorouter behavior for handling client certificates, select one of the following options in the **Router behavior for Client Certificate Validation** field.

Router behavior for Client Certificate Validation*

☐ Router does not request client certificates. This option is incompatible with XFCC options "TLS terminated for the first time at HAProxy" and "TLS terminated for the first time at the Router" because these options require mutual authentication.

☒ Router requests but does not require client certificates.

☐ Router requires client certificates.

- **Router does not request client certificates.** This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication. As client certificates are not requested, client will not provide them, and thus validation of client certificates will not occur.
- **Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes, validates them when presented, but does not require them. This is the default configuration.
- **Router requires client certificates.** The Gorouter validates that the client certificate is signed by a Certificate Authority that the Gorouter trusts. If the Gorouter cannot validate the client certificate, the TLS handshake fails.

⚠ warning: Requests to the platform will fail upon upgrade if your load balancer is configured with client certificates and the Gorouter does not have the certificate authority. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client Certificate Validation** in the **Networking** pane.

11. In the **TLS Cipher Suites for Router** field, review the TLS cipher suites for TLS handshakes between Gorouter and front-end clients such as load balancers or HAProxy. The default value for this field is `ECDHE-RSA-AES128-GCM-SHA256:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of Golang-supported TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with Gorouter. For a list of TLS ciphers supported by Gorouter, see [Securing Traffic into Cloud Foundry](#).

TLS Cipher Suites for Router *

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with Gorouter has at least one cipher suite in common with Gorouter.

💡 Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

12. In the **TLS Cipher Suites for HAProxy** field, review the TLS cipher suites for TLS handshakes between HAProxy and its clients such as load balancers and Gorouter. The default value for this field is the following: `DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384`. If you want to modify the default configuration, use an ordered, colon-delimited list of TLS cipher suites in the OpenSSL format. Operators should verify that the ciphers are supported by any clients or front-end components that will initiate TLS handshakes with HAProxy.

TLS Cipher Suites for HAProxy *

DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

Verify that every client participating in TLS handshakes with HAProxy has at least one cipher suite in common with HAProxy.

💡 Note: Specify cipher suites that are supported by the versions configured in the **Minimum version of TLS supported by HAProxy and Router** field.

13. Under **HAProxy forwards requests to Router over TLS**, select **Enable** or **Disable** based on your deployment layout.

HAProxy forwards requests to Router over TLS. When enabled, HAProxy will forward all requests to the Router over TLS. HAProxy will use the CA provided to verify the certificates provided by the Router. *


☒ Enable

Certificate Authority for HAProxy Backend *

You need to provide a certificate authority for the certificate and key provided in the "Certificate and Private Key for HAProxy and Router" field. HAProxy will verify those certificates using this CA when establishing a connection. If you generated that certificate and key using the "Generate RSA Certificate" feature, then your CA is the Ops Manager CA, and can be found by visiting the "/api/v0/certificate_authorities" API endpoint.

☐ Disable


◦ Enable HAProxy forwarding of requests to Router over TLS

| If you want to: | Encrypt communication between HAProxy and the Gorouter |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Leave Enable selected. 2. In the Certificate Authority for HAProxy Backend field, specify the Certificate Authority (CA) that signed the certificate you configured in the Certificate and Private Key for HAProxy and Router field. <div>  Note: If you used the Generate RSA Certificate link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the <code>/api/v0/certificate_authorities</code> endpoint in the Ops Manager API. </div> <ol style="list-style-type: none"> 3. Make sure that Gorouter and HAProxy have TLS cipher suites in common in the TLS Cipher Suites for Router and TLS Cipher Suites for HAProxy fields. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Load Balancer and Gorouter ◦ Providing a Certificate for Your SSL/TLS Termination Point ◦ Using the Ops Manager API |

◦ Disable HAProxy forwarding of requests to Router over TLS

| If you want to: | Use non-encrypted communication between HAProxy and Gorouter, or you are not using HAProxy |
|-------------------------------|---|
| Then configure the following: | <ol style="list-style-type: none"> 1. Select Disable. 2. If you are not using HAProxy, set the number of HAProxy job instances to <code>0</code> on the Resource Config page. See Disable Unused Resources. |
| See also: | <ul style="list-style-type: none"> ◦ Terminating SSL/TLS at the Gorouter Only ◦ Terminating SSL/TLS at the Load Balancer Only |

14. If you are not using SSL encryption or if you are using self-signed certificates, select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 **Note:** For production deployments, Pivotal does not recommend disabling SSL certificate verification.

15. (Optional) If you want HAProxy or the Gorouter to reject any HTTP (non-encrypted) traffic, select the **Disable HTTP on HAProxy and Gorouter** checkbox. When selected, HAProxy and Gorouter will not listen on port 80.

☐ Disable HTTP on HAProxy and Gorouter

16. (Optional) Select the **Disable insecure cookies on the Router** checkbox to set the secure flag for cookies generated by the router.
17. (Optional) To disable the addition of Zipkin tracing headers on the Gorouter, deselect the **Enable Zipkin tracing headers on the router** checkbox. Zipkin tracing headers are enabled by default. For more information about using Zipkin trace logging headers, see [Zipkin Tracing in HTTP Headers](#).
18. (Optional) To stop the Router from writing access logs to local disk, deselect the **Enable Router to write access logs locally** checkbox. You should consider disabling this checkbox for high traffic deployments since logs may not be rotated fast enough and can fill up the disk.
19. (Optional) By default, Gorouter support for the PROXY protocol is disabled. To enable the PROXY protocol, select **Enable support for PROXY protocol in CF Router**. When enabled, client-side load balancers that terminate TLS but do not support HTTP can pass along information from the originating client. Enabling this option may impact Gorouter performance. For more information about enabling the PROXY protocol in Gorouter, see the *HTTP Header Forwarding* sections in the [Securing Traffic in Cloud Foundry](#) topic.
20. **Bypass security checks for route service lookup** has potential security concerns, but may be needed for backwards compatibility. See the *Route Service Internal Lookup Considerations* section of [Route Services](#) for details.
21. (Optional) If you want to limit the number of app connections to the backend, enter a value in the **Max Connections Per Backend** field. You can use this field to prevent a poorly behaving app from all the connections and impacting other apps.

To choose a value for this field, review the peak concurrent connections received by instances of the most popular apps in your deployment. You can determine the number of concurrent connections for an app from the `httpStartStop` event metrics emitted for each app request.

If your deployment uses PCF Metrics, you can also obtain this peak concurrent connection information from [Network Metrics](#). The default value is

Max Connections Per Backend *

500

22. Under **Enable Keepalive Connections for Router**, select **Enable** or **Disable**. Keepalive connections are enabled by default. For more information, see [Keepalive Connections](#) in *HTTP Routing*.

Enable Keepalive Connections for Router *

☒ Enable

☐ Disable

23. (Optional) To accommodate larger uploads over connections with high latency, increase the number of seconds in the **Router Timeout to Backends** field.
24. (Optional) Increase the value of **Load Balancer Unhealthy Threshold** to specify the amount of time, in seconds, that the router continues to accept connections before shutting down. During this period, healthchecks may report the router as unhealthy, which causes load balancers to failover to other routers. Set this value to an amount greater than or equal to the maximum time it takes your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
25. (Optional) Modify the value of **Load Balancer Healthy Threshold**. This field specifies the amount of time, in seconds, to wait until declaring the Router instance started. This allows an external load balancer time to register the Router instance as healthy.

Load Balancer Unhealthy Threshold *

Load Balancer Healthy Threshold *

26. (Optional) If app developers in your organization want certain HTTP headers to appear in their app logs with information from the Gorouter, specify them in the **HTTP Headers to Log** field. For example, to support app developers that deploy Spring apps to PCF, you can enter [Spring-specific HTTP headers](#).

HTTP Headers to Log

27. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.

28. If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:

- **HAProxy Protected Domains:** Enter a comma-separated list of domains to protect from unknown source requests.
- **HAProxy Trusted CIDRs:** Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the **Protected Domains** can send traffic to PCF.

HAProxy Protected Domains

A comma-separated list of domains to protect from requests from unknown sources. Use this property in conjunction with "Trusted CIDRs" to protect these domains from requests from unknown sources.

HAProxy Trusted CIDRs

29. For **DNS Search Domains**, enter DNS search domains as a comma-separated list. Your containers append these search domains to hostnames to resolve them into full domain names.

DNS Search Domains

example.com, myapps.com

DNS search domains to be used in containers. A comma-separated list can be specified.

30. Select a sharding mode in the **Router Sharding Mode** field. The options are explained below. For more information, see [Sharding Routers for Isolation Segments](#).

Router Sharding Mode: When 'Isolation Segment Only' is selected, the routers of this tile will only have knowledge of applications deployed to the Cells of this tile; all other requests will receive a 404 response. When 'No Isolation Segments' is selected, the routers of this tile will reject requests for any isolation segment. Choose 'No Isolation Segments' to add a group of routers for the Elastic Runtime tile, as when a private point of entry for the system domain is desired.*

- ☒ Isolation Segment Only
- ☐ No Isolation Segment

Save

| Option Name | Description |
|------------------------|--|
| Isolation Segment Only | The routers for the tile acknowledge requests only from apps deployed within the cells of the tile. All other requests fail. |
| No Isolation Segment | The routers for the tile reject requests for any isolation segment. Choose this option to add a group of routers for the PAS tile, such as when you want a private point of entry for the system domain. |

31. Click **Save**.

Application Containers Perform the following steps to configure the PCF Isolation Segment tile: 1. Click ****Application Containers****.

Enable custom configuration that supports your applications at a container level.

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888

Segment Name *

DNS Servers

Docker Images Disk-Cleanup Scheduling on Cell VMs *

☐ Never clean up Cell disk-space

☐ Routinely clean up Cell disk-space

☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) *

10240

Disk cleanup will initiate whenever a Cell has exceeded this much disk-space for filesystem layers.

1. (Optional): Under **Private Docker Insecure Registry Whitelist**, enter one or more private Docker image registries that are secured with self-signed certificates. Use a comma-delimited list in the format ``IP:Port`` or ``Hostname:Port``. 1. Under **Segment Name**, enter the name of your isolation segment. This name must be unique across your PCF deployment. You use this name when performing the steps in the [Create an Isolation Segment](../adminguide/isolation-segments.html#create-an-is) section of the *Managing Isolation Segments* topic to create the isolation segment in the Cloud Controller Database (CCDB). 1. Select your preference for **Docker Images Disk-Cleanup Scheduling on Cell VMs**. If you choose **Clean up disk-space once threshold is reached**, enter a **Threshold of Disk-Used** in megabytes. For more information about the configuration options and how to configure a threshold, see [Configuring Docker Images Disk-Cleanup Scheduling](../opsguide/config-cell-cleanup.html). 1. Under **Enabling NFSv3 volume services**, select **Enable** or **Disable**. NFS volume services allow application developers to bind existing NFS volumes to their applications for shared file access. For more information, see the [Enabling NFS Volume Services](../opsguide/enable-vol-services.html) topic.

Note: In a clean install, NFSv3 volume services are enabled by default. In an upgrade, NFSv3 volume services match the setting of the previous deployment.

1. (Optional) To configure LDAP for NFSv3 volume services, perform the following steps:

- For **LDAP Service Account User**, enter the username of the service account in LDAP that will manage volume services.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses port 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the fully qualified path to the LDAP service account. For example, if you have a service account called `volume-services` that belongs to organizational units (OU) called `service-accounts` and `my-company`, and your domain is called `domain`, the fully qualified path looks like the following:

CN=volume-services,OU=service-accounts,OU=my-company,DC=domain,DC=com

2. By default, PAS manages container images using the [GrootFS](#) plugin for Garden-runC. If you experience issues with GrootFS, you can disable the plugin and use the image plugin built into Garden-runC.

Note: If you modify this setting, Pivotal recommends recreating all VMs in the BOSH Director config. You can do this by selecting the **Recreate all VMs** checkbox in the **Director Config** pane of the BOSH Director tile before you redeploy.

3. To enable Gorouter to verify app identity using TLS, select the **Router uses TLS to verify application identity** checkbox. Verifying app identity using TLS improves resiliency and consistency for app routes. For more information about Gorouter route consistency modes, see [Preventing Misrouting in HTTP Routing](#).
4. Click **Save**.

System Logging

1. In the **System Logging** menu, select an option underneath **Do you want to configure syslog for system components?**. **No** is selected by default. This setting only affects Diego cell, router, and HAProxy components within the isolation segment, not shared PAS system components.

Configure system logging. Complete the External Syslog fields only if using an external syslogd server.

Do you want to configure syslog for system components?*

☒ No

☐ Yes

[Save](#)

2. If you want to use syslog, select **Yes**.

Do you want to configure syslog for system components? *

☐ No

☒ Yes

Address *

Port *

Transport Protocol *

TCP protocol

☐ Enable TLS

Permitted Peer

TLS CA Certificate

☒ Use TCP for file forwarding local transport

Workaround to avoid truncation of very long (> 1024 bytes) log lines. May negatively impact performance.

☒ Don't Forward Debug Logs

Custom rsyslog Configuration

Save

3. Enter the address of your external syslog aggregation service in the **Address** field. The address can be a hostname or IP address.
4. Enter a port number in the **Port** field.
5. Select a protocol from the **Transport Protocol** menu. This is the protocol the system uses to transmit logs to syslog.
6. (Optional) Select the **Enable TLS** option if you want to transmit logs over TLS.
7. Enter a **Permitted Peer**.
8. Paste the certificate for your TLS certificate authority (CA) in the **TLS CA Certificate** field.
9. (Optional) Select the **Use TCP for file forwarding local transport** to transmit logs over TCP, rather than UDP. This prevents log truncation, but may cause performance issues.
10. (Optional) To forward DEBUG syslog messages to an external service, disable the **Don't Forward Debug Logs** checkbox. This checkbox is enabled in PCF Isolation Segment by default.

 **Note:** Some PCF Isolation Segment components generate a high volume of DEBUG syslog messages. Using the **Don't Forward Debug Logs**

checkbox prevents them from being forwarded to external services. PCF Isolation Segment still writes the messages to the local disk.

11. (Optional) To specify a custom syslog rule, enter it in the **Custom rsyslog Configuration** field in [RainerScript](#) [↗](#) syntax. For more information about customizing syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.


Advanced Features

The **Advanced Features** section of Pivotal Application Service (PAS) includes new functionality that may have certain constraints. Although these features are fully supported, Pivotal recommends caution when using them in production environments.

Diego Cell Memory and Disk Overcommit

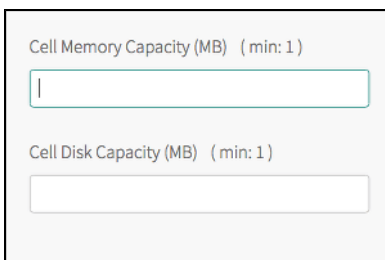
If your apps do not use the full allocation of disk space and memory set in the **Resource Config** tab, you might want use this feature. These fields control the amount to overcommit disk and memory resources to each Diego Cell VM.

For example, you might want to use the overcommit if your apps use a small amount of disk and memory capacity compared to the amounts set in the **Resource Config** settings for **Diego Cell**.

 **Note:** Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.


To enable overcommit, do the following:

1. Select **Advanced Features**.



The screenshot shows a configuration form with two input fields. The first field is labeled 'Cell Memory Capacity (MB) (min: 1)' and the second field is labeled 'Cell Disk Capacity (MB) (min: 1)'. Both fields are empty and have a light blue border.

2. Enter the total desired amount of Diego cell memory value in the **Cell Memory Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell memory capacity settings that this field overrides.
3. Enter the total desired amount of Diego cell disk capacity value in the **Cell Disk Capacity (MB)** field. Refer to the **Diego Cell** row in the **Resource Config** tab for the current Cell disk capacity settings that this field overrides.
4. Click **Save**.

 **Note:** Entries made to each of these two fields set the total amount of resources allocated, not the overage.

Configure Router Resources


1. Select **Resource Config**.

Resource Config

| JOB | INSTANCES | PERSISTENT DISK TYPE | VM TYPE | LOAD BALANCERS | INTERNET CONNECTED |
|------------|--------------|----------------------|---|----------------|-------------------------------------|
| Router | Automatic: 3 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |
| Diego Cell | Automatic: 3 | None | Automatic: xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB) | | <input checked="" type="checkbox"/> |
| HAProxy | Automatic: 3 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB) | | <input checked="" type="checkbox"/> |

Save

- If you are using a dedicated router for your isolation segment, follow the instructions below.

 **Note:** The configuration settings available in **Resource Config** vary depending on your IaaS.

- If you have the Load Balancers column in your Resource Config:
 - Enter the wildcard DNS entry attached to your load balancer into the **Router** row under **Load Balancers**.
- If you do not have the Load Balancers column in your Resource Config:
 - Navigate to the **Networking** section of the **PCF Isolation Segment** tile.
 - Specify **Router IPs**.
 - Attach the IP addresses to your load balancer manually.

- If you are not using HAProxy for this isolation segment, set the number of **Instances** to .

After Tile Configuration

After you configure the PCF Isolation Segment tile, perform the following steps:

- Create the isolation segment in the Cloud Controller Database (CCDB) by following the procedure in the [Create an Isolation Segment](#) section of the *Managing Isolation Segments* topic.
- Return to the Ops Manager Installation Dashboard and click **Apply Changes** to deploy the tile.

After the tile finishes deploying, see the [Managing Isolation Segments](#) topic for more information about managing an isolation segment.

Step 4: (Optional) Copy the Tile

If you want to create multiple isolation segments, perform the following steps to copy the PCF Isolation Segment tile with the Replicator tool:

- Download the Replicator tool from the **Pivotal Cloud Foundry Isolation Segment** section of [Pivotal Network](#).
- Navigate to the directory where you downloaded the Replicator tool.
- Replicate the tile:

```
./replicator \
--name "YOUR-NAME" \
--path /PATH/TO/ORIGINAL.pivotal \
--output /PATH/TO/COPY.pivotal
```

Replace the values above with the following:

- YOUR-NAME**: Provide a unique name for the new PCF Isolation Segment tile. The name must be ten characters or less and only contain alphanumeric characters, dashes, underscores, and spaces.
- /PATH/TO/ORIGINAL**: Provide the absolute path to the original PCF Isolation Segment tile you downloaded from Pivotal Network.
- /PATH/TO/COPY**: Provide the absolute path for the copy that the Replicator tool produces.

- Follow the procedures in this topic using the new `.pivotal` file, starting with [Step 1](#).

Upgrading Replicated Tiles

For information about upgrading replicated Isolation Segment tiles, see [Upgrading Replicated Tiles](#).

Getting Started with Small Footprint PAS

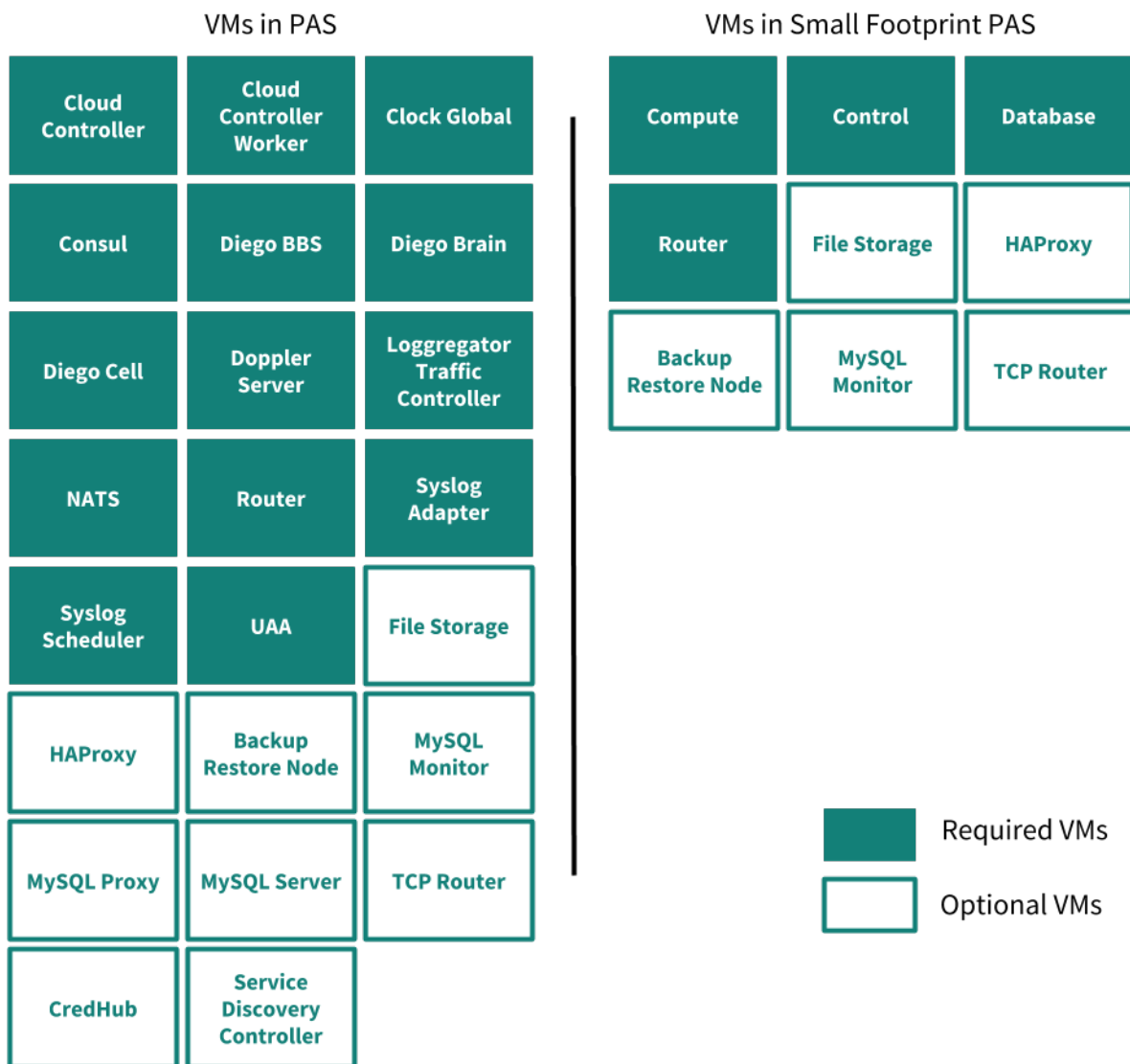
This topic describes the Small Footprint Pivotal Application Services (PAS) tile for Pivotal Cloud Foundry (PCF).

The Small Footprint PAS is a repackaging of the PAS components into a smaller deployment with fewer virtual machines (VMs). The [Limitations](#) section describes the limitations that come with a smaller deployment.

Differentiate Small Footprint PAS and PAS

A standard PAS deployment must have at least 14 VMs, but the Small Footprint PAS requires only four.

The following image displays a comparison of the number of VMs deployed by PAS and Small Footprint PAS.



Use Cases

Use the Small Footprint PAS tile for smaller PCF deployments on which you intend to host 2500 or fewer apps, as described in the [Limitations](#) section. If you want to use Small Footprint PAS in a production environment, ensure the *Limitations* described below are not an issue in your use case.

Note: The Small Footprint PAS is compatible with PCF service tiles.

The Small Footprint PAS tile is also ideal for the following use cases:

- **Proof-of-concept installations:**
 - Deploy PCF quickly and with a small footprint for evaluation or testing purposes.
- **Sandbox installations:**
 - Use Small Footprint PAS as a PCF operator sandbox for tasks such as testing compatibility.
- **Service tile R&D:**
 - Test a service tile against Small Footprint PAS instead of a standard PAS deployment to increase efficiency and reduce cost.


Limitations

The Small Footprint PAS has the following limitations:

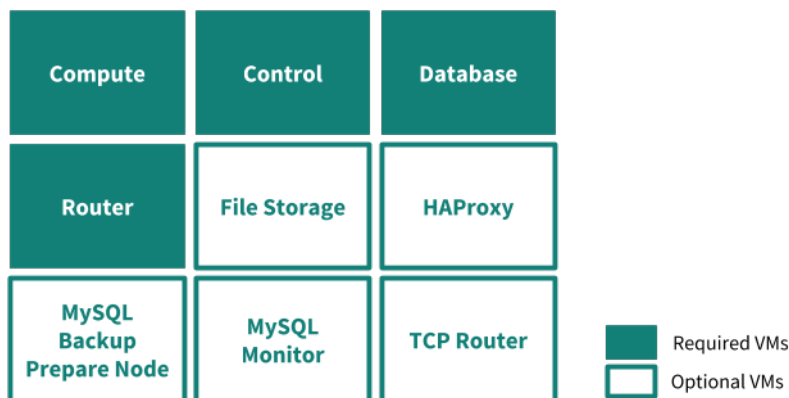
- **Number of app instances:**
 - The tile is not designed to support large numbers of app instances. You cannot scale the number of [Compute VMs](#) beyond instances in the **Resource Config** pane. The Small Footprint PAS is designed to support 2500 or fewer apps.
- **Increasing platform capacity:**
 - You cannot upgrade the Small Footprint PAS to the standard PAS tile. If you expect platform usage to increase beyond the capacity of the Small Footprint PAS, Pivotal recommends using the standard PAS tile.
- **Management plane availability during tile upgrades:**
 - You may not be able to perform management plane operations like deploying new apps and accessing APIs for brief periods during tile upgrades. The management plane is colocated on the [Control VM](#).
- **App availability during tile upgrades:**
 - If you require availability during your upgrades, you must scale your **Compute VMs** to a highly available configuration. Ensure sufficient capacity exists to move app instances between Compute VM instances during the upgrade.

Architecture

You can deploy the Small Footprint PAS tile with a minimum of four VMs, as shown in the image below.

 **Note:** The following image assumes that you are using an external blobstore.

VMs in Small Footprint PAS



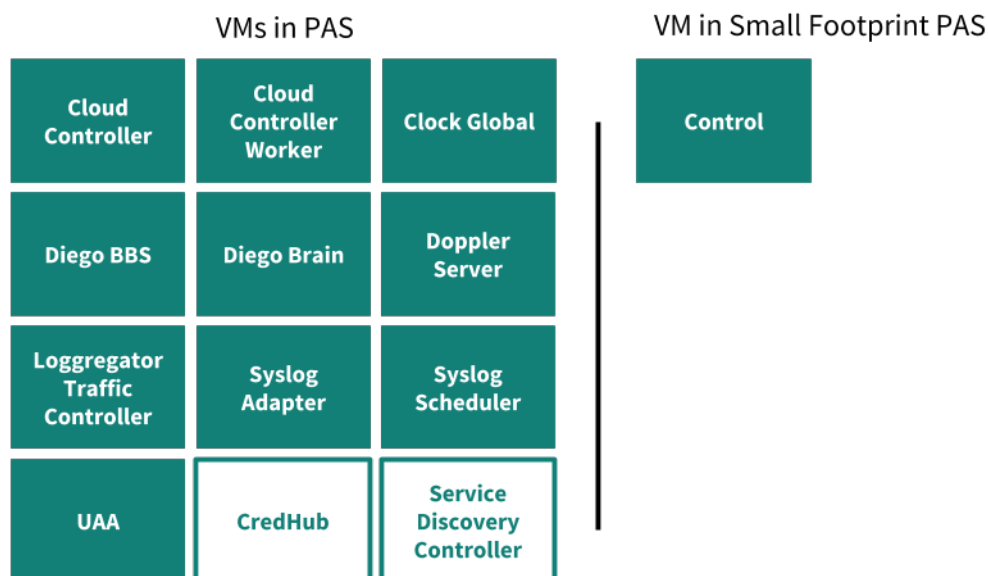
To reduce the number of VMs required for Small Footprint PAS, the *Control* and *Database* VMs include colocated jobs that run on a single VM in PAS. See the next sections for details.

For more information about the components mentioned on this page, see the *Architecture* section of the [Cloud Foundry Concepts](#) guide.

Control VM

The Control VM includes the PAS jobs that handle management plane operations, app lifecycles, logging, and user authorization and authentication. Additionally, all errands run on the Control VM, eliminating the need for a VM for each errand and significantly reducing the time it takes to run errands.

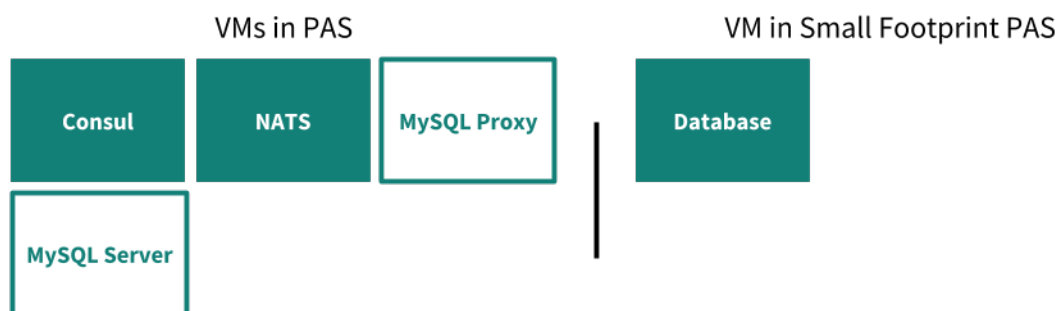
The following image shows all the jobs from PAS that are colocated on the Control VM in Small Footprint PAS.



Database VM

The database VM includes the PAS jobs that handle internal storage and messaging.

The following image shows all the jobs from PAS that are colocated on the Database VM in Small Footprint PAS.



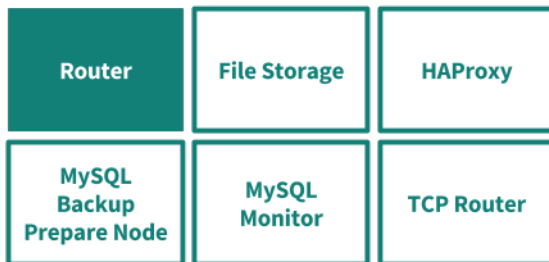
Compute VM

The *Compute* VM is the same as the Diego Cell VM in PAS.



Other VMs (Unchanged)

The following image shows the VMs performs the same functions in both versions of the PAS tile.



Requirements

The following topics list the minimum resources needed to run Small Footprint PAS and Ops Manager on the public IaaSes that PCF supports:

- [Installing PCF on AWS](#)
- [Installing PCF on Azure](#)
- [Installing PCF on GCP](#)
- [Installing PCF on vSphere](#)

Installing Small Footprint PAS

To install the Small Footprint PAS tile, follow the instructions for [Installing Pivotal Cloud Foundry](#) on your IaaS.

Follow the same installation and configuration steps as for PAS, with the following differences:


- **Selecting a product in Pivotal Network:**
 - When you navigate to the PAS tile on [Pivotal Network](#), select the **Small Footprint** release.
- **Configuring resources:**
 - The **Resource Config** pane in the Small Footprint PAS tile reflects the differences in VMs discussed in the *Architecture* section of this topic.
 - Small Footprint PAS does not default to a highly available configuration like PAS does. It defaults to a minimum configuration. To make Small Footprint PAS highly available, scale the VMs to the following instance counts:
 - **Compute:** 3
 - **Control:** 2
 - **Database:** 3
 - **Router:** 3
- **Configuring load balancers:**
 - If you are using an SSH load balancer, you must enter its name in the **Control VM** row of the **Resource Config** pane. There is no **Diego Brain** row in Small Footprint Runtime because the Diego Brain is colocated on the Control VM. You can still enter the appropriate load balancers in the **Router** and **TCP Router** rows as normal.

Troubleshooting Colocated Jobs Using Logs

If you need to troubleshoot a job that runs on the Control or Database VMs, do the following:

- Follow the procedures in *Advanced Troubleshooting with the BOSH CLI* to the log in to the BOSH Director for your deployment:
 - [Gather Credential and IP Address Information](#)
 - [SSH into Ops Manager](#)
 - [Log in to the BOSH Director](#)
- Use BOSH to list the VMs in your Small Footprint PAS deployment:

```
bosh -e MY-ENV -d MY-DEPLOYMENT vms
```

 **Note:** If you do not know the name of your deployment, you can run `bosh -e MY-ENV deployments` to list the deployments for your BOSH Director.

See the following example output:

```
$ bosh -e example-env -d example-deployment vms
Using environment 'example-env' as client 'ops_manager'
```

Task 182. Done

Deployment 'example-deployment'

| Instance | Process | State | AZ | IPs | VM CID | VM Type |
|---|---------|---------|----|-----|-------------------------|---|
| backup-prepare/8fd07242-cf7c-4a4d-ba69-85fe078114f9 | | running | | | us-central1-a 10.0.4.10 | vm-6ec72a47-55b0-4767-78af-759f1f295183 micro |
| compute/01c6947d-477e-4605-9e6b-5d130a58c70c | | running | | | us-central1-b 10.0.4.8 | vm-ce14173c-d93e-414c-6830-afbe0c713fc5 xlarge.disk |
| compute/28045395-5048-4c8d-8363-e22fc7b66847 | | running | | | us-central1-c 10.0.4.9 | vm-e3d8f696-5802-4552-4006-a1260563ed49 xlarge.disk |
| compute/2e3ed7dc-baa4-42ef-814d-980c6ab1c36b | | running | | | us-central1-a 10.0.4.7 | vm-6dc34e53-71f3-4741-674a-c42c4df9e559 xlarge.disk |
| control/12b1b027-7ffd-43ca-9dc9-7f4ff204d86a | | running | | | us-central1-a 10.0.4.6 | vm-9760b74e-e13e-4483-79b6-78ab3818b628 xlarge |
| ha_proxy/b0587c68-45a8-40e2-94d3-5d2ffcdaf858 | | running | | | us-central1-a 10.0.4.11 | vm-27d62bfc-af6d-4c8b-6e2a-cbba09eddd1e micro |
| mysql_monitor/5185d04e-e038-4664-a26a-d16d0d295a7f | | running | | | us-central1-a 10.0.4.15 | vm-6d215888-913b-44a3-4db3-52329c5ada53 micro |
| router/2043b22d-0c3b-4a02-873f-80a724c3ed08 | | running | | | us-central1-a 10.0.4.12 | vm-2b7cf5f4-5926-4f70-6e47-d994a6eff93b micro |
| router/72b54793-e0d0-4301-8932-76da5375e654 | | running | | | us-central1-c 10.0.4.14 | vm-e77bcdff-0c26-46cd-7783-6d766f4c5098 micro |
| router/e3d2ab7b-6191-46bb-ab62-c1db7268a942 | | running | | | us-central1-b 10.0.4.13 | vm-3e84523b-1988-475e-49e8-de80fd76c656 micro |
| database/681bcad5-fa8b-4cf1-912f-45140d96123f | | running | | | us-central1-a 10.0.4.5 | vm-e3cded4f-cf47-499f-4c96-992b3c6ebf9c large.disk |
| tcp_router/61a06e83-a62b-4afb-b452-441dc2dc1e4c | | running | | | us-central1-a 10.0.4.17 | vm-cc1f0a62-409f-47f9-58b0-0b8f46cf9ac0 micro |

13 vms

Succeeded

- Use BOSH to SSH into one of the Small Footprint PAS VMs.

```
bosh -e MY-ENV -d MY-DEPLOYMENT ssh VM-NAME/GUID
```

For example, to SSH into the Control VM, run the following:

```
$ bosh -e example-env -d example-deployment ssh control/12b1b027-7ffd-43ca-9dc9-7f4ff204d86a
```

- Run `sudo su` to act as super user.
- Use `monit` to list the processes running on the VM.

```
monit summary
```

See the following example output that lists the processes running on the Control VM. The processes listed reflect the colocation of jobs as outlined in the *Architecture* section of this topic.

```
control/12b1b027-7ffd-43ca-9dc9-7f4ff204d86a:/var/vcap/bosh_ssh/bosh_f9d2446b18b445e# monit summary
The Monit daemon 5.2.5 uptime: 5d 21h 10m
```

```
Process 'consul_agent'      running
Process 'bbs'              running
Process 'metron_agent'     running
Process 'locket'           running
Process 'route_registrar'  running
Process 'policy-server'    running
Process 'silk-controller'  running
Process 'uaa'              running
Process 'statsd_injector'  running
Process 'cloud_controller_ng' running
Process 'cloud_controller_worker_local_1' running
Process 'cloud_controller_worker_local_2' running
Process 'nginx_cc'         running
Process 'routing-api'      running
Process 'cloud_controller_clock' running
Process 'cloud_controller_worker_1' running
Process 'auctioneer'       running
Process 'cc_uploader'       running
Process 'file_server'       running
Process 'nsync_listener'   running
Process 'ssh_proxy'        running
Process 'tps_watcher'      running
Process 'stager'           running
Process 'loggregator_trafficcontroller' running
Process 'reverse_log_proxy' running
Process 'adapter'          running
Process 'doppler'          running
Process 'syslog_drain_binder' running
System 'system_localhost'  running
```

6. To access logs, navigate to `/vars/vcap/sys/log` :

```
cd /var/vcap/sys/log
```

7. Run `ls` to list the log directories for each process. See the following example output from the Control VM:

```
control/12b1b027-7ffd-43ca-9dc9-7f4ff204d86a:/var/vcap/sys/log# ls
adapter  cloud_controller_clock  file_server  nginx_cc  route_registrar  statsd_injector  uaa_ctl.err.log
auctioneer  cloud_controller_ng  locket      nginx_newrelic_plugin  routing-api  syslog_drain_binder  uaa_ctl.log
bbs        cloud_controller_worker  loggregator_trafficcontroller  nsync      silk-controller  syslog_forwarder
cc_uploader  consul_agent  metron_agent  policy-server  ssh_proxy  tps
cfdot      doppler      monit        reverse_log_proxy  stager      uaa
```

8. Navigate to the directory of the process that you want to view logs for. For example, for the Cloud Controller process, run `cd cloud_controller_ng/`. From the directory of the process, you can list and view its logs. See the following example output:

```
control/12b1b027-7ffd-43ca-9dc9-7f4ff204d86a:/var/vcap/sys/log/cloud_controller_ng# ls
cloud_controller_ng_ctl.err.log  cloud_controller_ng.log.2.gz  cloud_controller_ng.log.6.gz  drain  pre-start.stdout.log
cloud_controller_ng_ctl.log     cloud_controller_ng.log.3.gz  cloud_controller_ng.log.7.gz  post-start.stderr.log
cloud_controller_ng.log         cloud_controller_ng.log.4.gz  cloud_controller_worker_ctl.err.log  post-start.stdout.log
cloud_controller_ng.log.1.gz    cloud_controller_ng.log.5.gz  cloud_controller_worker_ctl.log  pre-start.stderr.log
```


Release Notes


The Small Footprint PAS tile releases alongside the PAS tile. For more information, see the [PAS Release Notes](#).

Upgrading Pivotal Cloud Foundry

Page last updated:

This topic describes upgrading Pivotal Cloud Foundry (PCF) to v2.2. The upgrade procedure below describes upgrading Pivotal Cloud Foundry Operations Manager (Ops Manager), Pivotal Application Service (PAS), and product tiles.

 **Breaking Changes:** Read the [Release Notes](#) and [Breaking Changes](#) for this release, including the Known Issues sections, before starting the upgrade process.

 **Warning:** Pivotal does not recommend that you skip minor versions when upgrading PCF. Skipping minor versions when upgrading PCF may result in breaking changes. To avoid additional breaking changes, upgrade PCF to the minor version that directly follows your current version of PCF.

The apps in your deployment continue to run during the upgrade. However, you cannot write to your deployment or make changes to apps during the upgrade.

For details about how upgrading PCF impacts individual PAS components, see [Understanding PAS Upgrades](#).


Prepare to Upgrade

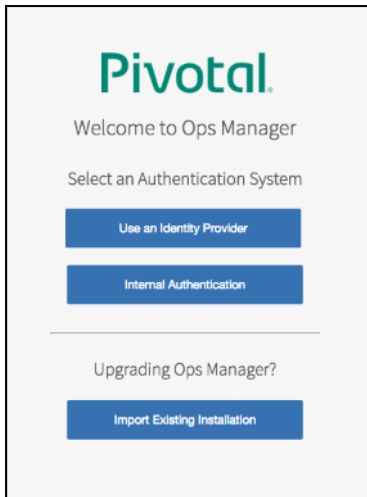
If you have not already, complete the steps in the [Upgrade Preparation Checklist for PCF v2.2](#).

Upgrade Ops Manager and Installed Products to v2.2

Follow these steps to upgrade Ops Manager and Installed Products to PCF v2.2.

Import Installation to Ops Manager v2.2 VM

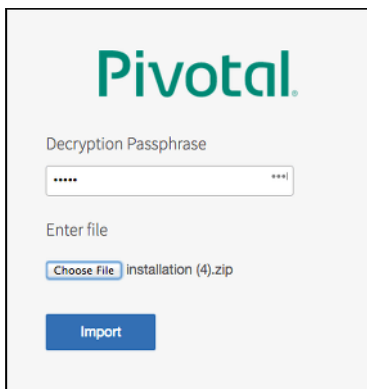
1. Download the Ops Manager VM Template v2.2 from the [Pivotal Network](#)  site.
2. Record the FQDN address of the existing Ops Manager VM.
3. To avoid conflicts, power off the existing Ops Manager VM.
4. Deploy the new Ops Manager VM by following the steps in one of these topics:
 - **AWS:** [Upgrading BOSH Director on AWS](#)
 - **Azure:** [Upgrading BOSH Director on Azure](#)
 - **GCP:** [Upgrading BOSH Director on GCP](#)
 - **OpenStack:** [Deploying Ops Manager to OpenStack](#)
 - **vSphere:** [Deploying Ops Manager on vSphere](#)
5. When redirected to the **Welcome to Ops Manager** page, select **Import Existing Installation**.



- When prompted, enter the **Decryption Passphrase** for this Ops Manager installation. You set this passphrase during your initial installation of Ops Manager.

Note: If lost, the **Decryption Passphrase** cannot be recovered.

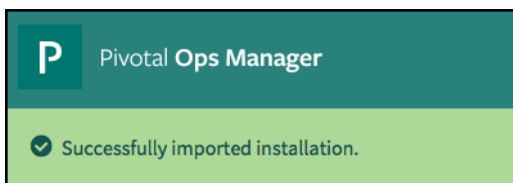
- Click **Choose File** and browse to the installation ZIP file exported in the [Export Your Installation](#) step of your upgrade preparation.



- Click **Import**.

Note: Some browsers do not provide feedback on the status of the import process, and might appear to hang.

- A “Successfully imported installation” message appears upon completion.



Import New PAS and Product Tiles

After upgrading to Ops Manager v2.2, upgrade your product versions:

- Import the product file to your Ops Manager **Installation Dashboard**.
- Hover over the product name in **Available Products** and click **Add**.
- Click the newly added tile to review any configurable options.
- (Optional) If you use other service tiles, you can upgrade them following the same procedure. See the [Upgrading PAS and Other Pivotal Cloud](#)

[Foundry Products](#) topic for more information.

Perform Your Upgrade

⚠ warning: If the installation fails or returns errors, contact [Support](#). Do not attempt to roll back the upgrade by restarting the previous (v2.1) Ops Manager VM.

1. Navigate to the Ops Manager **Installation Dashboard**.
2. Click **Apply Changes**. This immediately imports and applies upgrades to all tiles in a single transaction.

💡 Breaking Change: Only use **Apply Changes** to upgrade tiles immediately after upgrade. Do not use **Review Pending Changes** for selective deployment. For more information, see [Redeploy All Products After Upgrading to Ops Manager v2.2](#)

3. Click each service tile, select the **Status** tab, and confirm that all VMs appear and are in good health.
4. After confirming that the new installation functions correctly, remove the v2.1 Ops Manager VM.

Monitor Upgrade

During the upgrade, you can do the following to monitor your PCF foundation and help troubleshoot any issues.

Check Status and Performance

Note/Reason:

Monitor the progress of the upgrade, checking the status of the foundation at various locations.

Product/component:

PCF

Pivotal recommends live-monitoring your upgrade with PCF Healthwatch, which monitors and alerts on the current health, performance, and capacity of PCF. Healthwatch captures, calculates, stores, visualizes, and alerts on PCF platform metrics, including:

- BOSH-reported VM metrics
- Runtime component metrics
- [Key Performance Indicators](#) and [Key Scaling Indicators](#)
- Healthwatch-generated [super metrics](#)

For more information, see the [PCF Healthwatch documentation](#).

If you are not using PCF Healthwatch, you can do some or all of the following to monitor upgrade progress:

- Run BOSH CLI status checks:

- `bosh -e ALIAS task TASK_NUMBER`
- `bosh -e ALIAS vms --vitals, bosh -e ALIAS instances --ps`

- Check app availability
- Run cf CLI Commands
- Check the availability of the Ops Manager GUI
- Check NAS performance (if using NAS)
- Check vSphere performance (if on vSphere)

Check Diego State

Note/Reason:

See the [cfdot documentation](#) on GitHub for details.

Product/component:

PAS

Use the CF Diego Operator Toolkit (cfdot) to check Diego component instance count by current state.

(Optional) Take Snapshots of Storage Metrics

Note/Reason:

Pivotal recommends this if you have a large foundation and have experienced storage issues in the past.

Product/component:

PCF

Periodically take snapshots of storage metrics.

(Optional) Collect Logs

Note/Reason:

This information helps determine the cause of upgrade issues.

Product/component:

PCF

If you encounter problems during upgrade, collect the following information:

- All job logs
- Task debug logs for VM upgrade tasks
- Installation log from Ops Manager

After Upgrade

After your upgrade, do the following to prepare for use of your new environment, check its health status, and clean up.

Re-Create BOSH Alias

Re-create your alias using BOSH:

```
bosh alias-env ALIAS -e
DIRECTOR_IP
```

- **Note/Reason:** To log into BOSH after upgrading PCF, you need to recreate your alias.
- **Product/Component:** BOSH

Install New cf CLI

Download the version of the Cloud Foundry Command Line Interface (cf CLI) packaged with the [PAS](#) tile on Pivotal Network.

⚠ warning: Due to a regression with x.509 certificates in Go v1.10, Pivotal recommends downloading cf CLI v6.36.2 or later, which use Go v1.9. For more information, see the [v6.36.2](#) change log and [Known Issues](#) in the *Pivotal Application Service v2.2 Release Notes* topic.

Check the Health of Your Deployment

1. Run BOSH CLI commands to check system status:

- ```
bosh -e ALIAS -d DEPLOYMENT_NAME instances --ps
```
- ```
bosh -e ALIAS vms --vitals
```
- ```
bosh -e ALIAS -d DEPLOYMENT_NAME cck --report
```

**Note/Reason:** To ensure that all jobs and process are running as expected

**Product/Component:** PCF and all tiles

2. Push and horizontally scale a test application.

- **Note/Reason:** This is a performance test for PAS.
- **Product/Component:** PCF

3. If you are running PAS MySQL as a cluster, run the `mysql-diag` tool to validate health of the cluster.

- **Note/Reason:** See the BOSH CLI v2 instructions in the [Running mysql-diag](#) [↗](#) topic.
- **Product/Component:** PAS

## Check Resource Settings

If you added custom **VM Type** or **Persistent Disk Type** options, ensure that these values are correctly set and were not overwritten.

- **Note/Reason:** Verify that the Ops Manager **Resource Config** pane still lists your custom options.
- **Product/Component:** PCF

## Run BOSH Clean-Up

Run `bosh -e ALIAS clean-up --all` to clean up old stemcells, releases, orphaned disks, and other unused resources.

- **Product/Component:** Tiles

## What Happens During PAS Upgrades

This topic explains what happens to Pivotal Application Service (PAS) components and apps during a PAS upgrade.

### BOSH Drains Diego Cell VMs

During a PAS upgrade, BOSH drains all Diego cell VMs that host app instances. BOSH manages this process by upgrading a batch of cells one at a time.

When BOSH triggers an upgrade, each upgrading Diego cell enters evacuation mode. In evacuation mode, BOSH stops Diego cells and then schedules replacements for its app instances.

For more information, see the [Specific Guidance for Diego Cells](#) section of the *Configuring PAS for Upgrades* topic.

### cf push Can Become Unavailable

`cf push` is mostly available for the duration of a PAS upgrade. However, `cf push` can become unavailable when a single VM is in use or during BOSH Backup and Restore (BBR).

For more information, see [cf push Availability During Pivotal Application Service Upgrades](#).

## PAS Components Upgrade

This section describes the order in which Ops Manager upgrades components and runs tasks during a full platform upgrade. It also explains how the scale of different Pivotal Application Service (PAS) components affects uptime during upgrades, and which components are scalable.

When performing an upgrade, Ops Manager first upgrades individual components, and then runs one-time tasks.

1. The [Components](#) section describes how Ops Manager upgrades PAS components and explains how individual component upgrades affect broader PAS capabilities.
2. The [One-Time Tasks](#) section lists the tasks that Ops Manager runs after it upgrades the PAS components.

### Components

Ops Manager upgrades PAS components in a fixed order that honors component dependencies and minimizes downtime and other system limitations during the upgrade process.

The type and duration of downtime and other limitations that you can expect during a PAS upgrade reflect the following:

- Component instance scaling. See [How Single-Component Scaling Affects Upgrades](#)
- Component upgrade order. See [Component Upgrade Order and Behavior](#)

#### How Single-Component Scaling Affects Upgrades


In [Pivotal Cloud Foundry](#) (PCF) Ops Manager, the Pivotal Application Service (PAS) tile > **Resource Config** pane shows the components that the BOSH Director installs:

- **Scalable** component fields let you select the instance count from a range of settings or enter a custom value.
- **Unscalable** component fields allow a maximum of one instance.

When a component is scaled at a single instance, it can experience downtime and other limitations while the single VM restarts. This behavior might be acceptable for a test environment. To avoid downtime in a production environment, you should scale any scalable components, such as HAProxy, Router, and Diego cells, to more than one instance.

For more information about how the scale of each component affects upgrade behavior, see the [Component Upgrade Order and Behavior](#) table below.




 **Note:** A full Ops Manager upgrade may take close to two hours, and you will have limited ability to deploy an application during this time.

## Component Upgrade Order and Behavior

The table below lists components in the order that Ops Manager upgrades each. It also lists which components are scalable and explains how component downtime affects PAS app and control availability. The table includes the following columns:

- **Scalable:** Indicates whether the component is scalable above a single instance.

 **Note:** For components marked with a checkmark in this column, we recommend that you change the preconfigured instance value of `1` to a value that best supports your production environment. For more information about scaling a deployment, refer to the [Scaling Cloud Foundry](#) topic.

- **Extended Downtime:** Indicates that if there is only one instance of the component, that component is unavailable for up to five minutes during an Ops Manager upgrade.
- **Downtime Affects...:** Indicates the plane of the PAS platform that component downtime affects, if the component is scaled at single instance:
  - **Apps:** Downtime can affect app availability.
  - **Platform:** Apps remain available during component downtime, but you cannot push, stage, or restart apps, or run other Cloud Foundry command-line interface (cf CLI) commands.
- **Other Limitations and Information:** Provides the following information:
  - Component availability, behavior, and usage during an upgrade
  - Guidance on disabling the component before an upgrade

| Upgrade Order | Component               | Scalable | Extended Downtime | Downtime Affects... |          | Other Limitations and Information                                                                                                                                                                                                                                                              |
|---------------|-------------------------|----------|-------------------|---------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                         |          |                   | Apps                | Platform |                                                                                                                                                                                                                                                                                                |
| 1             | NATS                    | ✓        | ✓                 |                     |          |                                                                                                                                                                                                                                                                                                |
| 2             | File Storage            |          | ✓                 |                     | ✓        |                                                                                                                                                                                                                                                                                                |
| 3             | MySQL Proxy             | ✓        | ✓                 |                     | ✓        | The MySQL Proxy is responsible for managing failover of the MySQL Servers. If the Proxy becomes unavailable, then access to the MySQL Server could be broken.                                                                                                                                  |
| 4             | MySQL Server            | ✓        | ✓                 |                     | ✓        | The MySQL Server is responsible for persisting internal databases for the platform. If the MySQL Server becomes unavailable, then platform services that rely upon a database (Cloud Controller, UAA) will also become unavailable. See <a href="#">Effects of MySQL Downtime</a> for details. |
| 5             | Backup Restore Node     |          |                   |                     |          |                                                                                                                                                                                                                                                                                                |
| 6             | UAA                     | ✓        |                   |                     | ✓        | If a user has an active authorization token prior to performing an upgrade, they can still log in using either a UI or the CLI.                                                                                                                                                                |
| 7             | Cloud Controller        | ✓        | ✓                 |                     | ✓        |                                                                                                                                                                                                                                                                                                |
| 8             | HAProxy                 | ✓        | ✓                 | ✓                   |          | HAProxy is used to load-balance incoming requests to the Router. If HAProxy is unavailable, you may lose the ability to make requests to applications unless there is another routing path from your load balancer to the Router.                                                              |
| 9             | Router                  | ✓        | ✓                 | ✓                   |          | The Router is responsible for routing requests to their application containers. If the Router is not available, then applications cannot receive requests.                                                                                                                                     |
| 10            | MySQL Monitor           |          |                   |                     |          |                                                                                                                                                                                                                                                                                                |
| 11            | Clock Global            | ✓        |                   |                     |          |                                                                                                                                                                                                                                                                                                |
| 12            | Cloud Controller Worker | ✓        | ✓                 |                     |          |                                                                                                                                                                                                                                                                                                |
| 13            | Diego BBS               | ✓        | ✓                 |                     | ✓        |                                                                                                                                                                                                                                                                                                |
| 14            | Diego Brain             | ✓        | ✓                 |                     | ✓        |                                                                                                                                                                                                                                                                                                |

|    |                               |   |   |   |   |                                                                                                                                                                                                                                   |
|----|-------------------------------|---|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15 | Diego Cell                    | ✓ | ✓ | ✓ | ✓ | If you only have one Diego Cell, upgrading causes downtime for all apps that run on it. These include apps pushed with <code>cf push</code> and apps automatically installed by PAS, like Apps Manager and the App Usage Service. |
| 16 | Doppler Server                | ✓ |   |   |   | Ops Manager operators experience 2-5 minute gaps in logging.                                                                                                                                                                      |
| 17 | Loggregator Trafficcontroller | ✓ |   |   |   | Ops Manager operators experience 2-5 minute gaps in logging.                                                                                                                                                                      |
| 18 | TCP Router (if enabled)       | ✓ |   |   |   |                                                                                                                                                                                                                                   |

## One-Time Tasks

After Ops Manager upgrades components, it performs system checks and launches UI apps and other PAS components as Cloud Foundry apps. These tasks run in the following order:

|    |                                                                           |
|----|---------------------------------------------------------------------------|
| 1  | Apps Manager Errand - Push Apps Manager                                   |
| 2  | Smoke Test Errand - Run smoke tests                                       |
| 3  | Usage Service Errand - Push Usage Service app                             |
| 4  | Notifications Errand - Push Notifications app                             |
| 5  | Notifications UI Errand - Push Notifications UI                           |
| 6  | App Autoscaler Errand - Push App Autoscaler                               |
| 7  | App Autoscaler Smoke Test Errand - Run smoke tests against App Autoscaler |
| 8  | Register Autoscaling Service Broker                                       |
| 9  | Destroy Autoscaling Service Broker                                        |
| 10 | Bootstrap Errand - Recover MySQL cluster                                  |
| 11 | MySQL Rejoin Unsafe Errand                                                |

## Upgrading Installation Example

For sample performance measurements of an upgrading Cloud Foundry installation, see [Upgrade Load Example: Pivotal Web Services](#).

## Upgrade Preparation Checklist for PCF v2.2

This topic serves as a checklist for preparing to upgrade Pivotal Cloud Foundry (PCF) from v2.1 to v2.2.

This topic contains important preparation steps that you must follow before beginning your upgrade. Failure to follow these instructions may jeopardize your existing deployment data and cause the upgrade to fail.

After completing the steps in this topic, you can continue to [Upgrading Pivotal Cloud Foundry](#).

**Warning:** Pivotal does not recommend that you skip minor versions when upgrading PCF. Skipping minor versions when upgrading PCF may result in breaking changes. To avoid additional breaking changes, upgrade PCF to the minor version that directly follows your current version of PCF.

## Back Up Your PCF Deployment

Pivotal recommends backing up your PCF deployment before upgrading, to restore in the case of failure. To do this, follow the instructions in the [Backing Up Pivotal Cloud Foundry with BBR](#) topic.

## Find Your Decryption Passphrase for Ops Manager

To complete the Ops Manager upgrade, you must have your Ops Manager decryption passphrase. You defined this decryption passphrase during the initial installation of Ops Manager.

## Review Changes in PCF v2.2

Review each of the following links to understand the changes in the new release, such as new features, known issues, and breaking changes.

- **Release Notes**
  - [Ops Manager Release v2.2 Release Notes](#)
  - [PAS v2.2 Release Notes](#)
- **Known Issues**
  - [Ops Manager v2.2 Known Issues](#)
  - [PAS v2.2 Known Issues](#)
  - The following Pivotal Knowledge Base (KB) articles describe known issues for **PCF v2.2**:
    - [How to avoid app downtime while upgrading from PAS v2.1.x to v2.2.7 or Later](#)
    - [App Autoscaler Smoke Test Errand fails to retrieve any metrics from logcache](#)
    - [Operations Manager Validation Returns TLS Error When Configuring BOSH Director S3 Blobstore](#)
    - [Some Components Use Go v1.9 to Avoid x.509 Cert Errors in v1.10](#)
    - [Apps Serve Routes Even After App Deletion Due To MySQL Errors](#)
    - [Deployment Fails Because Monit Reports Job as Failed](#)
    - [Deploying PAS for Windows Tile Results in an Access is Denied Error](#)
    - [Timeouts Connecting to GCS Blobstores when Configured to use Service Account Key authentication](#)
    - [Spring Cloud Services Deployment fails with can't resolve link error in PAS 2.2](#)
    - [Unable to import Xenial stemcell when upgrading to tile that requires Xenial](#)
    - [Apps Manager shows a blank page after upgrading to PAS 2.2](#)
    - [Java Apps crash with too many open files after upgrading to PAS 2.2 using JBP 4.7 or earlier](#)
    - [App Autoscaler Smoke Test Errand fails to retrieve any metrics from logcache](#)
    - [Troubleshooting "NetworkReservationNotEnoughCapacity" Using the BOSH Command Line to Determine IP Usage](#)
    - [Diego Cell Garden healthcheck fails and becomes unhealthy](#)
    - [Java Applications crashing after upgrading to PCF 1.12 or higher](#)
    - [PAS backup-prepare job renamed to backup-restore may cause automation failures](#)
    - [PCF upgrade fails with StacklessAndStackfulMatchingBuildpacksExistError](#)
    - [Upgrade to RabbitMQ for PCF tile 1.13 fails with lock against the Mnesia DB](#)
- **Breaking Changes**

- [PCF v2.2 Breaking Changes](#)
- KPI Changes
  - [KPI Changes from PCF v2.1 to v2.2](#)
- Diego Network Communications:
  - [Diego Network Communications](#)

## Update Tiles and Add-Ons

The following section describes changes you must make to your product tiles and add-ons before upgrading PCF.

### Review Tile Compatibility

Before you upgrade to PCF v2.2, please check whether the service tiles that you currently have deployed on PCF v2.1 are compatible with PCF v2.2.

To check PCF versions supported by a service tile, either from Pivotal or a Pivotal partner:

- Navigate to the tile's download page on [Pivotal Network](#).
- Select the tile version in the **Releases** dropdown.
- See the **Depends On** section under **Release Details**. For more information, refer to the tile's release notes.

If the currently-deployed version of a tile is not compatible with PCF v2.2, you must upgrade the tile to a compatible version before you upgrade PCF. You do not need to upgrade tiles that are compatible with both PCF v2.1 and v2.2.

Some partner service tiles may be incompatible with PCF v2.2. Pivotal works with partners to ensure their tiles are updated to work with the latest versions of PCF. For more information about which partner service release compatibility, review the **Depends On** section of the partners tile download page, the partners services release documentation in [Pivotal Documentation](#), or contact the partner organization that produces the service tile.

The [Product Compatibility Matrix](#) provides an overview of which PCF versions support which versions of the most popular service tiles from Pivotal.

### Environment Details

Pivotal provides the empty table below as a model to print out or adapt for recording and tracking the tile versions that you have deployed in all of your environments.

|                                        |                                                   | Sandbox | Non-Prod | Prod | Other... |
|----------------------------------------|---------------------------------------------------|---------|----------|------|----------|
| Pivotal Cloud Foundry                  | <a href="#">Ops Manager</a>                       |         |          |      |          |
|                                        | <a href="#">Pivotal Application Service</a> (PAS) |         |          |      |          |
| Pivotal Cloud Foundry Services         | <a href="#">MySQL v2</a>                          |         |          |      |          |
|                                        | <a href="#">Redis</a>                             |         |          |      |          |
|                                        | <a href="#">RabbitMQ</a>                          |         |          |      |          |
|                                        | <a href="#">Single Sign On</a> (SSO)              |         |          |      |          |
|                                        | <a href="#">Spring Cloud Services</a>             |         |          |      |          |
|                                        | <a href="#">Concourse</a>                         |         |          |      |          |
|                                        | ...                                               |         |          |      |          |
| Pivotal Cloud Foundry Partner Services | <a href="#">New Relic</a>                         |         |          |      |          |
|                                        | ...                                               |         |          |      |          |

### Upgrade Services Tiles

Upgrade all service tiles to versions that are compatible with PCF v2.2. Service tiles are add-on products you install alongside your runtime. For example, MySQL for PCF, PCF Healthwatch, and RabbitMQ are service tiles.

Do not upgrade runtime tiles, such as PAS, PAS for Windows (PASW), or Pivotal Container Service (PKS), at this time.

Review the [Compatibility Matrix](#) and tile documentation to check version compatibility.

## Configure BOSH Director

With each release of a new PCF version, BOSH Director may require specific updates before upgrading to the new version. See the following sections for what action to take before upgrading to PCF v2.2:

1. If you disabled BOSH DNS, reenable it. In the **Director Config** pane of the **BOSH Director** tile, clear the **Disable BOSH DNS server for troubleshooting purposes** checkbox.
2. Check the required machine specifications for Ops Manager v2.2. These specifications are specific to your IaaS. If these specifications do not match your existing Ops Manager, modify the values of your Ops Manager VM instance. For example, if the boot disk of your existing Ops Manager is 50 GB and the new Ops Manager requires 100 GB, then increase the size of your Ops Manager boot disk to 100 GB.

## Disable Unused Errands

To save upgrade time, you can disable unused PAS post-deploy errands. See the [Post-Deploy Errands](#) section of the Errands topic for details. Only disable these errands if your environment does not need them.

In some cases, if you have previously disabled lifecycle errands for any installed product to reduce deployment time, you may want to re-enable these errands before upgrading. For more information, see the [Adding and Deleting Products](#) topic.

## Check OS Compatibility of PCF and BOSH-Managed Add-Ons

Before upgrading to PCF v2.2, operators who have deployed any PCF add-ons such as **IPsec for PCF**, **ClamAV for PCF**, or **File Integrity Monitoring for PCF** and who have deployed or are planning to deploy [PAS for Windows 2012R2](#) must modify the add-on manifest to specify a compatible OS stemcell.

For example, **File Integrity Monitor for PCF** (FIM) is not supported on Windows. Therefore, the manifest must use an `include` directive to specify the target OS stemcell of `ubuntu-trusty`.

To update an add-on manifest, do the following:

1. Locate your existing add-on manifest file. For example, for FIM, locate the `fim.yml` you uploaded to the Ops Manager VM.
2. Modify the manifest to include following `include` directive to your manifest:

```
include:
 stemcell:
 - os: ubuntu-trusty
```

- a. Re-upload the manifest file to your PCF deployment. For example instructions, see [Create the FIM Manifest](#).

If you are using any other BOSH-managed add-ons in your deployment, you should verify OS compatibility for those component as well. For more information about configuring BOSH add-on manifests, see the [BOSH documentation](#).

## Check Backup and Restore External Blobstore Add-On


If you have enabled external blobstore backups for an Azure Blobstore using the [Blobstore Add-On](#), you need to update your runtime configuration to remove the `sdk-preview` add-on before upgrading to PCF v2.2. If you do not remove this job, upgrading PAS fails with the error:

```
Preparing deployment: Preparing deployment (00:00:01)
L Error: Colocated job 'azure-blobstore-backup-restorer' is already added to the instance group 'backup-restore'.
```

After removing this job from your runtime configuration, ensure that the **Enable backup and restore** checkbox is enabled in the PAS tile > **File Storage** pane. See [External Azure Storage](#) for instructions.

## Check Certificate Authority Expiration Dates

Depending on the requirements of your deployment, you may need to rotate your Certificate Authority (CA) certificates. The non-configurable certificates in your deployment expire every two years. You must regenerate and rotate them so that critical components do not face a complete outage.

 **Note:** PCF uses SHA-2 certificates and hashes by default. You can convert existing SHA-1 hashes into SHA-2 hashes by rotating your Ops Manager certificates using the procedure described in the [Regenerating and Rotating Non-Configurable TLS/SSL Certificates](#) section of *Managing TLS Certificates*.

To retrieve information about all the RSA and CA certificates for the BOSH Director and other products in your deployment, you can use the `GET /api/v0/deployed/certificates?expires_within=TIME` request of the Ops Manager API.

In this request, the `expires_within` parameter is optional. Valid values for the parameter are `d` for days, `w` for weeks, `m` for months, and `y` for years. For example, to search for certificates expiring within one month, replace `TIME` with `1m`:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/certificates?expires_within=1m" \
-X GET \
-H "Authorization: Bearer UAA_ACCESS_TOKEN"
```

For information about regenerating and rotating CA certificates, see [Managing TLS Certificates](#).

## Check the Capacity of Your Deployment

The following sections describe steps for ensuring your deployment has adequate capacity to perform the upgrade.

### Confirm Adequate Disk Space

Confirm that you have adequate disk space for your upgrades. You need at least 20 GB of free disk space to upgrade PCF Ops Manager and Pivotal Application Service. If you plan to upgrade other products, the amount of disk space required depends on how many tiles you plan to deploy to your upgraded PCF deployment.

To check current persistent disk usage, select the **BOSH Director** tile from the **Installation Dashboard**. Select **Status** and review the value of the 

|               |
|---------------|
| PERS.<br>DISK |
|---------------|

 column. If persistent disk usage is higher than 50%, select **Settings > Resource Config**, and increase your persistent disk space to handle the size of the resources. If you do not know how much disk space to allocate, set the value to at least `100 GB`.

### Check Diego Cell RAM and Disk

Check that Diego cells have sufficient available RAM and disk capacity to support app containers.

The KPIs that monitor these resources are:

- `rep.CapacityRemainingMemory`
- `rep.CapacityRemainingDisk`

### Adjust Diego Cell Limits

If needed, adjust the maximum number of Diego cells that the platform can upgrade simultaneously, to avoid overloading the other cells. See [Managing Diego Cell Limits During Upgrade](#).

For PCF v1.10 and later, the maximum number of cells that can update at once, `max_in_flight` is 4%. This setting is configured in the BOSH manifest's Diego cell definition. See the [Preventing Overload](#) section for details.

Review the [Diego Cell Metrics](#) section of the KPI topic for more information about these KPIs.

## Review File Storage IOPS and Other Upgrade Limiting Factors

During the PCF upgrade process, a large quantity of data is moved around on disk.

To ensure a successful upgrade of PCF, verify that your underlying PAS file storage is performant enough to handle the upgrade. For more information about the configurations to evaluate, see [Upgrade Considerations for Selecting Pivotal Cloud Foundry Storage](#).

In addition to file storage IOPS, consider additional existing deployment factors that can impact overall upgrade duration and performance:

| Factor                                         | Impact                                                                                                                                                 |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network latency                                | Network latency can contribute to how long it takes to move app instance data to new containers.                                                       |
| Number of ASGs                                 | A large number of <a href="#">Application Security Groups</a> in your deployment can contribute to an increase in app instance container startup time. |
| Number of app instances and application growth | A large increase in the number of app instances and average droplet size since the initial deployment can increase the upgrade impact on your system.  |

To review example upgrade-related performance measurements of an existing production Cloud Foundry deployment, see the [Pivotal Web Services Performance During Upgrade](#) topic.

## Run BOSH Clean-Up

Run `bosh -e ALIAS clean-up --all` to clean up old stemcells, releases, orphaned disks, and other resources before upgrade. This cleanup helps prevent the product and stemcell upload process from exceeding the BOSH Director's available persistent disk space.

## Check the Health of Your Deployment

The following sections describe steps for ensuring your deployment is healthy before you perform the upgrade.

### Collect Foundation Health Status

For collecting foundation health status, Pivotal recommends PCF Healthwatch, which monitors and alerts on the current health, performance, and capacity of PCF. For more information, see the [PCF Healthwatch documentation](#).

If you are not using PCF Healthwatch, you can do some or all of the following to collect foundation health status:

- If your PCF deployment has external metrics monitoring set up, verify that VM CPU, RAM, and disk use levels are within reasonable levels.
- Run BOSH CLI commands to check system status:
  - `bosh -e ALIAS -d DEPLOYMENT_NAME instances --ps`.  
`bosh instances` with the flags `--ps`, `--vitals`, or `--failing` highlights individual job failure.
  - `bosh -e ALIAS vms --vitals`. This reveals VMs with high CPU, high memory, high disk utilization, and with `state != running`.
  - `bosh -e ALIAS -d DEPLOYMENT_NAME cck --report`
- Check Ops Manager GUI each PAS/Tiles the status page for CPU/RAM/DISK utilization
- Validate Ops Manager persistent disk usage is below 50%. If not, follow the procedure in [Confirm Adequate Disk Space](#).

(Optional) Check the logs for errors before proceeding with the upgrade. For more information, see [Viewing Logs in the Command Line Interface](#).

## Push and Scale a Test App

Check that a test app can be pushed and scaled horizontally, manually or through automated testing. This check ensures that the platform supports apps as expected before the upgrade.

## Validate Installed Buildpacks

Buildpacks may now have an [associated stack](#) denoting which stacks they are compatible with. During this transition, PAS will begin installing multiple versions of buildpacks for different stacks (e.g. `cflinuxfs2`, `cflinuxfs3`, etc.). To ensure that the buildpacks are [installed without errors](#), if you have multiple buildpacks installed with the same name all buildpacks with that name must be associated with a stack. Additionally, any buildpacks that do not

have an associated stack should be unlocked prior to upgrading. Refer to the [following documentation](#) for more information on associating a stack with an existing buildpack.

## Validate MySQL Cluster Health

If you are running PAS MySQL as a cluster, run the `mysql-diag` tool to validate health of the cluster.

See the BOSH CLI v2 instructions in the [Running mysql-diag](#) topic.

## Review Pending and Recent Changes

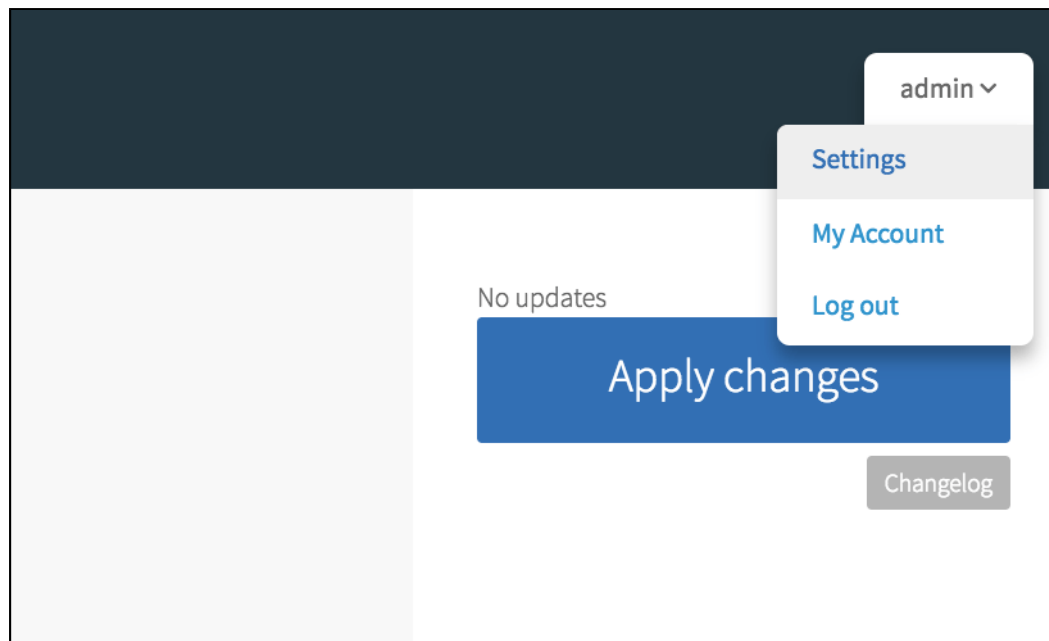
1. Confirm there are no outstanding changes in Ops Manager or any other tile. All tiles should be **green**. Click **Review Pending Changes**, then **Apply Changes** if necessary.
2. After applying changes, click **Recent Install Logs** to confirm that the changes completed cleanly:

```
Cleanup complete
{"type": "step_finished", "id": "clean_up_bosh.cleaning_up"}
Exited with 0.
```

## Export Your Installation

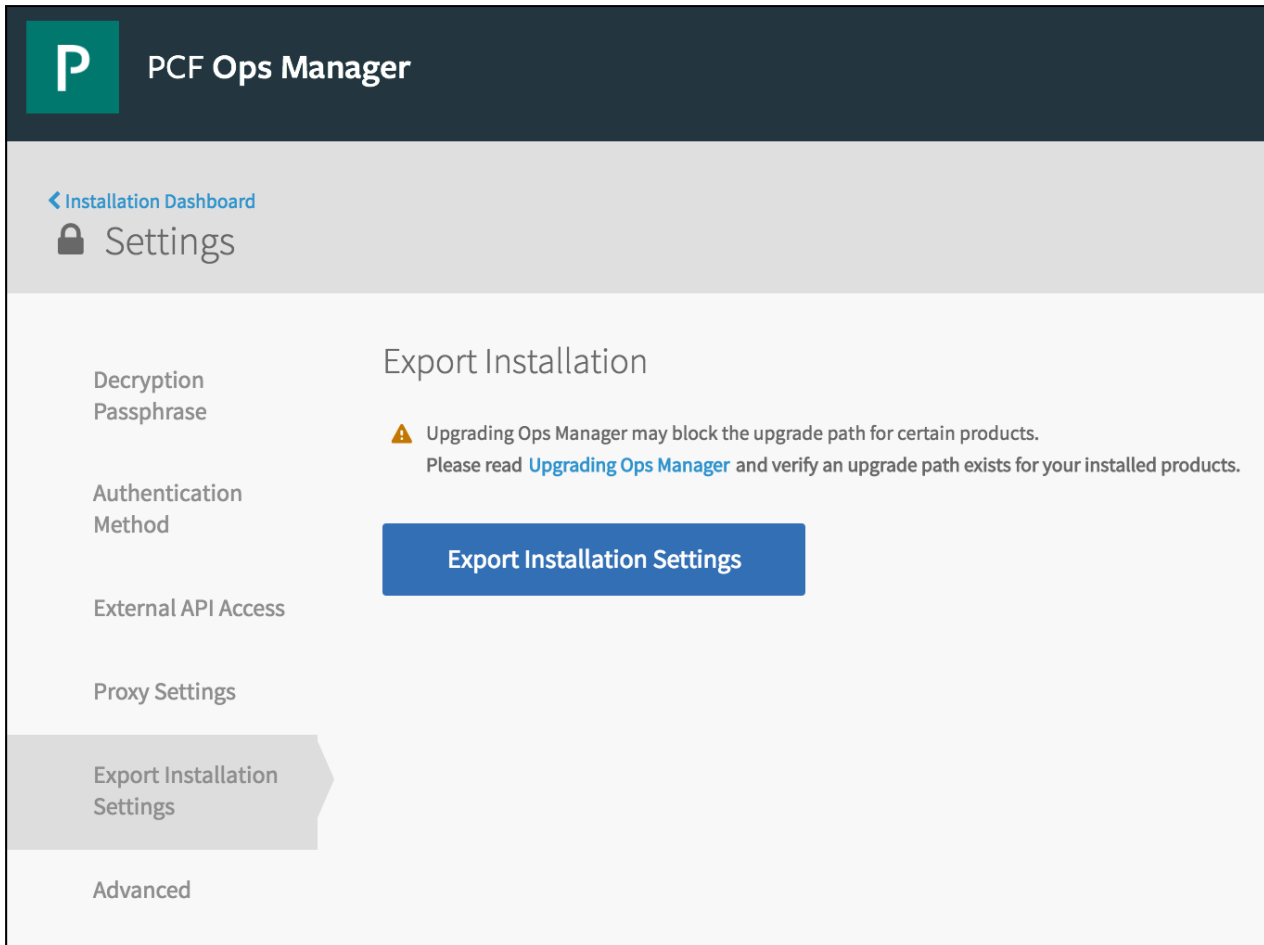
To export your installation, do the following:

1. In your Ops Manager v2.1 **Installation Dashboard**, click the account dropdown and select **Settings**.



2. On the **Settings** screen, select **Export Installation Settings** from the left menu, then click **Export Installation Settings**.



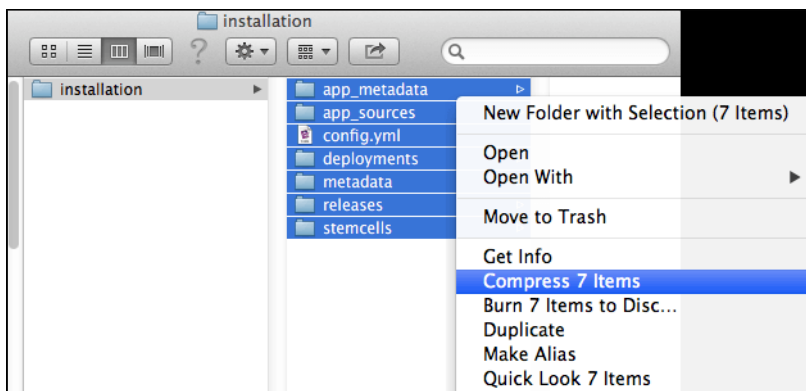


This exports the current PCF installation with all of its assets.

When you export an installation, the export contains the base VM images, necessary packages, and configuration settings, but does not include releases between upgrades if Ops Manager has already uploaded them to BOSH. When backing up PCF, you must take this into account by backing up the BOSH blobstore that contains the uploaded releases. BOSH Backup and Restore (BBR) backs up the BOSH blobstore. For more information, see [Backing Up Pivotal Cloud Foundry with BBR](#).

- The export time depends on the size of the exported file.
- Some browsers do not provide feedback on the status of the export process and might appear to hang.

**Note:** Some operating systems automatically unzip the exported installation. If this occurs, create a ZIP file of the unzipped export. Do not start compressing at the “installation” folder level. Instead, start compressing at the level containing the `config.yml` file:



**Warning:** If you fail to perform the remedial steps for this issue, this upgrade process may corrupt your existing usage data.

## Next Steps

Now that you have completed the Upgrade Preparation Checklist for PCF v2.2, continue to [Upgrading Pivotal Cloud Foundry](#).

## Complete Survey

Please take some time to help us improve this document by completing the [Upgrade Checklist Survey](#) [↗](#).

## Configuring PAS for Upgrades

This topic describes several configuration options for Pivotal Application Service (PAS) that can help ensure successful upgrades. In addition to following the [Upgrade Preparation Checklist](#), review the sections in this document to better understand how to prepare for PAS Upgrades.

### Limit PCF Component Instance Restarts

The `max_in_flight` variable limits how many instances of a component can restart simultaneously during updates or upgrades. Increasing the value of `max_in_flight` can make updates run faster, but setting it too high risks overloading VMs and causing failure. See [Best Practices](#) for guidance on setting `max_in_flight` values.

Values for `max_in_flight` can be any integer between 1 and 100, or a percentage of the total number of instances. For example, a `max_in_flight` value of `20%` in a deployment with 10 Diego cell instances would make no more than two cell instances restart at once.

### Set max\_in\_flight

The `max_in_flight` variable is a system-wide value with optional component-specific overrides. You can override the default value for individual jobs using an API endpoint.

#### Use the max\_in\_flight API Endpoint

Use the `max_in_flight` API endpoint to configure the maximum value for component instances that can start at a given time. This endpoint overrides product defaults. You can specify values as a percentage or an integer.

Use the string “default” as the `max_in_flight` value to force the component to use the deployment’s default value.

**Note:** The example below lists three JOB\_GUIDs. These three GUIDs are examples of the three different types of values you can use to configure `max_in_flight`. The endpoint only requires one GUID.

```
curl "https://EXAMPLE.com/api/v0/staged/products/PRODUCT-TYPE1-GUID/max_in_flight" \
-X PUT \
-H "Authorization: Bearer UAA_ACCESS_TOKEN" \
-H "Content-Type: application/json" \
-d '{
 "max_in_flight": {
 "JOB_1_GUID": 1,
 "JOB_2_GUID": "20%",
 "JOB_3_GUID": "default"
 }
}'
```

### Specific Guidance for Diego Cells

To upgrade Cloud Foundry, BOSH must drain all Diego cell VMs that host app instances. BOSH manages this process by upgrading a batch of cells at a time.

The number of cells that undergo upgrade simultaneously (either in a state of shutting down or coming back online) is controlled by the `max_in_flight` value of the Diego cell job. For example, if `max_in_flight` is set to `10%` and your deployment has 20 Diego cell job instances, then the maximum number of cells that BOSH can upgrade at a single time is `2`.

When BOSH triggers an upgrade, each Diego cell undergoing upgrade enters “evacuation” mode. Evacuation mode means that the cell stops accepting new work and signals the rest of the Diego system to schedule replacements for its app instances. This scheduling is managed by the [Diego auctioneer process](#).

The evacuating cells continue to interact with the Diego system as replacements come online. The cell undergoing upgrade waits until either its app instance replacements run successfully before shutting down the original local instances, or for the evacuation process to time out. This “evacuation timeout” defaults to 10 minutes.

If cell evacuation exceeds this timeout, then the cell stops its app instances and shuts down. The Diego system continues to re-emit start requests for the

app replacements.

## Prevent Overload

A potential issue arises if too many app instance replacements are slow to start or do not start successfully at all.

If too many app instances are starting concurrently, then the load of these starts on the rest of the system can cause other applications that are already running to crash and be rescheduled. These events can result in a cascading failure.

To prevent this issue, PCF provides two throttle configurations: the maximum number of in-flight diego cell instances and the maximum number of starting containers.

The values of the above throttle configurations depend on the version of PCF that you have deployed and whether you have overridden the default values.

Refer to the following table for existing defaults and, if necessary, determine the override values in your deployment.

| PCF Version            | Starting Container Count Maximum | Starting Container Count Overridable? | Maximum In Flight Diego Cell Instances | Maximum In Flight Diego Cell Instances Overridable? |
|------------------------|----------------------------------|---------------------------------------|----------------------------------------|-----------------------------------------------------|
| PCF 1.7.43 and earlier | No limit set                     | No                                    | 1 instance                             | No                                                  |
| PCF 1.7.44 to 1.7.49   | 200                              | No                                    | 1 instance                             | No                                                  |
| PCF 1.7.50 +           | 200                              | No                                    | 1 instance                             | No                                                  |
| PCF 1.8.0 to 1.8.29    | No limit set                     | No                                    | 10% of total instances                 | No                                                  |
| PCF 1.8.30 +           | 200                              | Yes                                   | 10% of total instances                 | No                                                  |
| PCF 1.9.0 to 1.9.7     | No limit set                     | No                                    | 4% of total instances                  | Yes                                                 |
| PCF 1.9.8 +            | 200                              | Yes                                   | 4% of total instances                  | Yes                                                 |
| PCF 1.10.0 and later   | 200                              | Yes                                   | 4% of total instances                  | Yes                                                 |
| PCF 1.12.0 and later   | 200                              | Yes                                   | 4% of total instances                  | Yes                                                 |

## Best Practices

Set the `max_in_flight` variable high enough that the remaining component instances are not overloaded by typical use. If component instances are overloaded during updates, upgrades, or typical use, users may experience downtime.

Some more precise guidelines include:

- For jobs with high resource usage, set `max_in_flight` low. For example, for Diego cells, `max_in_flight` allows non-migrating cells to pick up the work of cells stopping and restarting during migration. If resource usage is already close to 100%, scale up your jobs before making any updates.
- For quorum-based components (these are components with odd-numbered settings in the manifest), such as etcd, consul, and Diego BBS, set `max_in_flight` to 1. This preserves quorum and prevents a [split-brain scenario](#) from occurring as jobs restart.
- For other components, set `max_in_flight` to the number of instances that you can afford to have down at any one time. The best values for your deployment vary based on your capacity planning. In a highly redundant deployment, you can make the number high so that updates run faster. If your components are at high utilization, however, you should keep the number low to prevent downtime.
- Never set `max_in_flight` to a value greater than or equal to the number of instances you have running for a component.

## Set a Maximum Number of Starting Containers

This section describes how to use the auctioneer job to configure the maximum number of app instances starting at a given time. This prevents Diego from scheduling too much new work for your platform to handle concurrently. A lower default can prevent server overload during cold start, which may be important if your infrastructure is not sized for a large number of concurrent cold starts.

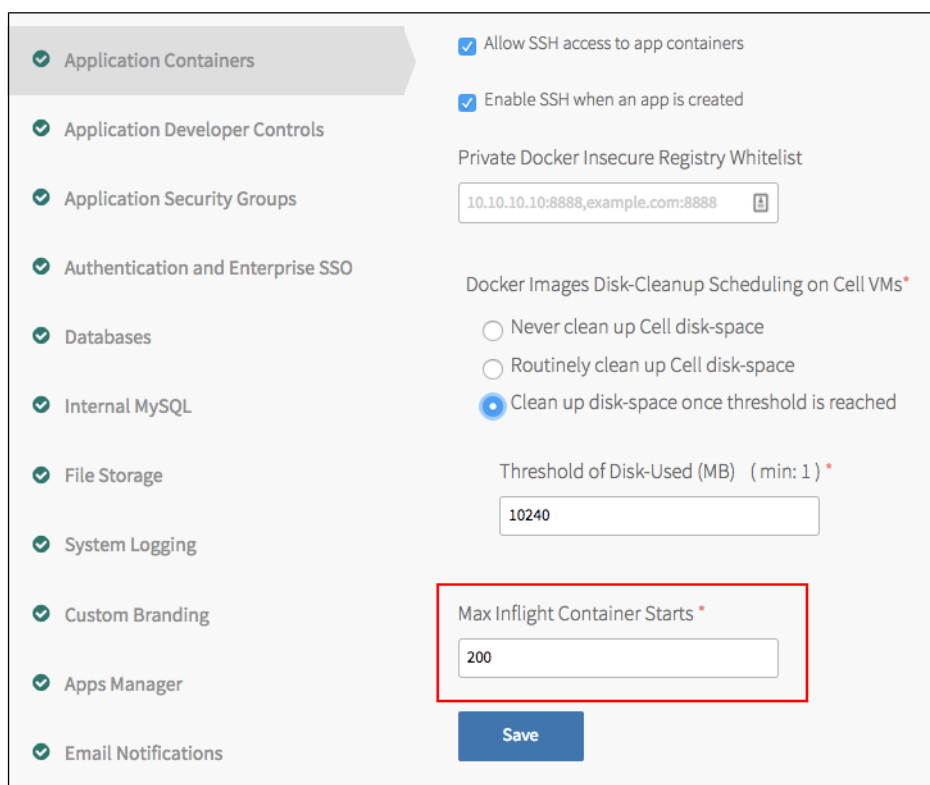
The auctioneer only schedules a fixed number of app instances to start concurrently. This limit applies to both single and multiple Diego Cells. For

example, if you set the limit to five starting instances, it does not matter if you have one Diego Cell with ten instances or five Diego Cells with two instances each. The auctioneer will not allow more than five instances to start at the same time.

If you are using a cloud-based IaaS, rather than a smaller on-premise solution, Pivotal recommends setting a larger default. By default, the maximum number of started instances is 200.

You can configure the maximum number of started instances in the Settings tab of the Pivotal Application Service (PAS) tile.

1. Log in to Operations Manager.
2. Click the PAS tile.
3. Click **Application instances** in the sidebar.
4. In the Max Inflight Container Starts field, type the maximum number of started instances.



The screenshot shows the 'Application Containers' settings page. On the left, a sidebar lists settings categories: Application Containers (selected), Application Developer Controls, Application Security Groups, Authentication and Enterprise SSO, Databases, Internal MySQL, File Storage, System Logging, Custom Branding, Apps Manager, and Email Notifications. The main content area includes checkboxes for 'Allow SSH access to app containers' and 'Enable SSH when an app is created', both checked. Below these is a 'Private Docker Insecure Registry Whitelist' field containing '10.10.10.10:8888,example.com:8888'. Further down is a section for 'Docker Images Disk-Cleanup Scheduling on Cell VMs\*' with three radio button options: 'Never clean up Cell disk-space', 'Routinely clean up Cell disk-space', and 'Clean up disk-space once threshold is reached' (selected). Below this is a 'Threshold of Disk-Used (MB) (min: 1) \*' field with the value '10240'. At the bottom, a red box highlights the 'Max Inflight Container Starts \*' field, which contains the value '200'. A 'Save' button is located at the bottom right of the settings area.

5. Click **Save**.

## Configure File Storage

This section describes critical factors to consider when evaluating the type of file storage to use in your Pivotal Cloud Foundry (PCF) deployment. The [Pivotal Application Service \(PAS\) blobstore](#) relies on the file storage system to read and write resources, app packages, and droplets.

During an upgrade of PCF, file storage with insufficient IOPS numbers can negatively impact the performance and stability of your PCF deployment.

If disk processing time takes longer than the evacuation timeout for Diego cells, then Diego cells and app instances may take too long to start up, resulting in a cascading failure.

However, the minimum required IOPS depends upon a number of deployment-specific factors and configuration choices. Use this section as a guide when deciding on the file storage configuration for your deployment.

To see an example of system performance and IOPS load during an upgrade, refer to [Upgrade Load Example: Pivotal Web Services](#).

## Select Internal or External File Storage

When you deploy PCF, you can select internal file storage or external file storage, either network-accessible or IaaS-provided, as an option in the PAS

tile.

Selecting internal storage causes PCF to deploy a dedicated virtual machine (VM) that uses either NFS or WebDAV for file storage. Selecting external storage allows you to configure file storage provided in network-accessible location or by an IaaS, such as Amazon S3, Google Cloud Storage, or Azure Storage.


Whenever possible, Pivotal recommends using external file storage.

## Calculate Potential Disk Load Requirements

As a best-effort calculation, estimate the total number of bits needed to move during a system upgrade to determine how IOPS-performant your file storage needs to be.

### ◦ Number of Diego Cells

- As a first calculation, determine the number of Diego cells that your deployment currently uses. To view the number of Diego cell instances currently running in your deployment, see the **Resource Config** section of your PAS tile. If you expect to scale up the number of instances, use the anticipated scaled number.

 **Note:** If your deployment uses more than 20 Diego cells, you should avoid using internal file storage. Instead, you should always select external or IaaS-provided file storage.

### ◦ Maximum In-Flight Load and Container Starts for Diego Cells

- Operators can limit the number of containers and Diego cell instances that Diego starts concurrently. If operators impose no limits, your file storage may experience exceptionally heavy load during an upgrade.

## Upgrade Load Example: Pivotal Web Services

Page last updated:

This topic provides sample performance measurements of a Cloud Foundry installation undergoing the workload associated with an upgrade.

To obtain these measurements, Pivotal repaved its production Pivotal Web Services (PWS) deployment. The repave process simulates system load that would be incurred when performing a rolling upgrade of Diego cells.

Use the measurements and configuration values published in this document as guidance when ensuring you have adequate file storage hardware prior to a platform upgrade.

For more information about the impact of upgrade on file storage performance, see [Upgrade Considerations for Selecting File Storage in Pivotal Cloud Foundry](#).


## Platform Configuration

The following table details the starting parameters and configuration of PWS.

| Configuration                                | Value                                         | How to Locate                                                                                                                                                                                                                                |
|----------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IaaS                                         | Amazon Web Services                           | Refer to your BOSH Director configuration or BOSH deployment manifest.                                                                                                                                                                       |
| File Storage                                 | AWS EBS (External with some elastic capacity) | Refer to your Pivotal Application Service (PAS) configuration or BOSH deployment manifest.                                                                                                                                                   |
| Version of CF                                | v252                                          | Refer to your BOSH Director and PAS configuration or BOSH deployment manifest.                                                                                                                                                               |
| Number of Diego Cells                        | 218                                           | To view the number of Diego cell instances currently running in your deployment, see the <b>Resource Config</b> section of your PAS tile or consult your Diego deployment manifest.                                                          |
| Maximum Number of Started Containers         | 250                                           | See <a href="#">PCF</a> documentation for configuration information.                                                                                                                                                                         |
| max_in_flight Configuration for Diego Cells  | 6                                             | To retrieve the existing <code>max_in_flight</code> value for the Diego Cell job in BOSH Director, use the Ops Manager API. See the Ops Manager API documentation. If you are running open source CF, consult your BOSH deployment manifest. |
| Number of Availability Zones (AZ)            | 2                                             | Consult your PAS or BOSH deployment AZ configuration.                                                                                                                                                                                        |
| Number of App Instances                      | 16231                                         | <code>datadog.nozzle.bbs.LRPsRunning</code>                                                                                                                                                                                                  |
| Number of Application Security Groups (ASGs) | 43                                            | As admin user, run the <code>cf security-groups</code> command. For more information, see <a href="#">Application Security Groups</a> .                                                                                                      |

## System Performance Measurements During Cell Repave

This table presents performance measurements taken during the Diego cell repave.

 **Note:** These measurements indicate the peak cumulative values of the entire system (250 Diego cells, ~15,000 application instances, and 2 AZs.)

Use these measurements as a baseline for expected system load during Diego cell upgrade.

| Measurement             | Value | Metric Used                                           |
|-------------------------|-------|-------------------------------------------------------|
| Cell CPU Consumption    | 36%   | <code>bosh.healthmonitor.system.cpu.usage</code>      |
| Cell Memory Consumption | ~50%  | <code>bosh.healthmonitor.system.memory.percent</code> |

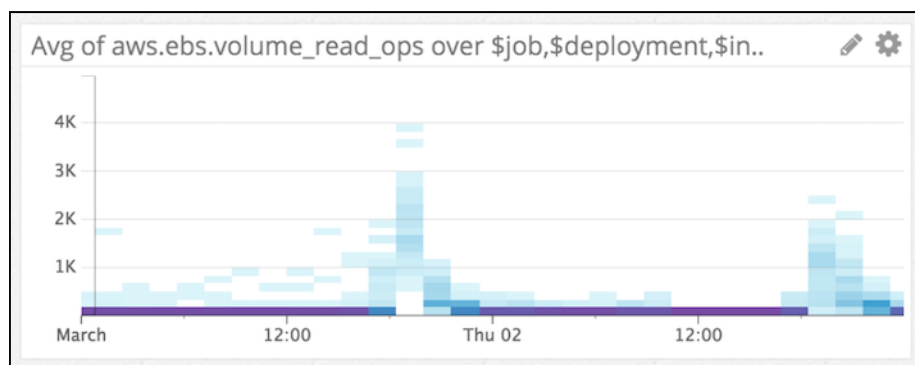
|                                                                 |                                             |                                       |
|-----------------------------------------------------------------|---------------------------------------------|---------------------------------------|
| Cell I/O Consumption (Read) During Normal Operations            | 43 Read I/O Operations per second           | <code>aws.ebs.volume_read_ops</code>  |
| Cell I/O Consumption (Read) During Upgrade                      | 1,943 Read I/O Operations per second        | <code>aws.ebs.volume_read_ops</code>  |
| Cell IO Consumption (Write) During Normal Operations            | 2,166 Write I/O Operations per second       | <code>aws.ebs.volume_write_ops</code> |
| Cell IO Consumption (Write) During Upgrade                      | 21,000 Write I/O Operations per second      | <code>aws.ebs.volume_write_ops</code> |
| Cell Network Consumption (Network Out) During Normal Operations | ~1.25 GB per minute                         | <code>aws.ec2.network_out</code>      |
| Cell Network Consumption (Network Out) During Upgrade           | ~1.25 GB per minute (no significant change) | <code>aws.ec2.network_out</code>      |
| Cell Network Consumption (Network In) During Normal Operations  | 2.11 GB per minute                          | <code>aws.ec2.network_in</code>       |
| Cell Network Consumption (Network In) During Upgrade            | 16.75GB per minute                          | <code>aws.ec2.network_in</code>       |

## Sample Performance Graphs

These DataDog graphs represent a timeline visualization of read and write operations during the repave event.

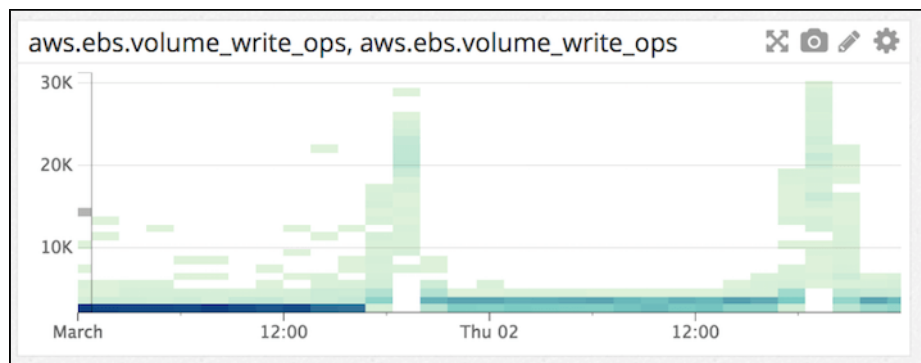
### Read I/O Operations

The read I/O operations sample was taken over 115 VMs and represent the number of read operations over 300 seconds for a single Diego cell.



### Write I/O Operations

The write I/O operations sample was taken over 115 VMs and represent the number of read I/O operations over 300 seconds for a single Diego cell.



## Summary

During the repave process, 250 Diego cells were updated. The repave process took 6 hours overall or about 3 hours for each Availability Zone.





## Upgrading PAS and Other Pivotal Cloud Foundry Products

Page last updated:

This topic describes how to upgrade to a point release of Pivotal Application Service (PAS) and other product tiles without upgrading Ops Manager. For example, use this topic to upgrade from PAS v2.2.0 to v2.2.1. You might need to perform this upgrade if a security update for PAS is released, or if new features are introduced in a point release of a product tile.

For PAS component and version information, see the [PAS release notes](#).

**Note:** If you cannot download products from Pivotal Network due to restricted network connectivity, see [Installing PCF in Airgapped Environments](#).

### Before You Upgrade to Point Releases

- You must have completed the [Upgrading Pivotal Cloud Foundry](#) procedure.
- Refer to the [Product Compatibility Matrix](#) before upgrading PAS.
- Important:** Read the Known Issues sections of the products you plan on installing before starting. See [Pivotal Cloud Foundry Release Notes](#) for all available product release notes.

### Upgrading PAS

**Note:** If you are using the [Pivotal Network API](#), the latest product versions will automatically appear in your **Installation Dashboard**.

To upgrade PAS without upgrading Ops Manager, do the following:

- Download the product file from [Pivotal Network](#).
- Import the product file to your Ops Manager **Installation Dashboard**.
- Click the plus icon next to the uploaded product description to add this product to your staging area.
- Click the newly added tile to review any configurable options.
- Click **Apply Changes** to install the service.

### Upgrading PCF Products

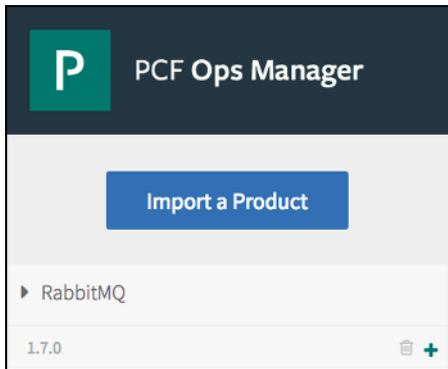
**Note:** If you are using the [Pivotal Network API](#), the latest product versions will automatically appear in your **Installation Dashboard**.

This section describes how to upgrade individual products like [Single Sign-On for PCF](#), [MySQL for PCF](#), [RabbitMQ® for PCF](#), and [Metrics for PCF](#) in your Pivotal Cloud Foundry (PCF) deployment. Ensure you review the individual product upgrade procedure for each tile.

- Browse to [Pivotal Network](#) and sign in.
- Download the latest PCF release for the product or products you want to upgrade. Every product is tied to exactly one stemcell. Download the stemcell that matches your product and version.
- Confirm that you have adequate disk space for your upgrades. You need at least 20 GB of free disk space to upgrade PCF Ops Manager and Pivotal Application Service. If you plan to upgrade other products, the amount of disk space required depends on how many tiles you plan to deploy to your upgraded PCF deployment.

To check current persistent disk usage, select the **BOSH Director** tile from the **Installation Dashboard**. Select **Status** and review the value of the **PERS. DISK** column. If persistent disk usage is higher than 50%, select **Settings > Resource Config**, and increase your persistent disk space to handle the size of the resources. If you do not know how much disk space to allocate, set the value to at least **100 GB**.

- Browse to the Pivotal Cloud Foundry Ops Manager web interface and click **Import a Product**.



5. Select the `.pivotal` file that you downloaded from Pivotal Network or received from your software distributor, then click **Open**. If the product is successfully added, it appears in your product list. If the product you selected is not the latest version, the most up-to-date version will appear on your product list.
6. Click the plus icon next to the product description to add the product tile to the **Installation Dashboard**.
7. Repeat the import, upload, and upgrade steps for each product you downloaded.
8. If you are upgrading a product that uses a self-signed certificate from v1.1 to v1.2, you must configure the product to trust the self-signed certificate. To configure a product to trust the self-signed certificate, do the following:
  - a. Click the product tile.
  - b. In the left-hand column, select the setting page containing the SSL certificate configuration. For example, for PAS, select the **HAProxy** page.
  - c. Check the **Trust Self-Signed Certificates** box.
  - d. Click **Save**.
9. Click **Apply Changes**.

## Upgrading Replicated Tiles

To upgrade a replicated tile, you must do the following:

- Generate a replica of the newer version of the tile using the replicator
- Give the new replica the same name as the existing replica.

See the following example workflow.

### Example Workflow

This example assumes the following:

- You used the replicator to generate a replica of v1 of the Isolation Segments tile.
- You used the `name` **seg-one**.
- You installed the tile in Ops Manager.

Here is the sample replicator command you used for the initial installation:

```
./replicator-darwin\
--name seg-one\
--path /download/p-isolation-segment-v1.pivotal\
--output /output/p-isolation-segment-v1-seg-one.pivotal
```

To upgrade to v2, follow these steps:

1. Download and unzip the new Isolation Segment Tile Replicator from [Pivotal Network](#). You must download the version of Tile Replicator that corresponds with the version of the Isolation Segment Tile you want to replicate.
2. Run the replicator command below to create the replica:

```
./replicator-darwin\
--name NAME-OF-EXISTING-REPLICA \
--path PATH-TO-NEW-TILE \
--output /output/p-isolation-segment-v2-seg-one.pivotal
```

Where:

- `NAME-OF-EXISTING-REPLICA` must be the same as the name used for the existing replica. This is **seg-one** in this example.
- `PATH-TO-NEW-TILE` is the path to the new Isolation Segment Tile.

3. After you have the replica tile **p-isolation-segment-v2-seg-one.pivotal**, upload it to Ops Manager. This upgrades the v1 replica tile in place.

## cf push Availability During Pivotal Application Service Upgrades

Page last updated:

This topic describes what you can expect regarding the availability of `cf push` during upgrades of Pivotal Application Service (PAS).

### Overview

Availability of `cf push` during PAS upgrades varies from release to release. There are various considerations, such as Cloud Controller database (CCDB) migrations or the number of VMs in use, that can impact `cf push` availability. However, `cf push` is mostly available for the duration of an upgrade.

### Impact on Single VMs vs. High-Availability Infrastructure

Having a single VM in use, such as a WebDAV, a HAProxy, a Gorouter, a UAA, or a Cloud Controller, impacts whether `cf push` is unavailable during an upgrade.

If you have scaled out your application to achieve high availability and are not using WebDAV, `cf push` should be available for the entire duration of the upgrade. However, upgrades to certain versions of PAS sometimes require a CCDB schema or data migration, which may cause `cf push` to be unavailable while Cloud Controllers are rolling during the upgrade.

### Availability During a BBR Backup

The Cloud Controller API is taken down during the `pre-backup-lock` stage of a BBR backup and put back up again during the `post-backup-unlock` stage. As a result, `cf push` becomes unavailable during that time. However, the backup that takes place between those stages is very short, no longer than a few minutes. The bulk of the BBR backup operation happens after the `post-backup-unlock` stage, so the Cloud Controller API and `cf push` are available for most of the duration of a BBR backup.

The [Uptimer](#) [↗](#) tool can help you measure `cf push` availability during an upgrade.

## PCF Dev Overview

Page last updated:

This guide describes how to install and use PCF Dev, a fully featured Pivotal Cloud Foundry (PCF) installation that runs on your workstation's native hypervisor.

PCF Dev enables application developers to test and debug their app on a local PCF deployment, and enables operators to test out features of PCF in their local environment.

PCF Dev includes Pivotal Application Service (PAS), Spring Cloud Services, Redis, RabbitMQ, and MySQL. It also supports all Cloud Foundry Command Line Interface (cf CLI) functionality. See the [Comparing PCF Dev to Pivotal Cloud Foundry](#) table below for more product details.

## Prerequisites

Before you can install PCF Dev, you must have the following:

- The latest version of the [cf CLI](#): Use the cf CLI to push and scale apps.
- You must have an Internet connection for DNS.
- At least 8 GB of available memory on your host machine. Pivotal recommends running on a host system with at least 16 GB of total RAM.
- Virtualization permissions.

## Installing PCF Dev

- [Installing PCF Dev on Mac OS X](#)
- [Installing PCF Dev on Microsoft Windows](#)
- [Installing PCF Dev on Linux](#)

## Configuring and Using PCF Dev

- [Configuring PCF Dev](#)
- [Using PCF Dev](#)
- [Using Services in PCF Dev](#)
- [Using Spring Cloud Services in PCF Dev](#)
- [Using PCF Dev Behind a Proxy](#)
- [Using PCF Dev Offline](#)
- [Using a Local OVA with PCF Dev](#)
- [PCF Dev on AWS](#)
- [Telemetry](#)
- [Frequently Asked Questions](#)

## Comparing PCF Dev to Pivotal Cloud Foundry

PCF Dev mirrors [PCF](#) in its key product offerings. If an application runs on PCF Dev, it runs on PCF with no modification in almost all cases. Review the table below for key product details.

|                          | PCF Dev                   | PCF         | CF                           |
|--------------------------|---------------------------|-------------|------------------------------|
| Space required           | 100 GB                    | 100GB+      | 50GB+                        |
| Memory required          | 8 GB                      | 50GB+       | variable                     |
| Deployment               | <code>cf dev start</code> | Ops Manager | <code>bosh create-env</code> |
| Estimated time-to-deploy | 30 Minutes                | Hour+       | Hour+                        |

|                                                                            | Pivotal<br>CF Dev                 | Pivotal<br>CF                | CF  |
|----------------------------------------------------------------------------|-----------------------------------|------------------------------|-----|
| Out-of-the-Box Services                                                    | MySQL<br>RabbitMQ<br>Spring Cloud | MySQL<br>RabbitMQ<br>GemFire | N/A |
| PAS                                                                        | ✓                                 | ✓                            | ✓   |
| Logging/Metrics                                                            | ✓                                 | ✓                            | ✓   |
| Routing                                                                    | ✓                                 | ✓                            | ✓   |
| Compatible with CF CLI                                                     | ✓                                 | ✓                            | ✓   |
| Deploy apps with any supported buildpack                                   | ✓                                 | ✓                            | ✓   |
| Supports Multi-Tenancy                                                     | ✓                                 | ✓                            | ✓   |
| Diego Support                                                              | ✓                                 | ✓                            | ✓   |
| Docker Support                                                             | ✓                                 | ✓                            | ✓   |
| User-Provided Services                                                     | ✓                                 | ✓                            | ✓   |
| High Availability                                                          |                                   | ✓                            | ✓   |
| Integration with 3rd party Authorization                                   |                                   | ✓                            | ✓   |
| BOSH Director<br>(i.e., can perform additional BOSH deployments)           | ✓                                 | ✓                            | ✓   |
| Day Two Lifecycle Operations<br>(e.g., rolling upgrades, security patches) |                                   | ✓                            | ✓   |
| Ops Manager                                                                |                                   | ✓                            |     |
| Apps Manager                                                               | ✓                                 | ✓                            |     |
| Tile Support                                                               |                                   | ✓                            |     |
| Developers have root-level access across cluster                           | ✓                                 |                              |     |
| Pre-provisioned                                                            | ✓                                 |                              |     |

## Backing Up and Restoring Pivotal Cloud Foundry

Page last updated:

Consider the following when backing up data in your Pivotal Cloud Foundry (PCF) deployment:

- If your deployment uses external databases, check that it is a [supported database configuration](#).
- If your PCF deployment uses internal databases, follow the backup and restore instructions for the MySQL server included in the [BBR](#) documentation.

### General Data Protection Regulation

The General Data Protection Regulation (GDPR) came into effect on May 25, 2018 and impacts any company processing the data of EU citizens or residents, even if the company is not EU-based. The GDPR sets forth how companies should handle privacy issues, securely store data, and respond to security breaches.

Backup artifacts may contain personal data covered by GDPR. For example, a backup of a PAS could contain a user email. For further information regarding personal data that may be stored in PCF, see [here](#).

## Backup and Restore with BBR

BOSH Backup and Restore (BBR) is a command-line tool for backing up and restoring BOSH deployments.

To perform a backup of your PCF deployment with BBR, see [Backing Up Pivotal Cloud Foundry with BBR](#).

To restore your PCF deployment with BBR, see [Restoring Pivotal Cloud Foundry from Backup with BBR](#).

To use BBR to back up and restore your PCF deployment, you must first set up a jumpbox to run BBR from. See [Setting Up Your Jumpbox for BBR](#).

To troubleshoot problems with BBR, see [Troubleshooting BBR](#).



## Disaster Recovery in Pivotal Cloud Foundry

This document provides an overview of the options and considerations for disaster recovery in Pivotal Cloud Foundry (PCF).

Operators have a range of approaches for ensuring they can recover Pivotal Cloud Foundry, apps, and data in case of a disaster. The approaches fall into the following two categories:

- Using data from a backup to restore the data in the PCF Deployment. See [Back up and Restore Using BOSH Backup and Restore \(BBR\)](#) for more information.
- Recreating the data in PCF by automating the creation of state in PCF. See [Disaster Recovery by Recreating the Deployment](#) for more information.

## Back up and Restore using BOSH Backup and Restore (BBR)

### What is BBR?

BOSH Backup and Restore (BBR) is a CLI for orchestrating backing up and restoring BOSH deployments and BOSH Directors. BBR triggers the backup or restore process on the deployment or Director, and transfers the backup artifact to and from the deployment or Director.

Use BOSH Backup and Restore to reliably create backups of core PCF components and their data. These core components include CredHub, UAA, BOSH Director, and PAS.

Each component includes its own backup scripts. This decentralized structure helps keep scripts synchronized with the components. At the same time, *locking* features ensure data integrity and consistent, distributed backups across your deployment.

For more information about the BBR framework, see [BOSH Backup and Restore](#) in the open source Cloud Foundry documentation.

### Backing up PCF

Backing up PCF requires backing up the following components:

- Ops Manager settings
- BOSH Director, including CredHub and UAA
- Pivotal Application Service
- Data services

For more information, see [Backing up Pivotal Cloud Foundry with BBR](#). With these backup artifacts, operators can recreate PCF exactly as it was when the backup was taken.

### Restoring PCF

The restore process involves creating a new PCF deployment starting with the Ops Manager VM. For more information, see [Restoring Pivotal Cloud Foundry from Backup with BBR](#).

The time required to restore the data is proportionate to the size of the data because the restore process includes copying data. For example, restoring a 1 TB blobstore takes one thousand times as long as restoring a 1 GB blobstore.

### Benefits

Unlike other backup solutions, using BBR to back up PCF enables the following:

- **Completeness:** BBR supports backing up BOSH, including releases, CredHub, UAA, and service instances created with an on-demand service broker. With PCF v1.12, Ops Manager export no longer includes releases.
- **Consistency:** BBR provides referential integrity between the database and the blobstore because a lock is held while both the database and blobstore are backed up.
- **Correctness:** Using the BBR restore flow addresses C2C and routing issues that can occur during restore.

## API Downtime During Backups

Apps are not affected during backups, but certain APIs are unavailable. The downtime occurs only while the backup is being taken, not while the backup is being copied to the jumpbox.

In a consistent backup, the blobs in the blobstore match the blobs in the Cloud Controller Database. To take a consistent backup, changes to the data are prevented during the backup. This means that the CF API, Routing API, Usage Service, Autoscaler, Notification Service, Network Policy Server, and CredHub are unavailable while the backup is being taken. UAA is in read-only mode during the backup.

## Backup Timings

The first three phases of the backup are lock, backup, and unlock. During this time, the API is unavailable. The drain and checksum phase starts once the backup scripts finish. BBR downloads the backup artifacts from the instances to the BBR VM, and performs a checksum to ensure the artifacts are not corrupt. The size of the blobstore significantly influences backup time.

The table below gives an indication of the downtime that you can expect. Actual downtime varies based on hardware and PCF configuration. These example timings were recorded with Pivotal Application Service (PAS) deployed on Google Cloud Platform (GCP) with all components scaled to one and only one app pushed.

| <i>Backup Timings</i> |                     |                                                                |                                                                  |                                        |
|-----------------------|---------------------|----------------------------------------------------------------|------------------------------------------------------------------|----------------------------------------|
| <i>API State</i>      | <i>Backup phase</i> | <i>Duration for External Versioned S3-Compatible Blobstore</i> | <i>Duration for External Unversioned S3-Compatible Blobstore</i> | <i>Duration for Internal Blobstore</i> |
| API unavailable       | lock                | 15 seconds                                                     | 15 seconds                                                       | 15 seconds                             |
|                       | backup              | <30 seconds                                                    | Proportional to blobstore size                                   | 10 seconds                             |
|                       | unlock              | 3 minutes                                                      | 3 minutes                                                        | 3 minutes                              |
| API available         | drain and checksum  | <10 seconds                                                    | <10 seconds                                                      | Proportional to blobstore size         |

## Blobstore backup and restore

Blobstores can be very large. To minimize downtime, BBR only takes blob metadata during the backup. For example, in the case of internal blobstores (Webdav/NFS), BBR takes a list of hardlinks that point to the blobs. Once the API becomes available, BBR makes copies of the blobs.

## Unsupported Products

- **Data services.** The Pivotal data services listed below do not support BBR. Operators of these services should use the automatic backups feature of each tile, available within Ops Manager.
  - MySQL for PCF
  - Pivotal Cloud Cache for PCF
  - RabbitMQ for PCF
  - Redis for PCF
- **External blobstores and databases.** BBR support for backing up and restoring external databases and blobstores varies across PCF versions. For more information, see [Supported Components](#) and [External Storage Support Across PCF Versions](#) in *Backing up Pivotal Cloud Foundry with BBR*.

## Best Practices

### Frequency of Backups

Pivotal recommends that you take backups in proportion to the rate of change of the data in PCF to minimize the number of changes lost if a restore is required. We suggest starting with backing up every 24 hours. If app developers make frequent changes, you should increase the frequency of backups.

### Retention of Backup Artifacts

Operators should retain backup artifacts based on the timeframe they need to be able to restore to. For example, if backups are taken every 24 hours and

PCF must be able to be restored to three days prior, three sets of backup artifacts should be retained.

Artifacts should be stored in two data centers other than the PCF data center. When deciding the restore timeframe, you should take other factors such as compliance and auditability into account.

## Security

Pivotal strongly recommends that you encrypt artifacts and stored them securely.

## Disaster Recovery by Recreating the Deployment

An alternative strategy for recovering PCF after a disaster is to have automation in place so that all the data can be recreated. This requires that every modification to PCF settings and state be automated, typically through use of a pipeline.

Recovery steps include creating a new PCF, recreating orgs, spaces, users, services, service bindings and other state, and re-pushing apps.

For more information about this approach, see the following Cloud Foundry Summit presentation: [Multi-DC Cloud Foundry: What, Why and How? ↗](#).

## Disaster Recovery for Different Topologies

### Active-Active

To prevent app downtime, some Pivotal customers run active-active, where they run two or more identical PCF deployments in different data centers. If one PCF deployment becomes unavailable, traffic is seamlessly routed to the other deployment. To achieve identical deployments, all operations to PCF are automated so they can be applied to both PCF deployments in parallel.

Because all operations have been automated, the automation approach to disaster recovery is a viable option for active-active. Disaster recovery requires recreating PCF, then running all the automation to recreate state.

This option requires discipline to automate all changes to PCF. Some of the operations that need to be automated are the following:

- App push, restage, scale
- Org, space, and user create, read, update, and delete (CRUD)
- Service instance CRUD
- Service bindings CRUD
- Routes CRUD
- Security groups CRUD
- Quota CRUD

Human-initiated changes always make their way into the system. These changes can include quotas being raised, new settings being enabled, and incident responses. For this reason, Pivotal recommends taking backups even when using an automated disaster recovery strategy.

### Using BBR Backup and Restore versus Recreating a Failed PCF Deployment in Active-Active

| Disaster Recovery             |                                                                                                                                                                 |                                                                                                                                                                                                                           |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | Restore the PCF Data                                                                                                                                            | Recreate the PCF Data                                                                                                                                                                                                     |
| Preconditions                 | IaaS prepared for PCF install                                                                                                                                   | IaaS prepared for PCF install                                                                                                                                                                                             |
| Steps                         | <ol style="list-style-type: none"> <li>1. Recreate PCF</li> <li>2. Restore</li> <li>3. Apply changes to make restored PCF match the other active PCF</li> </ol> | <ol style="list-style-type: none"> <li>1. Recreate PCF</li> <li>2. Trigger automation to recreate orgs, spaces, etc.</li> <li>3. Notify app developers to repush apps, recreate service instances and bindings</li> </ol> |
| RTO (Recovery Time Objective) |                                                                                                                                                                 |                                                                                                                                                                                                                           |
|                               |                                                                                                                                                                 |                                                                                                                                                                                                                           |

|                                       |                         |                                                                          |
|---------------------------------------|-------------------------|--------------------------------------------------------------------------|
| <b>Platform</b>                       | Time to recreate PCF    | Time to recreate PCF                                                     |
| <b>Apps</b>                           | Time to restore         | Time until orgs/spaces/etc have been recreated + apps have been repushed |
| <b>RPO (Recovery Point Objective)</b> |                         |                                                                          |
| <b>Platform</b>                       | Time of the last backup | Current time                                                             |
| <b>Apps</b>                           | Time of the last backup | Current time                                                             |

## Active-Passive

Instead of having a true active-active deployment across all layers, some Pivotal customers prefer to install a PCF or PAS deployment on a backup site. The backup site resides on-premises, in a co-location facility, or the public cloud. The backup site includes an operational deployment, with only the most critical apps ready to accept traffic should a failure occur in the primary data center. Disaster recovery in this scenario involves the following:

1. Switching traffic to the passive PCF, making it active.
2. Recovering the formerly-active PCF. Operators can choose to do this through automation, if that option is available, or by using BBR and the restore process.

The RTO and RPO for recreating the active PCF are the same as outlined in the table above.

## Reducing RTO

Both the restore and recreate data disaster recovery options require standing up a new PCF, which can take hours. If you require shorter RTO, several options involving a pre-created standby hardware and PCF are available:

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Active-cold</b>             | Public cloud environment ready for PCF installation, no PCF installed. This saves both IaaS costs and PCF instance costs. For on-prem installations, this requires hardware on standby, ready to install on, which may not be a realistic option.                                                                                                                                                                                                                                                                                                                          |
| <b>Active-warm</b>             | PCF installed on standby hardware and kept up to date, VMs scaled down to zero (spin them up each time there is a platform update), no apps installed, no orgs or spaces defined.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Active-inflate platform</b> | Bare minimum PCF install, either with no applications, or a small number of each app in a stopped state. On recovery, push a small number of apps or start current apps, while simultaneously triggering automation to scale the platform to the primary node size, or a smaller version if large percentages of loss are acceptable. This mode allows you to start sending some traffic immediately, while not paying for a full non-primary platform. This method requires data seeded, but it is usually acceptable to complete data sync while platform is scaling up. |
| <b>Active-inflate apps</b>     | Non-primary deployment scaled to the primary node size, or smaller version if large percentages of loss are acceptable, with a small number of Diego cells (VMs). On failover, scale Diego cells up to primary node counts. This mode allows you to start sending most traffic immediately, while not paying for all the AIs of a fully fledged node. This method requires data to be there very quickly after failure. It does not require real-time sync, but near-real time.                                                                                            |

There is a tradeoff between cost and RTO: the less the replacement PCF needs to be deployed and scaled, the faster the restore.

## Automating Backups

BBR generates the backup artifacts required for PCF, but does not handle scheduling, artifact management, or encryption. The BBR team has created a [starter Concourse pipeline](#) to automate backups with BBR.

Also, Stark & Wayne's Shield can be used as a front end management tool using the BBR plugin.

## Validating Backups

To ensure that backup artifacts are valid, the BBR tool creates checksums of the generated backup artifacts, and ensures that the checksums match the

artifacts on the jumpbox.

However, the only way to be sure that the backup artifact can be used to successfully recreate PCF is to test it in the restore process. This is a cumbersome, dangerous process so should be done with care. For instructions, see [Step 11: \(Optional\) Validate Your Backup](#) of the *Backing Up Pivotal Cloud Foundry with BBR*.

## Backing Up Pivotal Cloud Foundry with BBR

Page last updated:

This topic describes the procedure for backing up your critical backend Pivotal Cloud Foundry (PCF) components with BOSH Backup and Restore (BBR), a command-line tool for backing up and restoring BOSH deployments. To restore your backup, see the [Restoring Pivotal Cloud Foundry from Backup with BBR](#) topic.

To view the BBR release notes, see the [Cloud Foundry documentation](#).

During the backup, BBR stops the Cloud Controller API and the Cloud Controller workers to create a consistent backup. Only the API functionality, like pushing applications or using the Cloud Foundry Command Line Interface (cf CLI) are affected. The deployed applications do not experience downtime.

### warning

- **Security:** Backup artifacts can contain secrets. Secure backup artifacts by using encryption or other means.
- **Compatibility:** A BBR backup can only be restored to environments matching its source environment. To ensure that a restore environment is compatible with a backup see [Compatibility of Restore](#).
- **Failed Restore:** Restore is a destructive operation. BBR is designed to restore PCF after a disaster. If a restore fails, the environment might be left in an unusable state and require re-provisioning. For more information, see [Restoring Pivotal Cloud Foundry from Backup with BBR](#).
- **Service Data:** BBR does not back up any service data.
- **API Outage:** The Cloud Controller API does not send or receive calls during PCF restoration.

## Recommendations

Pivotal recommends the following:

- Follow the full procedure documented in this topic when creating a backup. This ensures that you always have a consistent backup of Ops Manager and PAS to restore from.
- Back up frequently, especially before making any changes to your PCF deployment, such as the configuration of any tiles in Ops Manager.

## Supported Components

BBR is a binary that can back up and restore BOSH deployments and BOSH Directors. BBR requires that the backup targets supply scripts that implement the backup and restore functions. BBR can communicate securely with external blobstores and databases, using TLS, if these are configured accordingly.


BBR can back up the following components:

- [Pivotal Application Service \(PAS\)](#)
- [BOSH Director](#)

### PAS

In PCF v2.2, BBR can back up and restore PAS configured with the following:


- An internal MySQL database or a supported external database. For a list of supported external databases, see the [Supported External Databases](#) section of *Configuring Cloud Foundry for BOSH Backup and Restore* in the Cloud Foundry documentation.
- An internal WebDAV/NFS blobstore, an external Amazon S3 or S3-compatible blobstore, or an external Azure blobstore.

 **Note:** In PAS v2.2, BBR supports backing up and restoring versioned and unversioned S3 or S3-compatible blobstores by default. To back up and restore Azure blobstores with BBR, you must install Blobstore Addon. For more information, see [Enabling External Blobstore Backups](#).

For guidance about backing up unsupported databases and blobstores, see [Unsupported External Blobstores and Databases in PAS](#) below.

### BOSH Director

The BOSH Director must have an internal PostgreSQL database and an internal blobstore to be backed up and restored with BBR. As part of backing up the BOSH Director, BBR backs up the BOSH UAA database and the CredHub database.

 **Note:** BBR support for backing up and restoring external databases and blobstores varies across PCF versions. For more information, see [External Storage Support Across PCF Versions](#) below.

## External Storage Support Across PCF Versions

The following table shows what types of external databases and blobstores you can back up and restore with BBR.


| Deployment Type | Ops Manager Version                        |        |     |     |
|-----------------|--------------------------------------------|--------|-----|-----|
|                 | PAS with External Database                 | Yes    | Yes | Yes |
|                 | BOSH Director with External Database       | No     | Yes | Yes |
|                 | PAS with Amazon S3 Blobstore*              | Yes    | Yes | Yes |
|                 | BOSH Director with Amazon S3 Blobstore*    | No     | No  | No  |
|                 | PAS with S3-Compatible Blobstore           | Yes    | Yes | Yes |
|                 | BOSH Director with S3-Compatible Blobstore | No     | No  | No  |
|                 | PAS with Azure Blobstore                   | Add-on | Yes | Yes |
|                 | PAS with GCS Blobstore                     | No     | No  | No  |
|                 | BOSH Director with GCS Blobstore           | No     | No  | No  |

\* Any S3 clone that supports the versioning API.


## Unsupported External Blobstores and Databases in PAS

If you configured an unsupported external blobstore or an unsupported external database in PAS, see the following guidelines to perform a backup successfully:

| Scenario                                                                                           | Action                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You configured a supported database and an unsupported external blobstore in PAS.                  | Follow the PCF backup process and copy the external blobstore by using the IaaS-specific tool.                                                                                  |
| You configured an unsupported external database and a supported blobstore in PAS.                  | Follow the PCF backup process and copy the external database by using the IaaS-specific tool.                                                                                   |
| You configured both an unsupported external database and an unsupported external blobstore in PAS. | Follow the PCF backup process but skip the <a href="#">Back Up Your PAS Deployment</a> section below. Copy the external database and blobstore by using the IaaS-specific tool. |

 **warning:** You might encounter inconsistencies between the blobstore and database. If apps do not appear during a restore, re-push those apps.

## Backing Up Services

 **warning:** BBR does not currently back up any service data.

Keep in mind the following when backing up services:

- BBR backs up and restores the service bindings, but not the service data.
- You can redeploy on-demand service instances manually during restore, but the data in the instance is not backed up.
- BBR does not back up managed services or their data.
- You can back up and restore brokered services with the procedures documented in this topic and in the [Restoring Pivotal Cloud Foundry from Backup with BBR](#) topic.

## Backup Workflow

To install BBR, you download the `bbr` executable and copy it to a jumpbox. Once installed on your jumpbox, you can run BBR commands, specifying the name of the BOSH deployment.

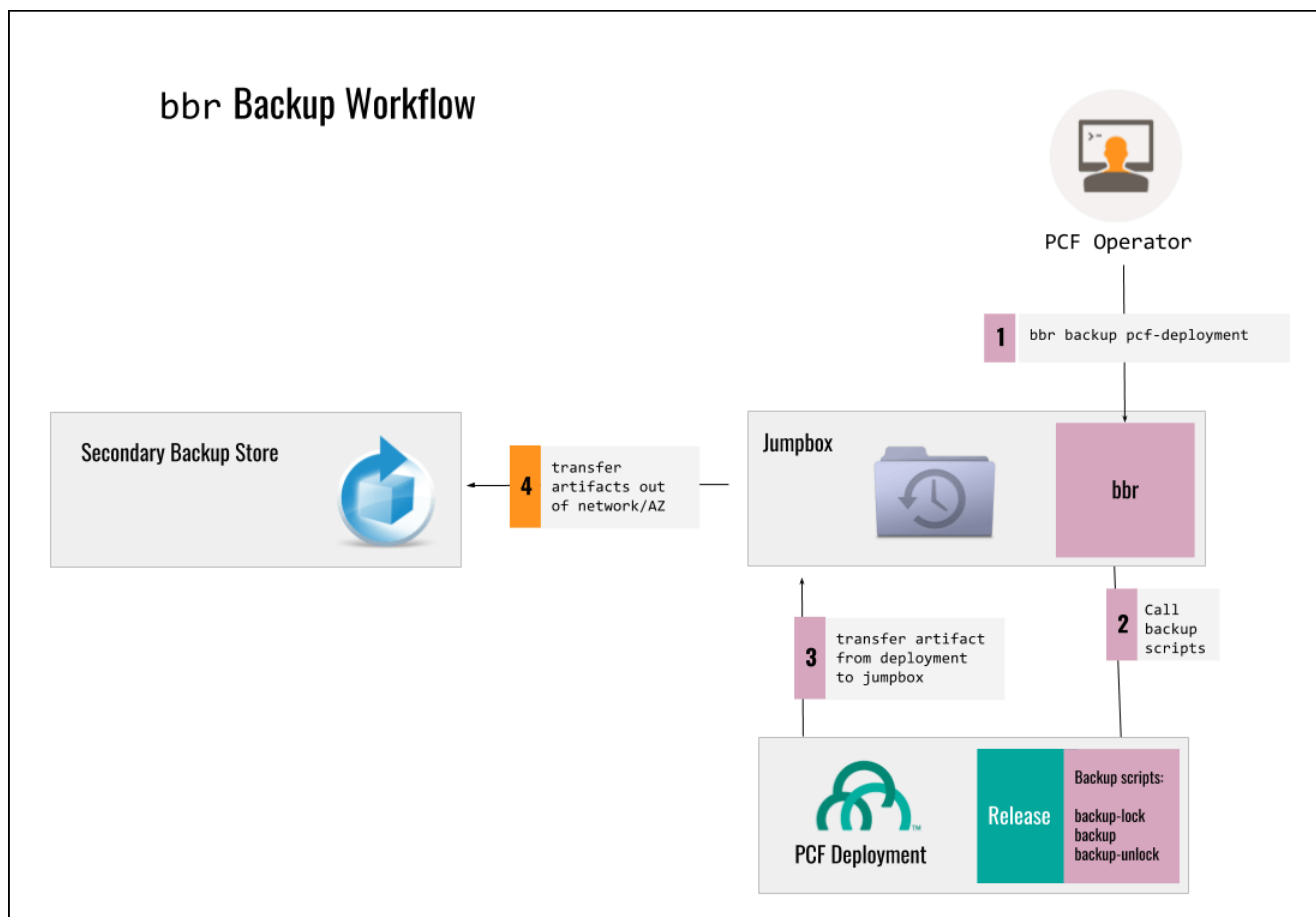
BBR examines the jobs in the BOSH deployment, and triggers the scripts in the following stages:

1. **Pre-backup lock:** The pre-backup lock scripts locks the job so backups are consistent across the cluster.
2. **Backup:** The backup script backs up the release.
3. **Post-backup unlock:** The post-backup unlock script unlocks the job after the backup is complete.

Scripts in the same stage are all triggered together. For instance, BBR triggers all pre-backup lock scripts before any backup scripts. Scripts within a stage can be triggered in any order.

The backup artifacts are drained to the jumpbox, where the operator can transfer them to storage and use them to restore PCF.

The following diagram shows a sample backup flow.



## Preparing to Create Your Backup

### Step 1: Set Up Your Jumpbox

You must have a jumpbox before you can install BBR to the jumpbox. A jumpbox is a separate, hardened server on your network that provides a controlled means of access to the VMs other computers on your network. Pivotal recommends using the Ops Manager VM as your jumpbox.



Pivotal recommends using the Ops Manager VM as your jumpbox. If you use the Ops Manager VM as your jumpbox, the path to the root Certificate Authority (CA) certificate is:



```
/var/tempest/workspaces/default/root_ca_certificate
```


You must have this path to run BBR commands.

Prepare your jumpbox for BBR by following the steps in [Setting Up Your Jumpbox for BBR](#).

 **Note:** Pivotal recommends that you regularly update the BBR binary on your jumpbox to the latest version. See [Transfer BBR Binary to Your Jumpbox](#) in *Setting Up Your Jumpbox for BBR* for more information. See the [jumpbox-deployment](#)  GitHub repository for an example jumpbox deployment.

## Step 2: Record the Cloud Controller Database Encryption Credentials

Perform the following steps to retrieve the Cloud Controller database encryption credentials from the PAS tile:

1. Navigate to Ops Manager in a browser and log in to the Ops Manager Installation Dashboard.
2. Select PAS **Credentials** and locate the Cloud Controller section.
3. Record the **Db Encryption Credentials**. You must provide these credentials when you contact [Pivotal Support](#)  for help restoring your installation.

|                  |                           |                                    |
|------------------|---------------------------|------------------------------------|
| Cloud Controller | VM Credentials            | <a href="#">Link to Credential</a> |
|                  | Db Encryption Credentials | <a href="#">Link to Credential</a> |
|                  | Encrypt Key               | <a href="#">Link to Credential</a> |
|                  | Locket Client Cert        | <a href="#">Link to Credential</a> |

## Step 3: Retrieve BOSH Director Credentials

To use BBR, you must retrieve and record the following credentials:

- Bosh Director Credentials
- Bbr Ssh Credentials
- Uaa Bbr Client Credentials

There are two ways to retrieve BOSH Director credentials:

- Ops Manager Installation Dashboard
- Ops Manager API

### Option 1: Ops Manager Installation Dashboard

To retrieve your BOSH Director credentials using the Ops Manager Installation Dashboard, perform the following steps:

1. Navigate to the Ops Manager Installation Dashboard.
2. Click the BOSH Director tile.
3. Click the **Credentials** tab.

| BOSH Director                                                |                              |                                    |
|--------------------------------------------------------------|------------------------------|------------------------------------|
| <div>Settings</div> <div>Status</div> <div>Credentials</div> |                              |                                    |
| JOB                                                          | NAME                         | CREDENTIALS                        |
| BOSH Director                                                | Vm Credentials               | <a href="#">Link to Credential</a> |
|                                                              | Agent Credentials            | <a href="#">Link to Credential</a> |
|                                                              | Registry Credentials         | <a href="#">Link to Credential</a> |
|                                                              | Director Credentials         | <a href="#">Link to Credential</a> |
|                                                              | Postgres Credentials         | <a href="#">Link to Credential</a> |
|                                                              | Blobstore Credentials        | <a href="#">Link to Credential</a> |
|                                                              | Health Monitor Credentials   | <a href="#">Link to Credential</a> |
|                                                              | Uaa Admin User Credentials   | <a href="#">Link to Credential</a> |
|                                                              | Uaa Login Client Credentials | <a href="#">Link to Credential</a> |
|                                                              | Uaa Jwt Key                  | <a href="#">Link to Credential</a> |
|                                                              | Bbr Ssh Credentials          | <a href="#">Link to Credential</a> |
|                                                              | Uaa Bbr Client Credentials   | <a href="#">Link to Credential</a> |
|                                                              | Bosh Commandline Credentials | <a href="#">Link to Credential</a> |
|                                                              | Blobstore Certificate        | <a href="#">Link to Credential</a> |

#### 4. Locate **Director Credentials**.

- Click **Link to Credentials** next to it.
- Verify the value of the `identity` field. It should be `director`.
- Copy and record the value of the `password` field.

#### 5. Locate **Bbr Ssh Credentials**.

- Click **Link to Credentials** next to it.
- Copy the value of the `private_key_pem` field.
- Run the following command to reformat the copied value, and save it in the current directory to a file named `PRIVATE-KEY-FILE`:

```
printf -- "YOUR-PRIVATE-KEY" > PRIVATE-KEY-FILE
```

Where:

- `YOUR-PRIVATE-KEY` is the text of your private key.
- `PRIVATE-KEY-FILE` is the path to the private key file you are creating.

For example:

```
$ printf -- "-----BEGIN RSA PRIVATE KEY----- MIIKeycontents -----END RSA PRIVATE KEY-----" > bbr_key.pem
```

#### 6. Locate the **Uaa Bbr Client Credentials**

- Click **Link to Credentials** next to it.

- b. Verify the value of the `identity` field. It should be `bbr_client`.
- c. Record the value of the `password` field.

## Option 2: Ops Manager API

To retrieve BOSH Director credentials using the Ops Manager API, perform the following steps:

1. Obtain your UAA access token. For more information, see [Access the API](#).
2. Retrieve the **Director Credentials** by performing the following steps:
  - a. Run the following command:

```
curl "https://OPS-MAN-FQDN/api/v0/deployed/director/credentials/director_credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token.

- b. Verify the value of the `identity` field. It should be `director`.
- c. Record the value of the `password` field.

3. Retrieve the **Bbr Ssh Credentials** by performing the following steps:

- a. Run the following command:

```
curl "https://OPS-MAN-FQDN/api/v0/deployed/director/credentials/bbr_ssh_credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token.

- b. Copy the value of the `private_key_pem` field.
- c. Run the following command to reformat the copied value, and save it in the current directory to a file named `PRIVATE-KEY-FILE`:

```
printf -- "YOUR-PRIVATE-KEY" > PRIVATE-KEY-FILE
```

Where:

- `YOUR-PRIVATE-KEY` is the text of your private key.
- `PRIVATE-KEY-FILE` is the path to the private key file you are creating.

For example:

```
$ printf -- "-----BEGIN RSA PRIVATE KEY----- MIIEkeycontents -----END RSA PRIVATE KEY-----" > bbr_key.pem
```

4. Retrieve the **Uaa Bbr Client Credentials** by performing the following steps:

- a. Run the following command:

```
curl "https://OPS-MAN-FQDN/api/v0/deployed/director/credentials/uaa_bbr_client_credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token.

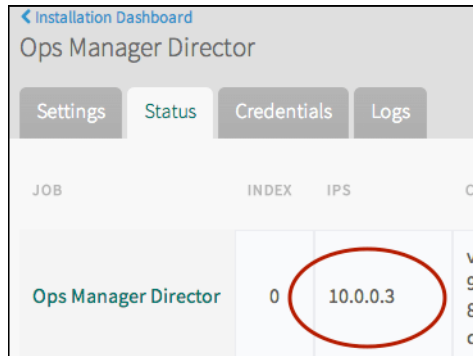
- b. Verify the value of the `identity` field. It should be `bbr_client`.
- c. Record the value of the `password` field.

For more information about using the Ops Manager API, see the [Using the Ops Manager API](#) topic.

## Step 4: Retrieve BOSH Director Address

Perform the following steps to retrieve the IP address of your BOSH Director from the BOSH Director tile:

1. If you are not using the Ops Manager VM as your jumpbox, install the latest [BOSH CLI](#) on your jumpbox.
2. From the Installation Dashboard in Ops Manager, select **BOSH Director** > **Status** and record the IP address listed for the Director. You access the



| JOB                  | INDEX | IPS      | CI                |
|----------------------|-------|----------|-------------------|
| Ops Manager Director | 0     | 10.0.0.3 | vr<br>9<br>8<br>d |

BOSH Director using this IP address.

3. From the command line, log into the BOSH Director, using the IP address that you recorded above, by running the following command:

```
bosh -e DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE log-in
```

Where:

- `DIRECTOR-IP` is the BOSH Director IP address recorded above.
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the root Certificate Authority (CA) certificate as outlined in [Step 1: Set Up your Jumpbox](#), above.

4. When prompted for **Email ()**, specify `director`.
5. When prompted for **Password ()**, enter the **Director Credentials** that you obtained in [Retrieve BOSH Director Credentials](#).  
For example:

```
$ bosh -e 10.0.0.3 \
--ca-cert /var/tempest/workspaces/default/root_ca_certificate log-in
Email (): director
Password (): *****
Successfully authenticated with UAA
Succeeded
```

## Step 5: Check Your BOSH Director

Perform the following steps to confirm that your BOSH Director is reachable and can be backed up.

### Connect to Your Jumpbox

You can establish a connection to your jumpbox in one of the following ways.

- [Connect with SSH](#)
- [Connect with BOSH\\_ALL\\_PROXY](#)

**Note:** These procedures require you have a jumpbox configured for SSH access. If you do not have a jumpbox, see [Enabling SSH Access](#) and [Tunneling](#) in the BOSH documentation.

For general information about the jumpbox, see [Setting Up Your Jumpbox for BBR](#).

### Connect with SSH


There are two options available to you to connect to your jumpbox with SSH:

- Ops Manager VM.
  - SSH through the command line.
1. To connect to your jumpbox through an Ops Manager VM, perform the following steps:
    - a. Log in to the Ops Manager VM:
    - b. If you are using the Ops Manager VM as your jumpbox, see the [Log in to the Ops Manager VM with SSH](#) section of *Advanced Troubleshooting with the BOSH CLI* for information about how to use SSH to connect to the Ops Manager VM.
  2. To connect to your jumpbox through the command line, perform the following steps:
    - a. Run the following command to SSH into your jumpbox:

```
ssh -i LOCAL-PATH-TO-JUMPBOX-PRIVATE-KEY JUMPBOX-USER@JUMPBOX-ADDRESS
```

Where:

- `LOCAL-PATH-TO-JUMPBOX-PRIVATE-KEY` is the local path to your private key file for the jumpbox host.
- `JUMPBOX-USER` is your jumpbox username.
- `JUMPBOX-ADDRESS` is the IP address of your jumpbox.

 **Note:** If you connect to your jumpbox with SSH, you must run the BBR commands in the following sections from within your jumpbox.

## Connect with BOSH\_ALL\_PROXY

Set and use `BOSH_ALL_PROXY`. Using `BOSH_ALL_PROXY` opens an SSH tunnel with SOCKS5 to the jumpbox. This tunnel enables you to forward requests to the BOSH Director through the jumpbox from your local machine.

Use one of the following methods to create the tunnel:

- **Tunnel created by BOSH CLI:** To provide the BOSH CLI with the SSH credentials it needs to create the tunnel, run the following command:

```
export BOSH_ALL_PROXY=ssh+socks5://JUMPBOX@JUMPBOX-IP:SOCKS-PORT?private_key=JUMPBOX-KEY-FILE
```

Where:

- `JUMPBOX` is the name of your jumpbox.
  - `JUMPBOX-IP` is the IP address of the jumpbox.
  - `SOCKS-PORT` is the local SOCKS port.
  - `JUMPBOX-KEY-FILE` is the local SSH private key for accessing the jumpbox.
- **Tunnel established separately:**


1. To establish the tunnel and make it available on a local port, run the following command:


```
ssh -4 -D SOCKS-PORT -fNC JUMPBOX@JUMPBOX-IP -i JUMPBOX-KEY-FILE
```

Where:

- `SOCKS-PORT` is the local SOCKS port.
  - `JUMPBOX` is the name of your jumpbox.
  - `JUMPBOX-IP` is the IP address of the jumpbox.
  - `JUMPBOX-KEY-FILE` is the local SSH private key for accessing the jumpbox.
2. To provide the BOSH CLI with access to the tunnel through use of the `BOSH_ALL_PROXY` environment variable, run the following command:

```
export BOSH_ALL_PROXY=socks5://localhost:SOCKS-PORT
```

 **Note:** Ensure the SOCKS port is not already in use by a different tunnel/process.

 **Note:** Using `BOSH_ALL_PROXY` can result in longer backup and restore times due to network performance degradation. Because all operations must pass through the proxy, moving backup artifacts can be significantly slower.


## Check Your BOSH Director

1. Run the BBR `pre-backup-check` command:

```
bbr director \
--private-key-path PRIVATE-KEY-FILE \
--username bbr \
--host HOST \
pre-backup-check
```

Where:

- `PRIVATE-KEY-FILE` is the path to the private key file that you created from **Bbr Ssh Credentials** in [Step 3: Retrieve BOSH Director Credentials](#).
- `HOST` is the address of the BOSH Director. If the BOSH Director is public, `HOST` is a URL, such as `https://my-bosh.xxx.cf-app.com`. Otherwise, `HOST` is the `BOSH-DIRECTOR-IP` which you retrieved in the [Step 4: Retrieve BOSH Director Address](#) section of this topic above.

 **Note:** Use the optional `--debug` flag to enable debug logs. See the [Logging](#) section below for more information.

2. After the pre-backup check succeeds, continue to [Step 5: Confirm Backup Restore Node is Deployed](#) below.  
If the pre-backup check fails, the BOSH Director might not have the correct backup scripts, or the connection to the BOSH Director might have failed.

## Step 6: Confirm Backup Restore Node is Deployed

When BBR backs up PAS, it needs a Backup Prepare node. This procedure confirms that the Backup Prepare node is deployed.

1. In Ops Manager, open the **Pivotal Application Service** tile.
2. In the **Resource Config** pane find the **Backup Prepare Node** job and check if the **Instances** dropdown is set to `1`.

|                     |                                |                   |                                             |
|---------------------|--------------------------------|-------------------|---------------------------------------------|
| Backup Prepare Node | <input type="text" value="1"/> | Automatic: 200 GB | Automatic: t2.micro (cpu: 1, ram: 1 GB, dis |
|---------------------|--------------------------------|-------------------|---------------------------------------------|

3. If the **Instances** dropdown is not set to `1`:
  - a. Set the **Instances** dropdown to `1`.
  - b. Click **Save**.
  - c. Navigate back to the Installation Dashboard and click **Apply Changes** to redeploy.

## Step 7: Identify Your Deployment

1. Log in to your BOSH Director.
2. To identify the name of the BOSH deployment that contains PCF, run the following command:

```
bosh -e BOSH-DIRECTOR-IP --ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE deployments
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director.

```
$ bosh -e BOSH-DIRECTOR-IP --ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE deployments
```

```
Name Release(s)
cf-example push-apps-manager-release/661.1.24
 cf-backup-and-restore/0.0.1
 binary-buildpack/1.0.11
 capi/1.28.0
 cf-autoscaling/91
 cf-mysql/35
 ...
```

In the above example, the name of the BOSH deployment that contains PCF is `cf-example`.

## Step 8: Check Your Deployment

Perform the following steps to check that your BOSH Director is reachable and has a deployment that can be backed up:

1. Run the BBR pre-backup check:

```
bbr deployment \
--target BOSH-DIRECTOR-IP \
--username BOSH-CLIENT \
--password BOSH-PASSWORD \
--deployment DEPLOYMENT-NAME \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
pre-backup-check
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.
- `BOSH-CLIENT`, `BOSH-PASSWORD` are the **Uaa Bbr Client Credentials**, identity and password, that you retrieved in the [Step 3: Retrieve BOSH Director Credentials](#) section above.
- `DEPLOYMENT-NAME` is the deployment name retrieved in the [Step 6: Identify Your Deployment](#) section above.
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director. For more information, see [Ensure BOSH Director Certificate Availability](#).

2. After the pre-backup check succeeds, continue to [Create Your Backup](#) below.

If the pre-backup check fails, the deployment you selected might not have the correct backup scripts, or the connection to the BOSH Director might have failed.


## Creating Your Backup

### Step 9: Export Installation Settings

Pivotal recommends that you back up your Ops Manager installation settings by exporting frequently.

When exporting your installation settings, keep in mind the following:

- This option is only available after you have deployed at least once.
- Always export your installation settings before following the steps in the [Deploy Ops Manager and Import Installation Settings](#) section of the *Restoring Pivotal Cloud Foundry from Backup with BBR* topic.
- Exporting your installation settings only backs up the settings you configured in Ops Manager. It does not back up your VMs or any external MySQL databases.
- Your Ops Manager settings are encrypted. Make sure you keep track of your Decryption Passphrase because this is needed to restore the Ops Manager settings.

 **Note:** When exporting installation settings for Ops Manager v1.12 and later, releases are not included in the output file. Releases are now included in the BOSH Director backup, therefore, the output file is much smaller than in previous Ops Manager versions.

There are two ways to export Ops Manager installation settings:

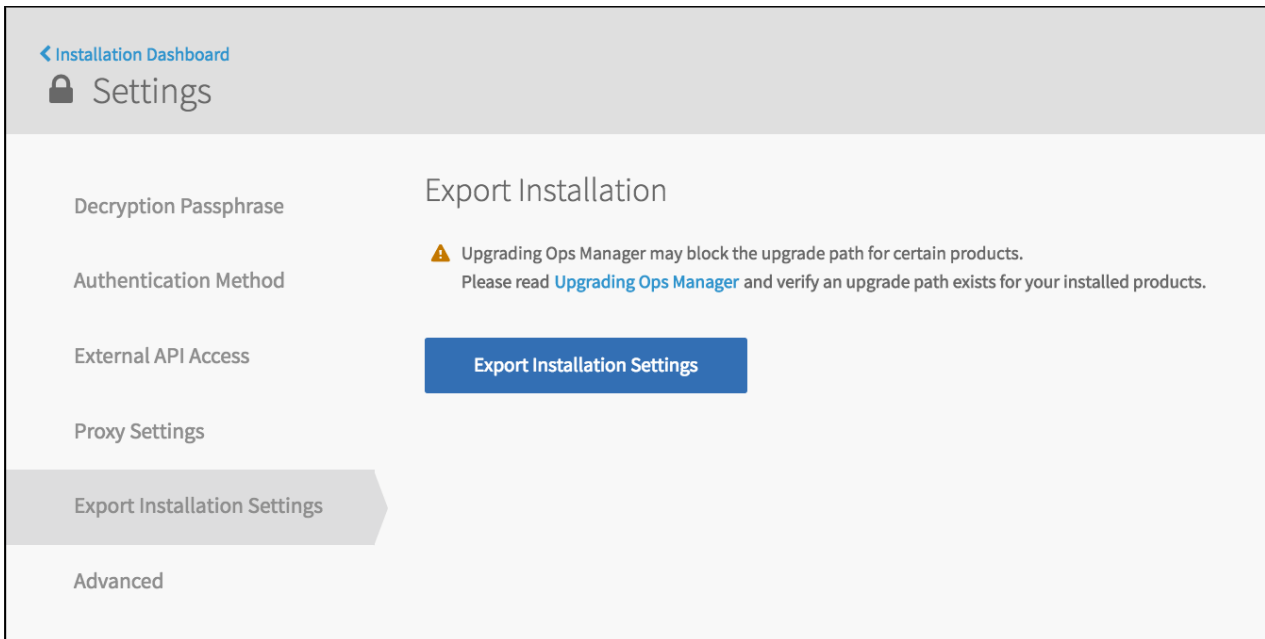
- [Use the Ops Manager UI](#)
- [Use the Ops Manager API](#)

#### Option 1: Use the Ops Manager UI

To export your installation settings using the Ops Manager UI, do the following:

1. From the **Installation Dashboard** in the Ops Manager interface, click your username at the top right navigation.
2. Select **Settings**.
3. Select **Export Installation Settings**.

## 4. Click **Export Installation Settings**.



## Option 2: Use the Ops Manager API

If you want to automate the back up process, you can use the Ops Manager API to export your installation settings.

### 1. To export your installation settings using the Ops Manager API, run the following command:

```
curl https://OPS-MAN-FQDN/api/v0/installation_asset_collection \
-H "Authorization: Bearer UAA-ACCESS-TOKEN" > installation.zip
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token. For more information, see [Access the API](#).

## Step 10: Back Up Your BOSH Director



### Notes:

- The BOSH Director backup can take more than 10 minutes.
  - Because the BBR `backup` command can take a long time to complete, Pivotal recommends you run it independently of the SSH session so that the process can continue running even if your connection to the jumpbox fails.
- Use `nohup`, a `screen`, or a `tmux` session.


### 1. Run the BBR `backup` command to back up your BOSH Director:

```
bbr director \
--private-key-path PRIVATE-KEY-FILE \
--username bbr \
--host HOST \
backup
```

Where:

- `PRIVATE-KEY-FILE` is the path to the private key file that you created from **Bbr Ssh Credentials** in [Step 3: Retrieve BOSH Director Credentials](#).
- `HOST` is the address of the BOSH Director:
  - If the BOSH Director is public, `HOST` is a URL, such as `https://my-bosh.xxx.cf-app.com`.
  - If the BOSH Director is not public, `HOST` is the `BOSH-DIRECTOR-IP` retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.



 **Note:** Use the optional `--debug` flag to enable debug logs. See [Logging](#) below for more information.

If your backup terminates early or fails you need to perform a clean-up.

1. To clean up, run the following `backup-cleanup` command:

```
bbr director \
--private-key-path PRIVATE-KEY-FILE \
--username bbr \
--host HOST \
backup-cleanup
```

Where:

- `PRIVATE-KEY-FILE` is the path to the private key file that you created from **Bbr Ssh Credentials** in [Step 3: Retrieve BOSH Director Credentials](#).
- `HOST` is the address of the BOSH Director:
  - If the BOSH Director is public, `HOST` is a URL, such as `https://my-bosh.xxx.cf-app.com`.
  - If the BOSH Director is not public, `HOST` is the `BOSH-DIRECTOR-IP` retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.

## Step 11: Back Up Your PAS Deployment

### Notes:

- Backing up PAS can take more than 5 minutes, and can take considerably longer with larger blobstores or slow network connections. The backup also incurs Cloud Controller downtime during which users are unable to push, scale, or delete apps. Your apps are not affected.
- Because the BBR `backup` command can take a long time to complete, Pivotal recommends you run it independently of the SSH session, so that the process can continue running even if your connection to the jumpbox fails. The command above uses `nohup` but you could also run the command in a `screen` or `tmux` session.

1. (Optional) If you are not using an internal blobstore or a versioned S3-compatible external blobstore, create a copy of the blobstore with your IaaS specific tool. Your blobstore backup might be slightly inconsistent with your PAS backup depending on the duration of time between performing the backups.
2. Run the BBR `backup` command to back up your PAS deployment:

```
bbr deployment \
--target BOSH-DIRECTOR-IP \
--username BOSH-CLIENT \
--password BOSH-PASSWORD \
--deployment DEPLOYMENT-NAME \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
backup
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.
  - `BOSH-CLIENT`, `BOSH-PASSWORD` are the **Uaa Bbr Client Credentials**, identity and password, that you retrieved in the [Step 3: Retrieve BOSH Director Credentials](#) section above.
  - `DEPLOYMENT-NAME` is the deployment name retrieved in the [Step 6: Identify Your Deployment](#) section above.
  - `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director.
  - Use the optional `--debug` flag to enable debug logs. For more information, see [Logging](#) below.
  - Use the optional `--with-manifest` flag to ensure that BBR downloads your current deployment manifest when backing up. These manifests are included in the Ops Manager export, but are useful for reference.
3. After the command successfully completes, continue to [Step 11: Transfer Backup Artifacts](#).  
If the command fails, perform the following steps:
    - a. Run the BBR `backup-cleanup` command:

```
bbr deployment \
--target BOSH-DIRECTOR-IP \
--username BOSH-CLIENT \
--password BOSH-PASSWORD \
--deployment DEPLOYMENT-NAME \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
backup-cleanup
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.
- `BOSH-CLIENT`, `BOSH-PASSWORD` are the **Uaa Bbr Client Credentials**, identity and password, that you retrieved in the [Step 3: Retrieve BOSH Director Credentials](#) section above.
- `DEPLOYMENT-NAME` is the deployment name retrieved in the [Step 6: Identify Your Deployment](#) section above.
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director.
- Use the optional `--debug` flag to enable debug logs. For more information, see [Logging](#) below.
- Use the optional `--with-manifest` flag to ensure that BBR downloads your current deployment manifest when backing up. These manifests are included in the Ops Manager export, but are useful for reference.

b. Run the BBR `backup` command again after checking the following:


- All the parameters in the command are set.
- The BOSH Director credentials are valid.
- The specified deployment exists.

## After Taking Your Backup

### Step 12: Transfer Backup Artifacts

After creating your backup successfully, perform the following steps:

1. Move the backup artifacts off the jumpbox to your preferred storage space. The backup created by BBR consists of a directory with the backup artifacts and metadata files. Pivotal recommends compressing and encrypting the files.
2. Make redundant copies of your backup artifacts and store them in multiple locations to minimize the risk of losing backups in the event of a disaster.
3. Attempt to restore every backup to validate the artifacts. Perform the procedures in the next step, [Step 12: Validate Your Backup](#).

 **Note:** Backup artifacts might contain data covered by European Union regulations. For more information, see [European Union's General Data Protection Regulation \(GDPR\)](#) below.

### Step 13: (Optional) Validate Your Backup

After backing up PCF, consider validating your backup by restoring it and checking the applications. BBR is designed for disaster recovery and BBR backups are only compatible with environments matching their source environment's configuration.

#### warning:

- **The VMs and disks from the backed-up BOSH Director must not be visible to the new BOSH Director** when validating your backup. As a result, Pivotal recommends that you deploy the new BOSH Director to a different IaaS network and account than the VMs and disks of the backed-up BOSH Director.
- **Data services outside of PCF might produce unexpected side effects during restoration.** Restored apps and services might attempt to connect to data services when you restore to a new environment. For example, consider an app that processes mail queues and connects to an external database. When you validate your backup in a test environment, the app might start processing the queue, and this work might be lost.

#### Validate Your Backup in a Second Environment

To spin up a second environment and test the backup, perform the following steps:

1. Export your Ops Manager installation by performing the steps in the [Step 8: Export Installation Settings](#) section above.
2. Create a new Ops Manager VM in a different network to the original. Ensure that the Ops Manager VM has enough persistent disk to accommodate the files exported in the previous step. Consult the topic specific to your IaaS:
  - [Deploying BOSH and Ops Manager to AWS](#)
  - [Configuring AWS for PCF](#)
  - [Deploying Ops Manager on GCP Manually](#)
  - [Provisioning the OpenStack Infrastructure](#)
  - [Deploying Operations Manager to vSphere](#)
3. Ensure that the restore environment is compatible with the backup. For more information, see [Compatibility of Restore](#).
4. Follow the instructions in the [Restoring Pivotal Cloud Foundry from Backup with BBR](#) topic.

## Validate Your PAS Backup Only

For a sandbox or other non-production environment, you can optionally perform an *in-place* restore of PAS only. In this case, you restore the PAS backup to the same PCF environment that the backup was created from. Follow the procedures in [Restoring PCF from Backup with BBR](#).

## Logging

BBR outputs logs to stdout. By default, BBR logs:

- The backup and restore scripts that it finds
- When it starts or finishes a stage, such as pre-backup scripts or backup scripts
- When the process is complete
- When any error occurs

If you require additional logging, use the optional `--debug` flag to print the following information:

- Logs about the API requests made to the BOSH server
- All commands executed on remote instances
- All commands executed on local environment
- Standard in and standard out streams for the backup and restore scripts when they are executed

## Cancel a Backup

If you need to cancel a backup, perform the following steps:

1. Enter `CTRL-C` to terminate the BBR process, then enter `yes` to confirm.
2. Run the BBR `backup-cleanup` command.

- For a canceled director backup, run the following:

```
bbr director \
--private-key-path PRIVATE-KEY-FILE \
--username bbr \
--host HOST \
backup-cleanup
```

Where:

- `PRIVATE-KEY-FILE` is the path to the private key file that you created from **Bbr Ssh Credentials** in [Step 3: Retrieve BOSH Director Credentials](#).
  - `HOST` is the address of the BOSH Director:
    - If the BOSH Director is public, `HOST` is a URL, such as `https://my-bosh.xxx.cf-app.com`.
    - If the BOSH Director is not public, `HOST` is the `BOSH-DIRECTOR-IP` retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.
- For a canceled deployment backup, run the following:

```
bbr deployment \
--target BOSH-DIRECTOR-IP \
--username BOSH-CLIENT \
--password BOSH-PASSWORD \
--deployment DEPLOYMENT-NAME \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
backup-cleanup
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in the [Step 4: Retrieve BOSH Director Address](#) section above.
- `BOSH-CLIENT`, `BOSH-PASSWORD` are the **Uaa Bbr Client Credentials**, identity and password, that you retrieved in the [Step 3: Retrieve BOSH Director Credentials](#) section above.
- `DEPLOYMENT-NAME` is the deployment name retrieved in the [Step 6: Identify Your Deployment](#) section above.
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director.
- Use the optional `--debug` flag to enable debug logs. For more information, see [Logging](#) above.
- Use the optional `--with-manifest` flag to ensure that BBR downloads your current deployment manifest when backing up. These manifests are included in the Ops Manager export, but are useful for reference.

## European Union’s General Data Protection Regulation (GDPR)

Backup artifacts might contain personal and other data covered by the European Union’s *General Data Protection Regulation (GDPR)*. For example, a PAS backup could contain user email addresses. As such, handle backup artifacts in accordance with organizational policies and applicable laws as they pertain to security, confidentiality, and privacy.

## Enabling External Blobstore Backups

Page last updated:

This topic provides instructions for enabling external blobstore backups in your Pivotal Application Service (PAS) tile.

BOSH Backup and Restore (BBR) supports the following:

- Versioned S3 or S3-Compatible Blobstores
- Unversioned S3 or S3-Compatible Blobstores
- Azure Blobstores

For more information, see [Backup and Restore with External Blobstores](#).

**Note:** To enable external blobstore backups for PAS, the **Backup Prepare Node** must be enabled. See [Enable Backup Prepare Node](#) in *Backing Up Pivotal Cloud Foundry with BBR*.

**Note:** The instructions below require the BOSH Command Line Interface (CLI) v2+. For more information, see [Install](#) in the BOSH documentation.

## External Blobstore Support

External blobstore backup support varies based on which version of Ops Manager you are running and what type of blobstore you are backing up.

In some cases, external blobstore support is included in the version of Ops Manager you are using. In other cases, installing Blobstore Add-On is required.

Refer to the table below to determine if external blobstore support is included in the version of Ops Manager you are using.

| Blobstore Type | Ops Manager Version |        |        |        |          |          |
|----------------|---------------------|--------|--------|--------|----------|----------|
|                | Versioned           | Add-On | Add-On | Add-On | Included | Included |
|                | Unversioned         | Add-On | Add-On | Add-On | Add-On   | Included |
|                | Azure               | Add-On | Add-On | Add-On | Add-On   | Included |

## S3 or S3-compatible Blobstores

In PAS v2.2, BBR supports backing up and restoring versioned and unversioned S3 or S3-compatible blobstores by default. For more information about configuring an S3 or S3-compatible blobstore, see [External S3 or Ceph Filestore](#).

**Note:**

- Backup artifacts of external, S3-compatible, versioned blobstores do not contain the physical blobs. BBR requires that the original buckets still exist to be restored.
- To protect yourself from losing a bucket, see [Enable Replication on Your External Blobstore](#) in *Backup and Restore with External Blobstores* in the Cloud Foundry documentation.

## Azure Blobstores

For information about configuring an Azure blobstore for backups and installing Blobstore Add-On, see the following sections:

- [Configure an Azure Blobstore for Backups](#)
- [Install Blobstore Add-On](#)

## Configure an Azure Blobstore for Backups

To configure your Azure blobstore for backups, enable soft deletes in your Azure Storage account. For more information, see [Soft delete for Azure Storage blobs](#) in the Microsoft documentation.

To save storage space and cost, Pivotal recommends that you configure a retention policy to permanently delete objects after a period of time.

## Install Blobstore Add-On

To enable BBR to back up and restore a PAS installation that uses an Azure blobstore, you must install Blobstore Add-On.

To install Blobstore Add-On, follow the instructions below:

1. On the Ops Manager Installation Dashboard, click the PAS tile.
2. From the URL in the address bar, record the deployment name of your PAS installation. The name begins with `cf`. For example, in `https://pcf.example.com/products/cf-3247176589a379f246d1`, the deployment name is `cf-3247176589a379f246d1`.
3. Navigate to the Ops Manager Installation Dashboard and click the BOSH Director tile.
4. In the BOSH Director tile, select the **Credentials** tab.
5. Locate **Director Credentials** and click the corresponding **Link to Credentials**. Record the identity and password.
6. Select the **Status** tab. Record the IP address of your BOSH Director.
7. From the [BOSH Backup and Restore](#) page in Pivotal Network, download the latest version of the add-on.
8. To copy the release archive to your Ops Manager instance, run the following command:

```
scp -i PATH-TO-PRIVATE-KEY backup-and-restore-sdk-addon-SEMMVER.tar.gz ubuntu@YOUR-OPS-MANAGER-VM-IP:~
```

Where:

- `PATH-TO-PRIVATE-KEY` is the path to your Ops Manager private key.
- `SEMMVER` is the semantic version of the add-on that you downloaded in the previous step.
- `YOUR-OPS-MANAGER-VM-IP` is the IP address of your Ops Manager VM.

9. SSH into the Ops Manager instance by following the instructions in [SSH Into Ops Manager VM](#).
10. In the Ops Manager VM, authenticate with your BOSH Director by following the instructions in [Log in to the BOSH Director](#). Use the Director Credentials and Director IP address that you recorded in previous steps.
11. To upload the release that you downloaded from Pivotal Network, run the following command:

```
bosh -e BOSH-DIRECTOR-IP --ca-cert /var/tempest/workspaces/default/root_ca_certificate upload-release backup-and-restore-sdk-addon-SEMMVER.tar.gz
```

Where:

- `BOSH-DIRECTOR-IP` is the IP address of your BOSH Director.
- `SEMMVER` is the semantic version of the add-on that you are uploading.

12. To confirm that the release upload has succeeded, run the following command:

```
bosh -e BOSH-DIRECTOR-IP --ca-cert /var/tempest/workspaces/default/root_ca_certificate releases
```

Where `BOSH-DIRECTOR-IP` is the IP address of your BOSH Director.

You should see a `backup-and-restore-sdk-addon-SEMMVER` entry.

13. To download your current runtime configuration and save it as a file named `runtime-config.yml`, run the following command:

```
bosh -e BOSH-DIRECTOR-IP --ca-cert /var/tempest/workspaces/default/root_ca_certificate runtime-config > runtime-config.yml
```

Where `BOSH-DIRECTOR-IP` is the IP address of your BOSH Director.

If you receive an error message that references a missing runtime configuration, create an empty file and save it as `runtime-config.yml`.

14. Append the following to the `releases` section of your `runtime-config.yml` file:

```
releases:
Append the below to the list of releases:
- name: backup-and-restore-sdk-addon
 version: RELEASE-VERSION
```

Where `RELEASE-VERSION` is the release version.

15. Append the following to the `addons` section of your `runtime-config.yml` file:

```
addons:
Append the below to the list of addons:
- name: sdk-preview
 jobs:
 - name: azure-blobstore-backup-restorer
 release: backup-and-restore-sdk-addon
 properties:
 enabled: true
 containers:
 droplets:
 name: NAME-OF-DROPLETS-CONTAINER
 azure_storage_account: AZURE-STORAGE-ACCOUNT
 azure_storage_key: AZURE-STORAGE-KEY
 packages:
 name: NAME-OF-PACKAGES-CONTAINER
 azure_storage_account: AZURE-STORAGE-ACCOUNT
 azure_storage_key: AZURE-STORAGE-KEY
 buildpacks:
 name: NAME-OF-BUILDPACKS-CONTAINER
 azure_storage_account: AZURE-STORAGE-ACCOUNT
 azure_storage_key: AZURE-STORAGE-KEY
 include:
 deployments:
 - PAS-DEPLOYMENT-NAME
 jobs:
 - name: mysql-backup
 release: cf-backup-and-restore
```

Replace the placeholder text as follows:

- In the `droplets`, `packages`, and `buildpacks` section, replace the text with the values configured in Ops Manager.
- In the `include` section, replace the text with the PAS deployment name that you recorded in a previous step.

16. (Optional) To configure backup and restore for Azure Sovereign Cloud, configure the `environment` property described in the [Backup and Restore SDK Documentation](#) topic in GitHub.

For more information about Azure Sovereign Cloud, see [Microsoft National Clouds](#) in the Microsoft documentation.

17. To complete updating the runtime configuration, run the following command:

```
bosh -e BOSH-DIRECTOR-IP --ca-cert /var/tempest/workspaces/default/root_ca_certificate update-runtime-config runtime-config.yml
```

Where `BOSH-DIRECTOR-IP` is the IP address of your BOSH Director.

18. Navigate to your Ops Manager Installation Dashboard and click **Apply Changes**.

## PAS Component Availability During Backup

This topic describes the operational impact of backing up Pivotal Application Service (PAS) components with BBR. To ensure correctness of backups, each component that requires backup has its own set of scripts. The sections in this topic describe the availability of each component during backup of its database.

### Cloud Controller

The Cloud Controller is unavailable during backup. Apps and Services continue to run as normal, but you cannot perform operations that require the [Cloud Controller API](#). This includes the following:

- Pushing new apps or creating new services
- Modifying existing apps or services
- Using the clients of the Cloud Controller API, such as the following:
  - The Cloud Foundry Command Line Interface (cf CLI)
  - Apps Manager and its integrations
  - The [Java client](#) used by Spring apps

The backup process for the Cloud Controller is as follows:

| Stage                 | Description                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 1: Pre-backup lock    | The processes running on the <b>Cloud Controller Worker</b> , <b>Cloud Controller</b> , and <b>Clock Global</b> VMs are stopped.             |
| 2: Backup             | The BBR SDK backup script runs to backup the Cloud Controller database (CCDB), which contains state information for apps on your deployment. |
| 3: Post-backup unlock | The processes start again on the <b>Cloud Controller Worker</b> , <b>Cloud Controller</b> , and <b>Clock Global</b> VMs.                     |

### UAA

UAA remains available in read-only mode during backup. This means that you cannot perform write operations for clients, users, groups, identity providers, or zone configuration. However, you can continue performing read operations, such as generating, validating, and revoking tokens. Additionally, UAA continues to authenticate users and authorize requests for users and clients.

The read-only behavior during backup applies to all of the following ways of accessing UAA: the UAA API, the UAA CLI, cf CLI, login screens, and services such as the Single Sign-On Service tile.

The backup process for UAA is as follows:

| Stage                 | Description                                                                                               |
|-----------------------|-----------------------------------------------------------------------------------------------------------|
| 1: Pre-backup lock    | UAA enters read-only mode.                                                                                |
| 2: Backup             | The BBR SDK backup script runs to backup the UAA database, which contains Cloud Foundry user credentials. |
| 3: Post-backup unlock | UAA exits read-only mode.                                                                                 |

### Routing API

The [Routing API](#) remains available during backup. However, you cannot perform write operations using the Routing API because the routing database is locked. All read operations offered by the Routing API remain available.


The BBR SDK backup script for the Routing API backs up its database, which contains router groups, routes, and internal implementation information.

### Usage Service

The Usage Service is unavailable during backup. You cannot access the API as described in [Monitoring App, Task, and Service Instance Usage](#). Additionally, you cannot view usage and accounting reports as described in [Monitoring Instance Usage with Apps Manager](#).



The backup process for Usage Service is as follows:


 **Note:** The Usage Service runs as a set of Cloud Foundry apps in the `system` org.

| Stage                 | Description                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 1: Pre-backup lock    | The Usage Service apps in the <code>system</code> org stop. This lock occurs before the Cloud Controller and UAA components lock.           |
| 2: Backup             | The BBR SDK backup script runs to backup the Usage Service database.                                                                        |
| 3: Post-backup unlock | The Usage Service apps in the <code>system</code> org start again. This unlock occurs after the Cloud Controller and UAA components unlock. |

## App Autoscaler

The [App Autoscaler service](#) is unavailable during backup. You cannot access the UI or API. For any apps configured to use the App Autoscaler, the service does not scale these apps during backup.

The backup process for App Autoscaler is as follows:

 **Note:** The App Autoscaler service runs as a set of Cloud Foundry apps in the `system` org.

| Stage                 | Description                                                                                                                              |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 1: Pre-backup lock    | The Autoscaler apps in the <code>system</code> org stop. This lock occurs before the Cloud Controller and UAA components lock.           |
| 2: Backup             | The BBR SDK backup script runs to backup the App Autoscaler database.                                                                    |
| 3: Post-backup unlock | The Autoscaler apps in the <code>system</code> org start again. This unlock occurs after the Cloud Controller and UAA components unlock. |

## NFS Volume Service

The NFS service broker backup scripts rely on the locking of the Cloud Controller to stop traffic to its service. This is because the Cloud Controller is responsible for invoking the NFS service broker.

When the Cloud Controller locks during backup, you cannot create or delete new instances or bindings of a volume service. However, apps already bound to a volume service continue to operate normally during backups.

The NFS service broker backup script performs a backup of the database used to store service instances and service bindings for the NFS service broker.

## Notification Service

The Notification Service is not available during backup with BBR due to its dependency on the Cloud Controller. Notifications cannot be sent while the Cloud Controller is unavailable.

## Network Policy Server

The Network Policy Server is unavailable during backup. While existing policies are still enforced, you cannot use the cf CLI to add or remove policies for Container Networking as documented in [Administering Container-to-Container Networking](#).

## CredHub

Runtime CredHub is unavailable during backup. If the service instance credentials for an app are stored in CredHub, the app cannot fetch those credentials during backup. In some cases, apps may not start if they cannot fetch credentials for a service instance binding.



## Restoring PCF from Backup with BBR

Page last updated:

This topic describes the procedure for restoring your critical backend Pivotal Cloud Foundry (PCF) components with BOSH Backup and Restore (BBR), a command-line tool for backing up and restoring BOSH deployments. To perform the procedures in this topic, you must have backed up PCF by following the steps in the [Backing Up Pivotal Cloud Foundry with BBR](#) topic.

To view the BBR release notes, see [BOSH Backup and Restore Release Notes](#).

The procedures described in this topic prepare your environment for PCF, deploy Ops Manager, import your installation settings, and use BBR to restore your PCF components.

**⚠ warning:** Restoring PCF with BBR is a destructive operation. If the restore fails, the new environment may be left in an unusable state and require reprovisioning. Only perform the procedures in this topic for the purpose of disaster recovery, such as recreating PCF after a storage-area network (SAN) corruption.

**⚠ warning:** When validating your backup, the VMs and disks from the backed-up BOSH Director should not be visible to the new BOSH Director. As a result, Pivotal recommends that you deploy the new BOSH Director to a different IaaS network and account than the VMs and disks of the backed up BOSH Director.

**💡 Note:** If the BOSH Director you are restoring had any deployments that were deployed manually rather than through an Ops Manager tile, you must restore them manually at the end of the process. For more information, see [\(Optional\) Step 16: Restore Non-Tile Deployments](#).

## Compatibility of Restore

This section describes the restrictions for a backup artifact to be restorable to another environment. This section is for guidance only, and Pivotal highly recommends that operators validate their backups by using the backup artifacts in a restore.

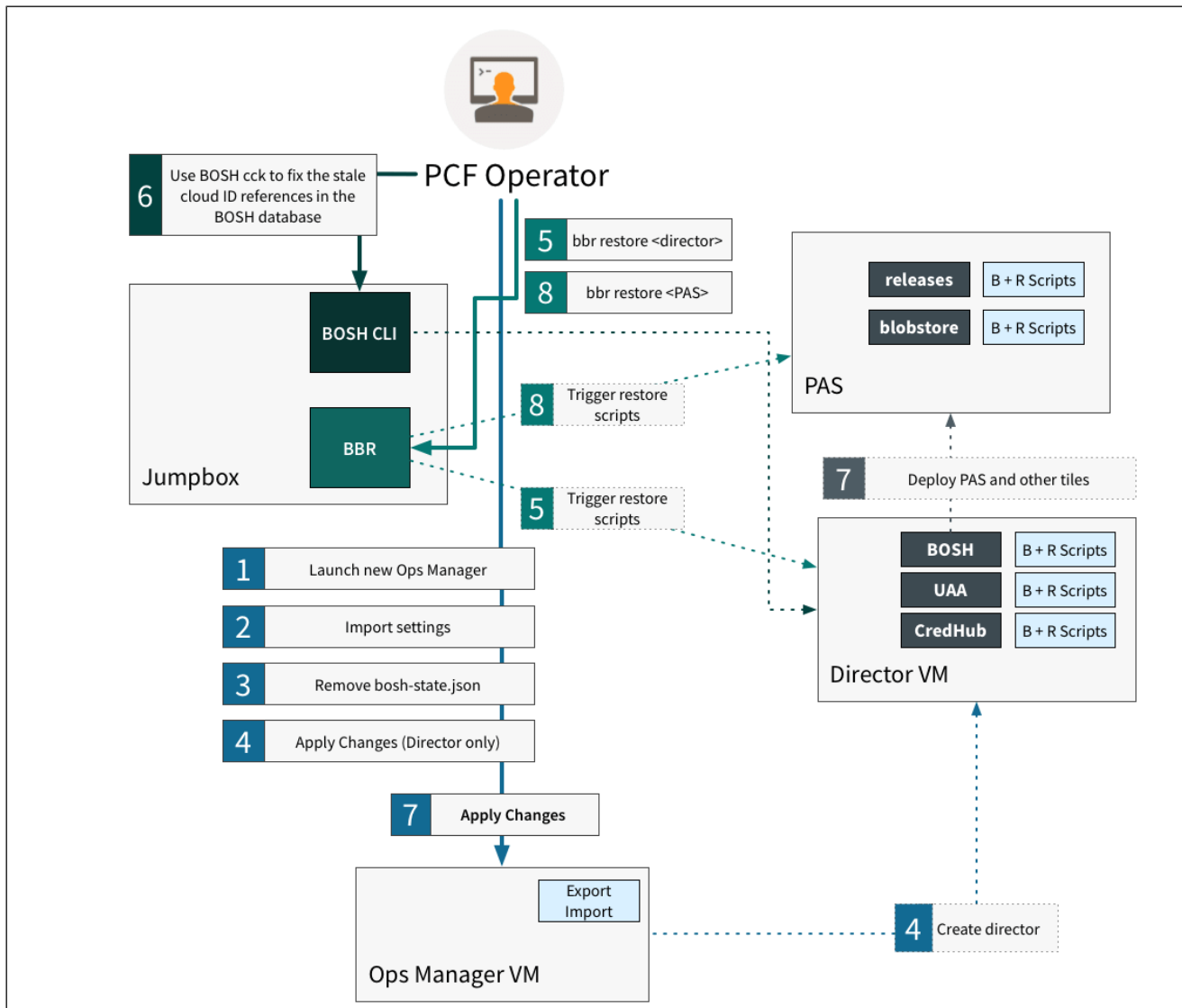
Consult the following restrictions for a backup artifact to be restorable:

- **CIDR ranges:** BBR requires the IP address ranges to be the same in the restore environment as in the backup environment.
- **Topology:** BBR requires the BOSH topology of a deployment to be the same in the restore environment as it was in the backup environment.
- **Naming of instance groups and jobs:** For any deployment that implements the backup and restore scripts, the instance groups and jobs must have the same names.
- **Number of instance groups and jobs:** For instance groups and jobs that have backup and restore scripts, there must be the same number of instances.
- **Limited validation:** BBR puts the backed up data into the corresponding instance groups and jobs in the restored environment, but can't validate the restore beyond that. For example, if the MySQL encryption key is different in the restore environment, the BBR restore might succeed although the restored MySQL database is unusable.
- **PCF version:** BBR can restore to the same version of PCF that was backed up. BBR does not support restoring to other major, minor, or patch releases.

**💡 Note:** A change in VM size or underlying hardware will not affect BBR's ability to restore data, as long as there is adequate storage space to restore the data.

## Restore Workflow

Click the diagram below to see the full-size image.



The diagram above shows the flow of the PCF restore process in a series of steps performed by the PCF operator. The following steps will be covered in more detail throughout this topic.

1. **Launch new Ops Manager:** Perform the procedures for your IaaS to deploy Ops Manager. See part one of the [Deploy Ops Manager and Import Installation Settings](#) step below for more information.
2. **Import settings:** You can import settings either with the Ops Manager UI or API. See part two of the [Deploy Ops Manager and Import Installation Settings](#) step below for more information.
3. **Remove bosh-state.json:** SSH into your Ops Manager VM and delete the `bosh-state.json` file. See the [Remove BOSH State File](#) step below for more information.
4. **Apply Changes (Director only):** Use the Ops Manager API to only deploy the BOSH Director. See the [Deploy the BOSH Director](#) step below for more information.
5. **bbr restore <director>:** Run the BBR restore command from your jumpbox to restore the BOSH Director. See the [Restore the BOSH Director](#) step below for more information.
6. **Use BOSH cck to fix the stale cloud ID references in the BOSH database:** For each deployment in the BOSH Director, you will need to run a `bosh cloud-check` command. See the [Remove Stale Cloud IDs for All Deployments](#) step below for more information.
7. **Apply Changes:** Click **Apply Changes** from the Ops Manager Installation Dashboard.
8. **bbr restore PAS:** Run the BBR restore command from your jumpbox to restore PAS. See the [Restore PAS](#) step below for more information.

## Prepare to Restore

This section provides the steps you need to perform before restoring your PCF backup with BBR.

### Step 1: (Optional) Prepare Your Environment

In an event of a disaster, you may lose not only your VMs and disks, but your IaaS resources as well, such as networks and load balancers.

If you need to recreate your IaaS resources, prepare your environment for PCF by following the instructions specific to your IaaS in [Installing Pivotal Cloud Foundry](#).

**Note:** The instructions for installing PCF on Amazon Web Services (AWS) and OpenStack combine the procedures for preparing your environment and deploying Ops Manager into a single topic. The instructions for the other supported IaaSes split these procedures into two separate topics.

If you recreate your IaaS resources, you must also add those resources to Ops Manager by performing the procedures in the [Step 3: \(Optional\) Configure Ops Manager for New Resources](#) section.

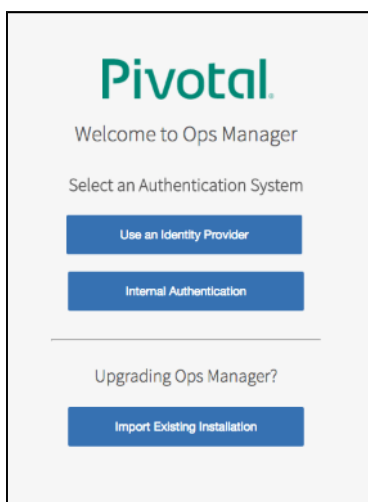
### Step 2: Deploy Ops Manager and Import Installation Settings

1. Perform the procedures for your IaaS to deploy Ops Manager:

- **AWS:**
  - If you configured AWS manually, see *Step 12: Launch an Ops Manager API* through *Step 19: Create a MySQL Database Using AWS RDS* of [Installing PCF on AWS Manually](#).
  - If you used Terraform to install PCF on AWS, see [Installing PCF on AWS Using Terraform](#).
- **GCP:** See [Deploying Ops Manager on GCP Manually](#).
- **OpenStack:** See *Step 4: Create Ops Manager Image* through *Step 9: Create a DNS Entry* in [Deploying Ops Manager to OpenStack](#).
- **vSphere:** See [Deploying Ops Manager on vSphere](#).

2. Import your installation settings. This can be done in two ways:

- a. Using the Ops Manager UI:
  - i. Access your new Ops Manager by navigating to `YOUR-OPS-MAN-FQDN` in a browser.
  - ii. On the **Welcome to Ops Manager** page, click **Import Existing Installation**.



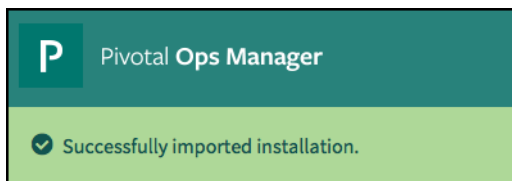
iii. In the import panel, perform the following tasks:

- Enter the **Decryption Passphrase** in use when you exported the installation settings from Ops Manager.
- Click **Choose File** and browse to the installation zip file that you exported in the [Step 9: Export Installation Settings](#) section of the *Backing Up Pivotal Cloud Foundry with BBR* topic.

iv. Click **Import**.

**Note:** Some browsers do not provide feedback on the status of the import process, and may appear to hang. The import process takes at least 10 minutes, and takes longer the more tiles that were present on the backed-up Ops Manager.

v. A **Successfully imported installation** message appears upon completion.



b. Using the Ops Manager API:

```
curl "https://OPS-MAN-FQDN/api/v1/installation_asset_collection" \
-X POST \
-H "Authorization: Bearer UAA-ACCESS-TOKEN" \
-F 'installation[file]=@installation.zip' \
-F 'passphrase=DECRYPTION-PASSPHRASE'
```

Where:

- **OPS-MAN-FQDN** is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- **UAA-ACCESS-TOKEN** is the UAA access token. For more information about how to retrieve this token, see [Using the Ops Manager API](#).
- **DECRYPTION-PASSPHRASE** is the decryption passphrase in use when you exported the installation settings from Ops Manager.

**Warning:** Do not click **Apply Changes** in Ops Manager until the instruction in Step 14: Redeploy PAS.

## Step 3: (Optional) Configure Ops Manager for New Resources

If you recreated IaaS resources such as networks and load balancers by following the steps in the [Step 1: \(Optional\) Prepare Your Environment](#) section above, perform the following steps to update Ops Manager with your new resources:

1. Enable Ops Manager advanced mode. For more information, see [How to Enable Advanced Mode in the Ops Manager](#) in the Pivotal Knowledge Base.

**Note:** In advanced mode Ops Manager will allow you to make changes that are normally disabled. You may see warning messages when you save changes.

2. Navigate to the Ops Manager Installation Dashboard and click the BOSH Director tile.
3. If you are using Google Cloud Platform (GCP), click **Google Config** and update:
  - a. **Project ID** to reflect the GCP project ID.
  - b. **Default Deployment Tag** to reflect the environment name.
  - c. **AuthJSON** to reflect the service account.
4. Click **Create Networks** and update the network names to reflect the network names for the new environment.

5. If your BOSH Director had an external hostname, you must change it in **Director Config > Director Hostname** to ensure it does not conflict with the hostname of the backed up Director.
6. Return to the Ops Manager Installation Dashboard and click the Pivotal Application Service (PAS) tile.
7. Click **Resource Config**. If necessary for your IaaS, enter the name of your new load balancers in the **Load Balancers** column.
8. If necessary, click **Networking** and update the load balancer SSL certificate and private key under **Certificates and Private Keys for HAProxy and Router**.
9. If your environment has a new DNS address, update the old environment DNS entries to point to the new load balancer addresses. For more information, see the [Step 4: Configure Networking](#) section of the *Using Your Own Load Balancer* topic and follow the link to the instructions for your IaaS.
10. If your PAS uses an external blobstore, ensure that the PAS tile is configured to use a different blobstore, otherwise it will attempt to connect to the blobstore that the backed up PAS is using.
11. Ensure your **System Domain** and **Apps Domain** under PAS **Domains** are updated to refer to the new environment's domains.
12. Ensure that there are no outstanding warning messages in the BOSH Director tile, then disable Ops Manager advanced mode. For more information, see [How to Enable Advanced Mode in the Ops Manager](#) in the Pivotal Knowledge Base.

## Step 4: Remove BOSH State File

1. SSH into your Ops Manager VM. For more information, see the [SSH into Ops Manager](#) section of the *Advanced Troubleshooting with the BOSH CLI* topic.
2. To delete the `/var/tempest/workspaces/default/deployments/bosh-state.json` file, run the following on the Ops Manager VM:

```
sudo rm /var/tempest/workspaces/default/deployments/bosh-state.json
```

3. In a browser, navigate to your Ops manager's fully-qualified domain name.
4. Log in to Ops Manager.
5. Import the required stemcell for each tile that requires one. For more information about importing stemcells, see [Importing and Managing Stemcells](#).

## Step 5: Deploy the BOSH Director

Perform the steps in the [Applying Changes to BOSH Director](#) topic to use the Ops Manager API to only deploy the BOSH Director.

## Step 6: Transfer Artifacts to Jumpbox

In the [Step 9: Back Up Your PAS Deployment](#) section of the *Backing Up Pivotal Cloud Foundry with BBR* topic, in the *After Taking the Backups* section you moved the TAR and metadata files of the backup artifacts off your jumpbox to your preferred storage space. Now you must transfer those files back to your jumpbox.

## Restore Your Backup

This section provides the steps you need to perform to restore your PCF backup with BBR.

## Step 7: Retrieve BOSH Director Credentials

To use BBR, you must retrieve and record the following credentials:

- Bosh Director Credentials
- Bbr Ssh Credentials

- Uaa Bbr Client Credentials

There are two ways to retrieve BOSH Director credentials:

- Ops Manager Installation Dashboard
- Ops Manager API

### Option 1: Ops Manager Installation Dashboard

To retrieve your BOSH Director credentials using the Ops Manager Installation Dashboard, perform the following steps:

1. Navigate to the Ops Manager Installation Dashboard.
2. Click the BOSH Director tile.
3. Click the **Credentials** tab.

| BOSH Director                                                |                              |                                    |
|--------------------------------------------------------------|------------------------------|------------------------------------|
| <div>Settings</div> <div>Status</div> <div>Credentials</div> |                              |                                    |
| JOB                                                          | NAME                         | CREDENTIALS                        |
| BOSH Director                                                | Vm Credentials               | <a href="#">Link to Credential</a> |
|                                                              | Agent Credentials            | <a href="#">Link to Credential</a> |
|                                                              | Registry Credentials         | <a href="#">Link to Credential</a> |
|                                                              | Director Credentials         | <a href="#">Link to Credential</a> |
|                                                              | Postgres Credentials         | <a href="#">Link to Credential</a> |
|                                                              | Blobstore Credentials        | <a href="#">Link to Credential</a> |
|                                                              | Health Monitor Credentials   | <a href="#">Link to Credential</a> |
|                                                              | Uaa Admin User Credentials   | <a href="#">Link to Credential</a> |
|                                                              | Uaa Login Client Credentials | <a href="#">Link to Credential</a> |
|                                                              | Uaa Jwt Key                  | <a href="#">Link to Credential</a> |
|                                                              | Bbr Ssh Credentials          | <a href="#">Link to Credential</a> |
|                                                              | Uaa Bbr Client Credentials   | <a href="#">Link to Credential</a> |
|                                                              | Bosh Commandline Credentials | <a href="#">Link to Credential</a> |
|                                                              | Blobstore Certificate        | <a href="#">Link to Credential</a> |

4. Locate **Director Credentials**.

- a. Click **Link to Credentials** next to it.
- b. Verify the value of the `identity` field. It should be `director`.
- c. Copy and record the value of the `password` field.

5. Locate **Bbr Ssh Credentials**.

- a. Click **Link to Credentials** next to it.
- b. Copy the value of the `private_key_pem` field.
- c. Run the following command to reformat the copied value, and save it in the current directory to a file named `PRIVATE-KEY-FILE`:



```
printf -- "YOUR-PRIVATE-KEY" > PRIVATE-KEY-FILE
```

Where:

- `YOUR-PRIVATE-KEY` is the text of your private key.
- `PRIVATE-KEY-FILE` is the path to the private key file you are creating.

For example:

```
$ printf -- "-----BEGIN RSA PRIVATE KEY----- MIIEkeycontents -----END RSA PRIVATE KEY-----" > bbr_key.pem
```

## 6. Locate the Uaa Bbr Client Credentials

- Click **Link to Credentials** next to it.
- Verify the value of the `identity` field. It should be `bbr_client`.
- Record the value of the `password` field.

## Option 2: Ops Manager API

To retrieve BOSH Director credentials using the Ops Manager API, perform the following steps:

- Obtain your UAA access token. For more information, see [Access the API](#).
- Retrieve the **Director Credentials** by performing the following steps:
  - Run the following command:

```
curl "https://OPS-MAN-FQDN/api/v0/deployed/director/credentials/director_credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token.

- Verify the value of the `identity` field. It should be `director`.
- Record the value of the `password` field.

## 3. Retrieve the Bbr Ssh Credentials by performing the following steps:

- Run the following command:

```
curl "https://OPS-MAN-FQDN/api/v0/deployed/director/credentials/bbr_ssh_credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token.

- Copy the value of the `private_key_pem` field.
- Run the following command to reformat the copied value, and save it in the current directory to a file named `PRIVATE-KEY-FILE`:

```
printf -- "YOUR-PRIVATE-KEY" > PRIVATE-KEY-FILE
```

Where:

- `YOUR-PRIVATE-KEY` is the text of your private key.
- `PRIVATE-KEY-FILE` is the path to the private key file you are creating.

For example:

```
$ printf -- "-----BEGIN RSA PRIVATE KEY----- MIIEkeycontents -----END RSA PRIVATE KEY-----" > bbr_key.pem
```

## 4. Retrieve the Uaa Bbr Client Credentials by performing the following steps:

- Run the following command:

```
curl "https://OPS-MAN-FQDN/api/v0/deployed/director/credentials/uaa_bbr_client_credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token.

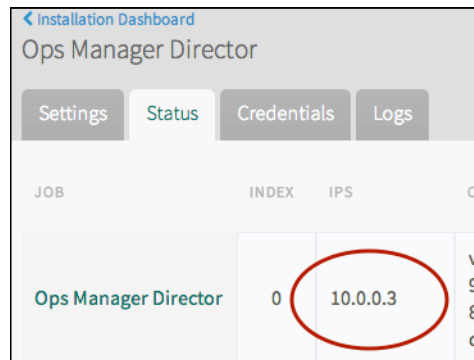
- Verify the value of the `identity` field. It should be `bbr_client`.
- Record the value of the `password` field.

For more information about using the Ops Manager API, see the [Using the Ops Manager API](#) topic.

## Step 8: Retrieve BOSH Director Address

Perform the following steps to retrieve the IP address of your BOSH Director from the BOSH Director tile:

- If you are not using the Ops Manager VM as your jumpbox, install the latest [BOSH CLI](#) on your jumpbox.
- From the Installation Dashboard in Ops Manager, select **BOSH Director > Status** and record the IP address listed for the Director. You access the



| JOB                  | INDEX | IPS      | CI                |
|----------------------|-------|----------|-------------------|
| Ops Manager Director | 0     | 10.0.0.3 | vi<br>9<br>8<br>d |

BOSH Director using this IP address.

- From the command line, log into the BOSH Director, using the IP address that you recorded above, by running the following command:

```
bosh -e DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE log-in
```

Where:

- `DIRECTOR-IP` is the BOSH Director IP address recorded above.
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the root Certificate Authority (CA) certificate as outlined in [Step 1: Set Up your Jumpbox](#), above.

- When prompted for **Email ()**, specify `director`.
- When prompted for **Password ()**, enter the **Director Credentials** that you obtained in [Retrieve BOSH Director Credentials](#).  
For example:

```
$ bosh -e 10.0.0.3 \
--ca-cert /var/tempest/workspaces/default/root_ca_certificate log-in
Email (): director
Password (): *****
Successfully authenticated with UAA
Succeeded
```

## Step 9: Restore the BOSH Director



### Notes:

- The BBR BOSH Director restore command can take at least 15 minutes to complete.
- Pivotal recommends that you run it independently of the SSH session, so that the process can continue running even if your connection to the

jumpbox fails. The command above uses `nohup` but you could also run the command in a `screen` or `tmux` session.

1. SSH into your jumpbox. If you are using the Ops Manager VM as your jumpbox, see the [Log in to the Ops Manager VM with SSH](#) section of *Advanced Troubleshooting with the BOSH CLI* for procedures on how to use SSH to connect to the Ops Manager VM.
2. Ensure the BOSH Director backup artifact is in the folder you from which you will run BBR.
3. Run the BBR restore command from your jumpbox to restore the BOSH Director:

```
bbr director \
--private-key-path PRIVATE-KEY-FILE \
--username bbr \
--host HOST \
restore \
--artifact-path PATH-TO-DIRECTOR-BACKUP
```

Where:

- `PATH-TO-DIRECTOR-BACKUP` is the path to the Director backup you want to restore.
  - `PRIVATE-KEY-FILE` is the path to the private key file you created in [Step 7: Retrieve BOSH Director Credentials](#).
  - `HOST` is the address of the BOSH Director.
    - If the BOSH Director is public, `HOST` is a URL, such as `https://my-bosh.xxx.cf-app.com`.
    - If the BOSH Director is not public, `HOST` is the `BOSH-DIRECTOR-IP` retrieved in [Step 8: Retrieve BOSH Director Address](#).
  - Use the optional `--debug` flag if you want to enable debug logs. See the [Logging](#) section of the *Backing Up Pivotal Cloud Foundry with BBR* topic for more information.
4. After the command succeeds, continue to [Step 10: Identify Your Deployment](#).

If the command fails, complete the following procedure:

- a. Run the BBR restore-cleanup command:

```
bbr director \
--private-key-path PRIVATE-KEY-FILE \
--username bbr \
--host HOST \
restore-cleanup
```

Where:

- `PRIVATE-KEY-FILE` is the path to the private key file you created in [Step 7: Retrieve BOSH Credentials](#).
  - `HOST` is the address of the BOSH Director.
    - If the BOSH Director is public, `HOST` is a URL, such as `https://my-bosh.xxx.cf-app.com`.
    - If the BOSH Director is not public, `HOST` is the `BOSH-DIRECTOR-IP` retrieved in [Step 8: Retrieve BOSH Director Address](#).
- b. Run the BBR restore command again after checking the following:
    - All the parameters in the command are set.
    - The BOSH Director credentials are valid.
    - The specified deployment exists.
    - The source deployment is compatible with the target deployment.
    - That the jumpbox can reach the BOSH Director.

## Step 10: Identify Your Deployment

1. Log in to your BOSH Director.
2. To identify the name of the BOSH deployment that contains PCF, run the following command:

```
bosh -e BOSH-DIRECTOR-IP --ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE deployments
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not

verifiable by the local machine's certificate chain.

For example:

```
$ bosh -e BOSH-DIRECTOR-IP --ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE deployments
```

| Name       | Release(s)                         |
|------------|------------------------------------|
| cf-example | push-apps-manager-release/661.1.24 |
|            | cf-backup-and-restore/0.0.1        |
|            | binary-buildpack/1.0.11            |
|            | capi/1.28.0                        |
|            | cf-autoscaling/91                  |
|            | cf-mysql/35                        |
|            | ...                                |

In the above example, the name of the BOSH deployment that contains PCF is `cf-example`. `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the root Certificate Authority (CA) certificate for the BOSH Director. If you are using the Ops Manager VM as your jumpbox, the path is `/var/tempest/workspaces/default/root_ca_certificate`.

## Step 11: Remove Stale Cloud IDs for All Deployments

1. Review the deployments listed when performing [Step 10: Identify Your Deployment](#).
2. To reconcile the BOSH Director's internal state with the state in the IaaS, run the following command for each deployment:

```
bosh -e BOSH-DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
-d DEPLOYMENT-NAME -n cck \
--resolution delete_disk_reference \
--resolution delete_vm_reference
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.
- `DEPLOYMENT-NAME` is the deployment name retrieved in [Step 10: Identify Your Deployment](#).

3. To delete disk references, run the following command:

```
bosh cloud-check
```

If the `bosh cloud-check` command does not successfully delete disk references, and you see a message similar to the following, perform the additional procedures in the [Remove Unused Disks](#) section below.

```
Scanning 19 persistent disks: 19 OK, 0 missing ...
```

## Step 12: Redeploy PAS

### Determine the Required Stemcells

Perform either the following procedures to determine which stemcell is used by PAS:

- Review the Stemcell Library:
  1. Go to **Stemcell Library**.
  2. Record the PAS stemcell release number from the **Staged** column.
- Review a Stemcell List Using BOSH CLI:
  1. To retrieve the stemcell release using the BOSH CLI, run the following command:

```
bosh -e BOSH-DIRECTOR-IP deployments
```

Where `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).

For example:

```
$ bosh -e BOSH-DIRECTOR-IP deployments
Using environment '10.0.0.5' as user 'director' (bosh.*.read, openid, bosh.*.admin, bosh.read, bosh.admin)

Name Release(s) Stemcell(s) Team(s) Cloud Config
cf-9cb6995b7d746cd77438 push-apps-manager-release/661.1.24 bosh-google-kvm-ubuntu-trusty-go_agent/3421.9 - latest
...
```

For more information about stemcells in Ops Manager, see [Importing and Managing Stemcells](#).

## Upload Stemcells

1. Download the stemcell from [Pivotal Network](#).
2. Run the following command to upload the stemcell used by PAS:

```
bosh -e BOSH-DIRECTOR-IP \
-d DEPLOYMENT-NAME \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
upload-stemcell \
--fix PATH-TO-STEMCELL
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
  - `DEPLOYMENT-NAME` is the deployment name retrieved in [Step 10: Identify Your Deployment](#).
  - `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.
  - `PATH-TO-STEMCELL` is the path to your tile's stemcell.
3. To ensure the stemcells for all of your other installed tiles have been uploaded, repeat the last step, running the `bosh upload-stemcell --fix PATH-TO-STEMCELL` command, for each stemcell that is different from the already uploaded PAS stemcell.

## Redeploy PAS

1. From the Ops Manager Installation Dashboard, navigate to **PAS Resource Config**.
2. Ensure the number of instances for MySQL Server is set to `1`.

**⚠ warning:** Restore will fail if there is not exactly one MySQL Server instance deployed.

3. Ensure that all errands needed by your system are set to run.
4. Return to the Ops Manager Installation Dashboard and click **Apply Changes** to redeploy.

## Step 13: (Optional) Restore Service Data

**⚠ warning:** BBR does not back up or restore any service data.

For this step, restore data to pre-provisioned service tiles.

The procedures for restoring service data vary. Consult the documentation for your service tile for more information.

For example, if you are using Redis for PCF v1.14, see [Using BOSH Backup and Restore \(BBR\)](#).

## Step 14: Restore PAS

## Notes:

- The BBR PAS restore command can take at least 15 minutes to complete.
- Pivotal recommends that you run it independently of the SSH session, so that the process can continue running even if your connection to the jumpbox fails. The command above uses `nohup` but you could also run the command in a `screen` or `tmux` session.

1. Refer to the table in [Enabling External Blobstore Backups](#). If external blobstore support is not included in the version of Ops Manager and PAS you are using, restore the external blobstore with your IaaS-specific tools before restoring PAS.
2. Run the BBR restore command from your jumpbox to restore PAS:

```
bbr deployment \
--target BOSH-DIRECTOR-IP \
--username BOSH-CLIENT \
--password BOSH-PASSWORD \
--deployment DEPLOYMENT-NAME \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
restore \
--artifact-path PATH-TO-PAS-BACKUP
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
  - `BOSH-CLIENT`, `BOSH-PASSWORD` are the **Uaa Bbr Client Credentials**, identity and password, that you retrieved in [Step 7: Retrieve BOSH Director Credentials](#).
  - `DEPLOYMENT-NAME` is the deployment name retrieved in [Step 10: Identify Your Deployment](#).
  - `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.
  - `PATH-TO-PAS-BACKUP` is the path to the PAS backup you want to restore.
3. If desired, scale the MySQL Server job back up to its previous number of instances by navigating to the **Resource Config** section of the PAS tile. After scaling the job, return to the Ops Manager Installation Dashboard.
  4. Click **Review Pending Changes**.
  5. Review your changes. For more information, see [Reviewing Pending Product Changes](#).
  6. Click **Apply Changes** to deploy.

## Step 15: (Optional) Restore On-Demand Service Instances

If you have on-demand service instances provisioned by an on-demand service broker, perform the following steps to restore them after successfully restoring PAS:

1. Navigate to an on-demand service tile in the **Installation Dashboard**.
2. Select the **Errands** tab.
3. Ensure the **Upgrade All Service Instances** errand is **On**.
4. Repeat for all on-demand service tiles.
5. Return to the **Installation Dashboard** and run **Apply Changes**. This will include running the Upgrade All Service Instances errand for the on-demand service, which will redeploy the on-demand service instances.
6. (Optional) Restore service data to every on-demand service instance.
7. Any app on PAS bound to an on-demand service instance may need to be restarted to start consuming the restored on-demand service instances.

## Step 16: (Optional) Restore Non-Tile Deployments

If you have any deployments that were deployed manually with the BOSH Director rather than through an Ops Manager tile, perform the following steps to restore the VMs.

1. To obtain a list of all deployments on your BOSH Director, run the following command:

```
bosh -e BOSH-DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
deployments
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.

2. Identify the names of the deployments that you need to restore. Do not include the deployments from Ops Manager tiles.

3. Run the following command for each deployment you need to restore:

```
bosh -n -e BOSH-DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
-d DEPLOYMENT-NAME \
cck --resolution=recreate_vm
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.
- `DEPLOYMENT-NAME` is the deployment name retrieved in [Step 10: Identify Your Deployment](#).

4. Run the following command to verify the status of the VMs in each deployment:

```
bosh -e BOSH-DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE \
-d DEPLOYMENT-NAME \
vms
```

Where:


- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.
- `DEPLOYMENT-NAME` is the deployment name retrieved in [Step 10: Identify Your Deployment](#).

The process state for all VMs should show as `running`.

## After Restoring Your Backup

This section provides the steps you need to perform after restoring your PCF backup with BBR.

### Step 17: Remove Unused Disks

 **warning:** This is a very destructive operation.

Disks from a previous deployment will prevent recreated deployments from working.

#### Use BOSH To Clean Up Disks

1. To clean up disk references, run the following command:

```
bosh cloud-check
```

#### Manually Clean Up Disks

If `bosh cloud-check` does not clean up all disk references, you must manually delete the remaining disks.

1. To delete the remaining disks, perform one of the following procedures:

- Use the BOSH CLI to delete the disks by performing the following steps:

1. Target the redeployed BOSH Director using the BOSH CLI by performing the procedures in [Step 8: Retrieve BOSH Director Address](#).
2. List the deployments by running the following command:

```
bosh -e BOSH-DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE deployments
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.

3. Delete each deployment with the following command:

```
bosh -d DEPLOYMENT-NAME delete-deployment
```

Where:

- `DEPLOYMENT-NAME` is the deployment name retrieved in [Step 10: Identify Your Deployment](#).

- Log in to your IaaS account and delete the disks manually.

1. To retrieve a list of disk IDs, run the following command:

```
bosh -e BOSH-DIRECTOR-IP \
--ca-cert PATH-TO-BOSH-SERVER-CERTIFICATE instances -i
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP retrieved in [Step 8: Retrieve BOSH Director Address](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is the path to the Certificate Authority (CA) certificate for the BOSH Director, if the certificate is not verifiable by the local machine's certificate chain.

Once the disks are deleted, continue with [Step 11: Remove Stale Cloud IDs for All Deployments](#).



## Setting Up Your Jumpbox for BBR

Page last updated:

This topic describes how to set up your jumpbox for BOSH Backup and Restore (BBR).

To use BBR to back up and restore your Pivotal Cloud Foundry (PCF) deployment, you must first set up a jumpbox to run BBR from. The Ops Manager VM might be suitable.

### Step 1: Configure your Jumpbox

Configure your jumpbox to meet the following requirements:

- Your jumpbox must have sufficient space for the backup. A PCF backup requires at least 1.5 GB.
- Your jumpbox must exist on the same network as the VMs in your PCF deployment because BBR connects to the VMs at their private IP addresses. BBR does not support SSH gateways.
- Because BBR copies the backed-up data from the VMs to the jumpbox, you should have minimal network latency between them to reduce transfer times.

Consult the following table for more information about the network access permissions required by BBR.

| VM                 | Default Port | Description                                                      |
|--------------------|--------------|------------------------------------------------------------------|
| BOSH Director      | 25555        | BBR interacts with the BOSH Director API.                        |
| Deployed Instances | 22           | BBR uses SSH to orchestrate the backup on the instances.         |
| BOSH Director UAA  | 8443         | BBR interacts with the UAA API for authentication, if necessary. |

### Step 2: Transfer BBR Binary to Your Jumpbox

Perform the following steps to transfer the `bbr` binary to your jumpbox:

1. Download the latest [BOSH Backup and Restore](#) release from Pivotal Network.
2. Extract the `bbr` binary file from the BBR release.
3. To add executable permissions to the `bbr` binary file run the following command:

```
chmod a+x bbr
```

For example:

```
$ chmod a+x bbr
```

4. To securely copy the BBR binary to your jumpbox, run the following command:

```
rsync -Pv -e "ssh -i LOCAL-PATH-TO-JUMPBOX-PRIVATE-KEY" LOCAL-PATH-TO-BINARY-FILE JUMPBOX-USER@JUMPBOX-ADDRESS:
```

Where:

- `LOCAL-PATH-TO-JUMPBOX-PRIVATE-KEY` is the local path to your private key file for the jumpbox host.
- `LOCAL-PATH-TO-BINARY-FILE` is the local path for the binary file.
- `JUMPBOX-USER` is your jumpbox username.
- `JUMPBOX-ADDRESS` is the IP address of your jumpbox.

### Step 3: Ensure BOSH Director Certificate Availability

If the certificate chain on your local machine cannot verify the Certificate Authority (CA) certificate for the BOSH Director, you must have the path to the root CA certificate to run BBR commands.

If you have configured the Ops Manager VM as your jumpbox, the path to the root CA certificate is `/var/tempest/workspaces/default/root_ca_certificate`.

If you have configured another machine as your jumpbox, use the Ops Manager API to download the CA certificate.

1. To download the CA certificate using the Ops Manager API, run the following command:

```
curl -k "https://OPS-MAN-FQDN/api/v0/security/root_ca_certificate" \
-H "Authorization: Bearer UAA-ACCESS-TOKEN" \
|jq --raw-output '.root_ca_certificate_pem' > PATH-TO-BOSH-SERVER-CERTIFICATE
```

Where:

- `OPS-MAN-FQDN` is the fully-qualified domain name (FQDN) for your Ops Manager deployment.
- `UAA-ACCESS-TOKEN` is your UAA access token. For more information, see [Access the API](#).
- `PATH-TO-BOSH-SERVER-CERTIFICATE` is file path location where you want the certificate to be written.

The open source `jq` utility is available to [download](#) [↗](#).



**Note:** See the [Using the Ops Manager API](#) topic to obtain a `UAA-ACCESS-TOKEN` using the UAA CLI.

## Troubleshooting BBR

Page last updated:

This topic lists common troubleshooting scenarios and their solutions when using BOSH Backup and Restore (BBR) to back up and restore Pivotal Cloud Foundry (PCF).

### Troubleshooting During a Restore

This section provides solutions for errors that occur during a restore.

#### Restore Fails with a MySQL Monit Start Timeout

##### Symptom

While running the BBR restore command, restoring the job `mysql-restore` fails with the following error:

```
1 error occurred:

* restore script for job mysql-restore failed on mysql/0.
...
Monit start failed: Timed out waiting for monit: 2m0s
```

##### Explanation

This happens when the MySQL job fails to start within the timeout period. It ends up in an **Execution Failed** state and `monit` never tries to start it again.

##### Solution

Ensure that your MySQL Server cluster has only one instance. If there is more than one instances of MySQL Server, the restore fails with a `monit start` timeout. Scale down to one instance and retry.

If your MySQL Server cluster is already scaled down to one node, it may have taken longer than normal to restart the cluster. Follow the procedure below to manually verify and retry.

1. To list the VMs in your deployment, run the following command:

```
bosh -e BOSH-DIRECTOR-IP --ca-cert /var/tempest/workspaces/default/root_ca_certificate \
-d DEPLOYMENT-NAME \
ssh
```

Where:

- `BOSH-DIRECTOR-IP` is the BOSH Director IP. For how to retrieve this IP address, see [Retrieve BOSH Director Address](#).
- `DEPLOYMENT-NAME` is the deployment name. For how to retrieve the deployment name, see [Identify Your Deployment](#).

2. Locate the `mysql` VM.

3. SSH into the `mysql` VM.

4. To check that the MySQL job process is running, perform one of the following from the `mysql` VM:

- If you selected **Internal Databases - MySQL - Percona XtraDB Cluster** when you configured the PAS tile, run the following command:

```
ps aux | grep galera-init
```

- If you selected **Internal Databases - MySQL - MariaDB Galera Cluster** when you configured the PAS tile, run the following command:

```
ps aux | grep mariadb_ctrl
```

For example:

```
$ ps aux | grep galera-init
```

For more information, see the *Deploying PAS* topic for your IaaS. For example, if you run PAS on AWS, see [Deploying PAS on AWS](#).

5. Run the following command to check that `monit` reports that the MySQL job process is in an **Execution Failed** state:

```
sudo monit summary
```

6. If so, run the following command from the `mysql` VM to disable monitoring:

```
monit unmonitor
```

7. Run the following command to enable monitoring:

```
monit monitor
```

8. After a few minutes, run the following command:

```
monit summary
```

The command should report that all the processes are running.

9. Re-attempt the restore with BBR.

## Deployment Does Not Match the Structure of the Backup

### Symptom

The following error displays:

```
Deployment 'deployment-name' does not match the structure of the provided backup
```

### Explanation

The instance groups with the restore scripts in the destination environment don't match the backup metadata. For example, they may have the wrong number of instances of a particular instance group, or the metadata names an instance group that doesn't exist in the destination environment.

### Solution

BBR only supports restoring to an environment that matches your original environment. Pivotal recommends altering the destination environment to match the structure of the backup.

## General Troubleshooting

This section provides solutions for general errors.

### Connection Error

## Symptom

BBR displays an error message containing “SSH Dial Error” or another connection error.

## Explanation

The jumpbox and the VMs in the deployment are experiencing connection problems.

## Solution

Perform the following steps:

1. To ensure your deployment is healthy, run the following command:

```
bosh vms
```

2. To clean up the data from the failed backup on the instances, run the following command:

```
bbr deployment backup-cleanup
```



**Note:** This step must be performed, otherwise, further BBR commands fail.

3. Repeat the BBR operation.

## Error Running Metadata Script

### Symptom

BBR backup or restore fails with a metadata error:

```
1 error occurred:
error 1:
An error occurred while running metadata script for job redis-server on redis/0ce9f81f-1756-480b-8e3e-a4609b14b6a6: error from metadata
```

### Explanation

There is a problem with your PCF install.

### Solution

Contact [Pivotal Support](#) 

## Using Ops Manager

Ops Manager is a web application that you use to deploy and manage a [Pivotal Cloud Foundry](#) (PCF) PaaS. This is a guide to deploying and using Ops Manager.

## Browser Support

Ops Manager is compatible with current and recent versions of all major browsers. Pivotal recommends using the current version of Chrome, Firefox, or Safari for the best Ops Manager experience.

## Ops Manager API

Use the Ops Manager API to automate any Ops Manager task.

See the [Using Ops Manager API](#) topic to learn how to get started using the [Ops Manager API](#).

## Using Ops Manager and Installed Products

- [Using the Ops Manager Interface](#)
- [Adding and Deleting Products](#)
- [Applying Changes to BOSH Director](#)
- [Retrieving Credentials from Your Deployment](#)
- [Floating Stemcells](#)
- [Configuring BOSH Director on vSphere](#)
- [vSphere Service Account Requirements](#)
- [Creating UAA Clients for BOSH Director](#)
- [Configuring BOSH Director on OpenStack](#)
- [Deploying PAS on vSphere](#)
- [Installing PAS after Deploying Pivotal Cloud Foundry on OpenStack](#)
- [Using Your Own Load Balancer](#)
- [Pivotal Cloud Foundry User Types](#)
- [Creating and Managing Ops Manager User Accounts](#)
- [Creating New PAS User Accounts](#)
- [Logging In to Apps Manager](#)
- [Adding Existing SAML or LDAP Users to a Pivotal Cloud Foundry Deployment](#)
- [Deleting an AWS Installation from the Console](#)
- [Modifying Your Ops Manager Installation and Product Template Files](#)
- [Managing Errands in Ops Manager](#)

## Backing Up

- [Backing Up and Restoring Pivotal Cloud Foundry](#)

## Monitoring, Logging, and Troubleshooting

- [Monitoring Virtual Machines in Pivotal Cloud Foundry](#)
- [Diagnosing Problems in PCF](#)
- [Troubleshooting Problems in PCF](#)

- [Troubleshooting Ops Manager for VMware vSphere](#)
- [Recovering MySQL from PAS Downtime](#)
- [Advanced Troubleshooting with the BOSH CLI](#)

## Using the Ops Manager API

This topic explains how to start using the Ops Manager API.

Platform operators use the Ops Manager API to automate deployments, retrieve and manage credentials, and otherwise work under the hood of the [Ops Manager interface](#).

[Tile developers](#) use the Ops Manager API to test and debug Pivotal Cloud Foundry (PCF) product tiles.

For the complete Ops Manager API documentation, see either of the following:

- <https://docs.pivotal.io/pivotalcf/2-2/opsman-api>
- `https://YOUR-OPS-MANAGER-FQDN/docs`, adding `/docs` to the URL of your Ops Manager

## Requirements

You must install the User Account and Authentication Command Line Interface (UAAC) to perform the procedures in this topic. To install the UAAC, run the following command from a terminal window:

```
$ gem install cf-uaac
```

## Step 1: Authenticate

To use the Ops Manager API, you must authenticate and retrieve a token from the Ops Manager User Account and Authentication (UAA) server. For more information about UAA, see the [User Account and Authentication \(UAA\) Server](#) topic.

Perform the procedures in the [Internal Authentication](#) or [External Identity Provider](#) section below depending on which authentication system you configured for Ops Manager.

### Internal Authentication

If you configured your Ops Manager for Internal Authentication, perform the following procedures specific to your IaaS:

#### vSphere

You need the credentials used to import the PCF .ova or .ovf file into your virtualization system.

1. From a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
2. When prompted, enter the password that you set during the .ova deployment into vCenter. For example:

```
$ ssh ubuntu@my-opsmanager-fqdn.example.com
Password: *****
```

3. Proceed to [Authenticate into Ops Manager](#).

#### AWS, Azure, and OpenStack

1. Locate the Ops Manager FQDN on the AWS [EC2 instances](#) page, Azure [Virtual machines](#) page, or the OpenStack [Access & Security](#) page.
2. Run `chmod 600 ops_mgr.pem` to change the permissions on the `.pem` file to be more restrictive:

```
$ chmod 600 ops_mgr.pem
```

3. Run `ssh -i ops_mgr.pem ubuntu@OPS-MANAGER-FQDN` to SSH into the Ops Manager VM. Replace `OPS-MANAGER-FQDN` with the fully qualified domain



name of Ops Manager. For example:

```
$ ssh -i ops_mgr.pem ubuntu@my-opsmanager-fqdn.example.com
```

4. Proceed to [Authenticate into Ops Manager](#).

## GCP

1. Confirm that you have installed the gcloud CLI. If you do not have the gcloud CLI, see [the Google Cloud Platform documentation](#).
2. Run `gcloud config set project MY-PROJECT` to configure your Google Cloud Platform project. For example:

```
$ gcloud config set project gcp
```

3. Run `gcloud auth login MY-GCP-ACCOUNT`. For example:

```
$ gcloud auth login user@example.com
```

4. Run `gcloud compute ssh MY-INSTANCE --zone MY-ZONE`. For example:

```
$ gcloud compute ssh om-pcf-1a --zone us-central1-b
```

5. Run `sudo su - ubuntu` to switch to the `ubuntu` user.
6. Proceed to [Authenticate into Ops Manager](#).

## Authenticate into Ops Manager

1. After successfully SSHing into the Ops Manager VM, use the UAAC to target your Ops Manager UAA server:

```
$ uaac target https://OPS-MAN-FQDN/uaa
```

2. Retrieve your token to authenticate:

```
$ uaac token owner get
Client ID: opsman
Client secret: [Leave Blank]
User name: OPS-MAN-USERNAME
Password: OPS-MAN-PASSWORD
```

Replace `OPS-MAN-USERNAME` and `OPS-MAN-PASSWORD` with the credentials that you use to log in to the Ops Manager web interface.

## External Identity Provider

If you configured your Ops Manager for an external Identity Provider with SAML, perform the following steps:

1. From your local machine, target your Ops Manager UAA server:

```
$ uaac target https://OPS-MAN-FQDN/uaa
```

2. Retrieve your token to authenticate. When prompted for a passcode, retrieve it from `https://OPS-MAN-FQDN/uaa/passcode`.

```
$ uaac token sso get
Client ID: opsman
Client secret: [Leave Blank]
Passcode: YOUR-PASSCODE
```

If authentication is successful, the UAAC displays the following message: `Successfully fetched token via owner password grant.`

## Step 2: Access the API

Ops Manager uses authorization tokens to allow access to the API. You must pass an access token to the API endpoint in a header that follows the format

```
Authorization: Bearer YOUR-ACCESS-TOKEN .
```

The following example procedure retrieves a list of deployed products. See the [Ops Manager API documentation](#) for the full range of API endpoints.

If you use Internal Authentication, you must perform the following procedures from the Ops Manager VM. If you use an External Identity Provider, you may perform the procedures from your local machine.

1. List your tokens:

```
$ uaac contexts
```

Locate the entry for your Ops Manager FQDN. Under `client_id: opsman`, record the value for `access_token`.

2. Use the `GET /api/v0/deployed/products` endpoint to retrieve a list of deployed products, replacing `UAA-ACCESS-TOKEN` with the access token recorded in the previous step:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

The request produces the following response:

```
[{"installation_name":"p-bosh","guid":"p-bosh-00000000000000000000","type":"p-bosh","product_version":"1.10.0"}, {"installation_name":"cf-00000000000000000000","guid":"cf-00000000000000000000","type":"cf","product_version":"1.10.0"}]
```

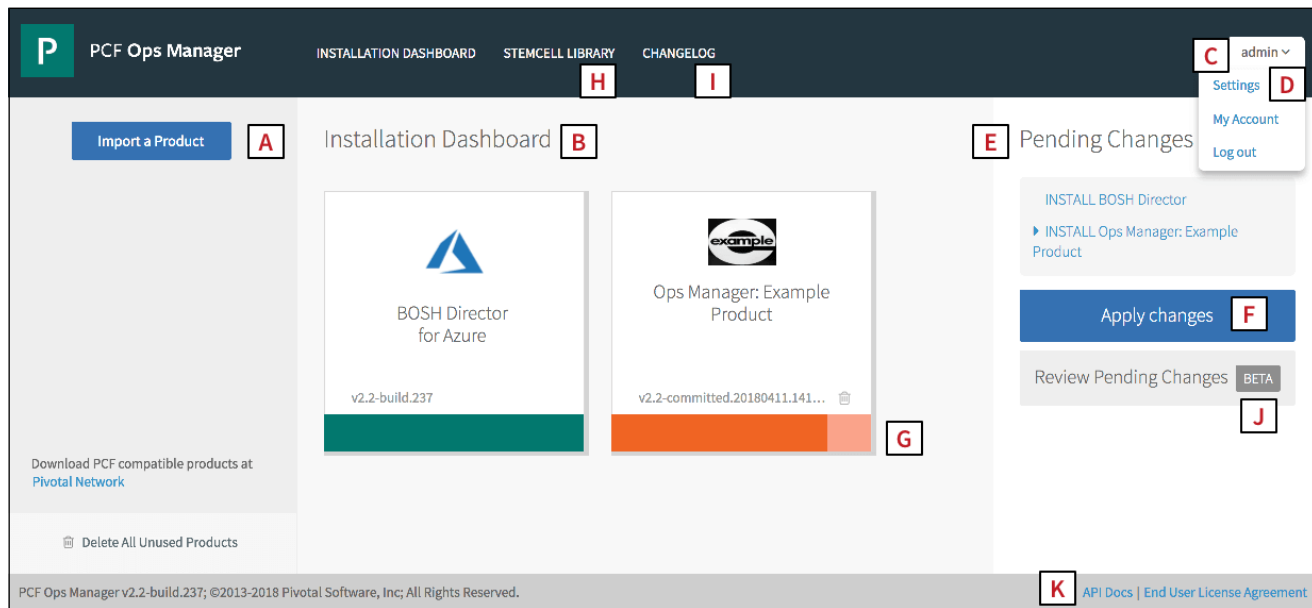
## Using the Ops Manager Interface

Page last updated:

This topic describes key features of the [Pivotal Cloud Foundry](#) (PCF) Operations Manager interface.

### Installation Dashboard Page

The following screenshot shows the Installation Dashboard. Each section is labeled with a red letter. Click the image to see it at full size.

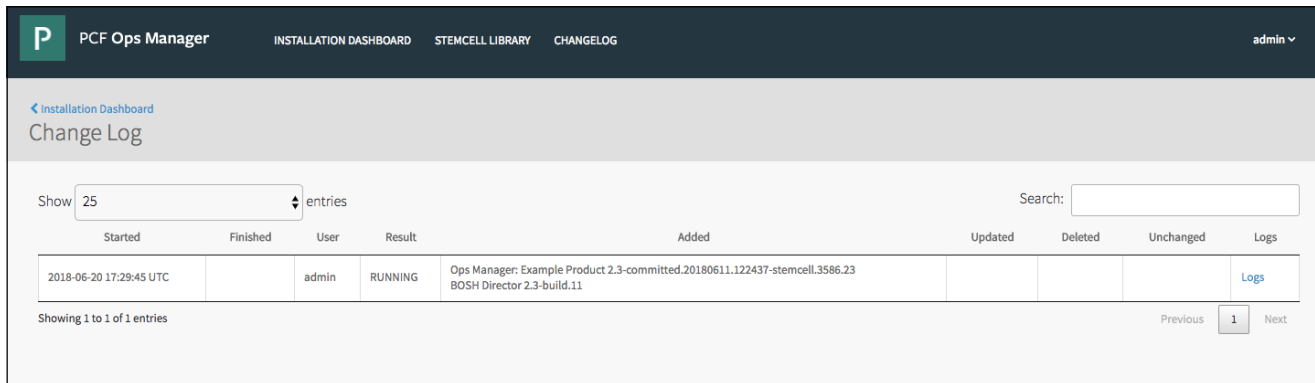


The following list describes each labeled section of the Installation Dashboard:

- **A**— Displays a list of products you have imported that are ready for installation.
  - Click the **Import a Product** link to add a new product to Ops Manager.
  - If an upgrade is available, an active **Upgrade** button appears when you hover over the name of the product. If you are using the [Pivotal Network API](#), the latest version of an existing product appears automatically.
  - Click **Delete All Unused Products** to delete any unused products.
- **B**— **Installation Dashboard**: Displays a product tile for each installed product.
- **C**— **User account menu**: Use this menu to navigate to your **Settings** page, view **My Account** to change your email and password, or log out of the Installation Dashboard.
- **D**— **Settings**: This menu option opens a page with several configuration panes. See the [Settings Page](#) section of this topic for details.
- **E**— **Pending Changes view**: Displays queued products and updates that will install during the next deploy. Click on a product to expand its list of errands and change the errand run rules for the next deploy. For more information, see [Managing Errands in Ops Manager](#).
- **F**— **Apply Changes button**: Click the button to apply pending changes, as listed, to your deployment. Click **Change Log** to view the logs of past installation updates.
- **G**— **Orange bar**: Indicates that additional configuration for the product tile is required before deployment. Click on the product tile to complete its configuration. In addition, the **Apply Changes** button is low lit to indicate that changes cannot be applied without additional product configuration.
- **H**— **Stemcell Library**: Click the link to open the Stemcell Library. In the Stemcell Library you can import stemcells, stage stemcells, and review your stemcell version numbers. For more information, see [Importing and Managing Stemcells](#).
- **I**— **Change Log**: Click the link to view and search a log of your previous installations. See the [Change Log Page](#) section of this topic for details.
- **J**— **Review Pending Changes BETA**: Click the button to go to the “Review Pending Changes” page, which organizes pending changes by tile. You are able to enable or disable each tile to selectively deploy individual tiles. For more information, see [Reviewing Pending Product Changes](#).
- **K**— **API Docs**: Click the link to go to the Ops Manager API documentation, which details how you can manage Ops Manager through the API rather than with the user interface. For more information about the Ops Manager API, see [Using the Ops Manager API](#).

## Change Log Page

Navigate to the **Change Log** page by clicking the corresponding link in the dashboard header. This page lets you view changes between current and past deployments.



The table columns display attributes associated with each deployment:

- **Started:** The date and time, in UTC format, when the deployment began.
- **Finished:** The date and time, in UTC format, when the deployment ended.
- **User:** The user that initiated the deployment.
- **Added:** The tiles that were newly added to the build.
- **Updated:** The tiles that were changed from the previous build.
- **Deleted:** The tiles that were removed from the previous build.
- **Unchanged:** The tiles that were not changed between deployments.
- **Logs:** A link to the Installation Log for the respective entry.

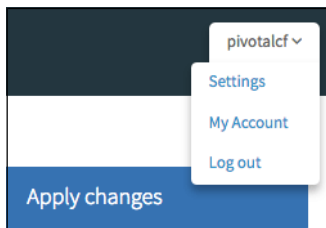
## Using the Change Log Page

Configure the **Change Log** page by modifying the following fields:

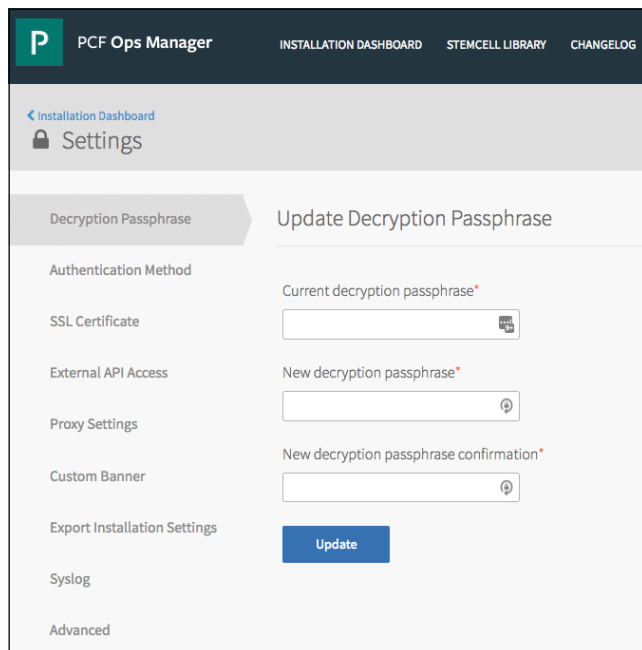
- **Installation Dashboard:** Click **Installation Dashboard** to return to Ops Manager’s Installation Dashboard. Alternatively, click the **Back** button in your web browser.
- **Show X entries:** Click the number displayed in the **Show X entries** dropdown to choose between 10, 25, 50, and 100 entries.
- **Search:** Type in the search box to sort the Change Log page by text or integer matches. As you type, matching entries appear on the screen.
- **Previous / Next:** Click **Previous**, **Next**, or the number between them to load older or newer entries.

## Settings Page

Navigate to the **Settings** page by clicking your user name located at the upper right corner of the screen and selecting **Settings**.



The Settings configuration screen displays the following:



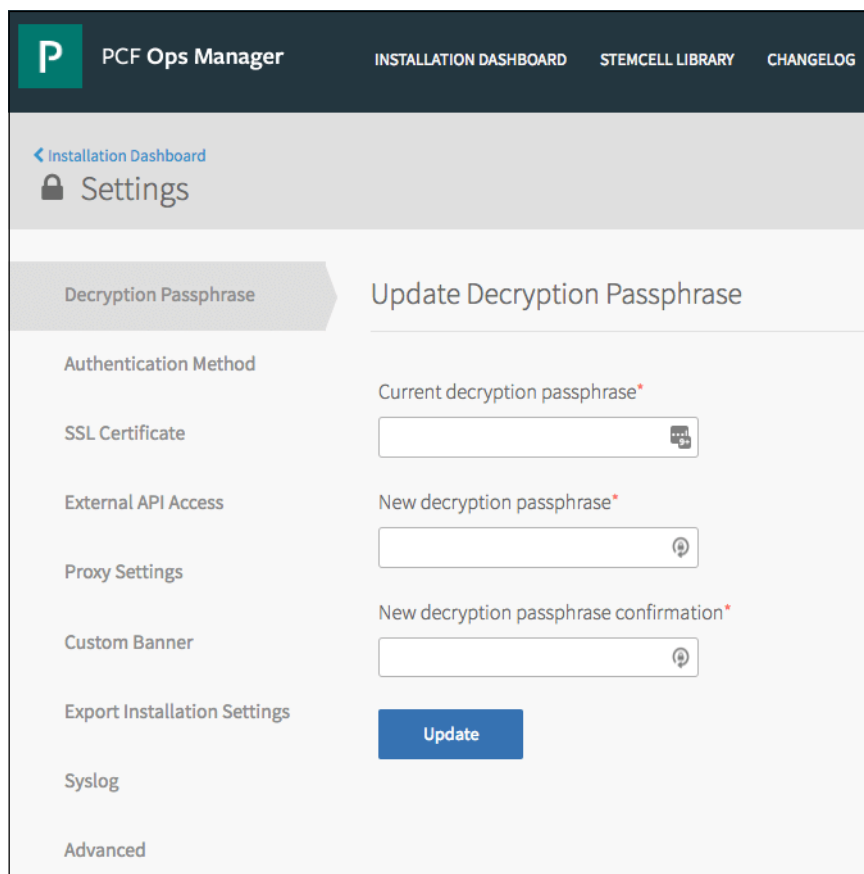
The screenshot shows the PCF Ops Manager interface. The top navigation bar includes the Pivotal logo, 'PCF Ops Manager', and links to 'INSTALLATION DASHBOARD', 'STEMCELL LIBRARY', and 'CHANGELOG'. Below this is a breadcrumb trail: '< Installation Dashboard' followed by 'Settings'. The 'Settings' page has a left sidebar with a list of configuration panes: 'Decryption Passphrase' (highlighted), 'Authentication Method', 'SSL Certificate', 'External API Access', 'Proxy Settings', 'Custom Banner', 'Export Installation Settings', 'Syslog', and 'Advanced'. The main content area is titled 'Update Decryption Passphrase' and contains three input fields: 'Current decryption passphrase\*', 'New decryption passphrase\*', and 'New decryption passphrase confirmation\*'. Each field has a password icon on the right. At the bottom of the form is a blue 'Update' button.

The following sections describe each configuration pane:

**Note:** Modifying these settings does not require you to return to the Installation Dashboard and click **Apply Changes**. These settings apply to the Ops Manager VM. The BOSH Director does not apply them to your PCF deployment.

## Decryption Passphrase

Reset your decryption passphrase by entering your current one and a new one.



This screenshot is identical to the one above, showing the 'Update Decryption Passphrase' form in the PCF Ops Manager Settings. It includes the same navigation elements, sidebar, and form fields: 'Current decryption passphrase\*', 'New decryption passphrase\*', 'New decryption passphrase confirmation\*', and the 'Update' button.

## Authentication Method


You can switch Identity Providers by entering your **Current Decryption Passphrase**, **SAML IDP Metadata**, **SAML Admin Group**, **Groups Attribute**, and optionally, your **BOSH IDP Metadata**. For more information about setting up your SAML Identity Provider, view the following instructions for your configuration:

- Amazon Web Services. See [Configuring BOSH Director on AWS](#).
- Google Cloud Platform. See [Configuring BOSH Director on GCP Manually](#).
- Microsoft Azure. See [Configuring BOSH Director on Azure Manually](#).
- OpenStack. See [Configuring BOSH Director on OpenStack](#).
- vSphere. See [Configuring BOSH Director on vSphere](#).

The screenshot shows the PCF Ops Manager interface. The top navigation bar includes the Pivotal logo, 'PCF Ops Manager', and links to 'INSTALLATION DASHBOARD', 'STEMCELL LIBRARY', and 'CHANGELOG'. Below this is a breadcrumb trail: 'Installation Dashboard' > 'Settings'. The 'Settings' page has a left sidebar with various configuration categories: 'Decryption Passphrase', 'Authentication Method' (which is highlighted), 'SSL Certificate', 'External API Access', 'Proxy Settings', 'Custom Banner', 'Export Installation Settings', 'Syslog', and 'Advanced'. The main content area is titled 'Authentication Settings'. It begins with a message: 'You are currently using Internal Auth as your Identity Provider. To switch to SAML, fill in the following form.' The form contains several fields: 'Current Decryption Passphrase\*' (a text input with a copy icon), 'SAML IDP Metadata\*' (a large text area with a note 'IDP Metadata (Full URL or XML)'), 'BOSH IDP Metadata' (another large text area with a note 'Bosh IDP Metadata (Full URL or XML) - will use same metadata as above if left blank.'), 'SAML Admin Group\*' (a text input), 'Groups Attribute\*' (a text input with a note 'The groups attribute tag name with which you configured the SAML server.'), and a checkbox for 'Provision an admin client in the Bosh UAA'. At the bottom of the form is a blue button labeled 'Setup SAML'.


## External API Access

Enter your [Pivotal Network API](#) token to connect your **Installation Dashboard** to the Pivotal Network.


PCF Ops Manager

[INSTALLATION DASHBOARD](#)
[STEMCELL LIBRARY](#)
[CHANGELOG](#)

[< Installation Dashboard](#)


Settings

Decryption Passphrase
Authentication Method
SSL Certificate
External API Access
Proxy Settings
Custom Banner
Export Installation Settings
Syslog
Advanced

### Pivotal Network Settings


Configure your [Pivotal Network](#) API token to enable update checking.

Set API token

Save


## Proxy Settings

If you are using a proxy to connect to Ops Manager, update your proxy settings by providing a **Http proxy**, **Https proxy**, or **No proxy**.


PCF Ops Manager


[INSTALLATION DASHBOARD](#)
[STEMCELL LIBRARY](#)
[CHANGELOG](#)

[< Installation Dashboard](#)


Settings

Decryption Passphrase
Authentication Method
SSL Certificate
External API Access
Proxy Settings
Custom Banner
Export Installation Settings
Syslog
Advanced

### Update Proxy Settings

Http proxy


Https proxy

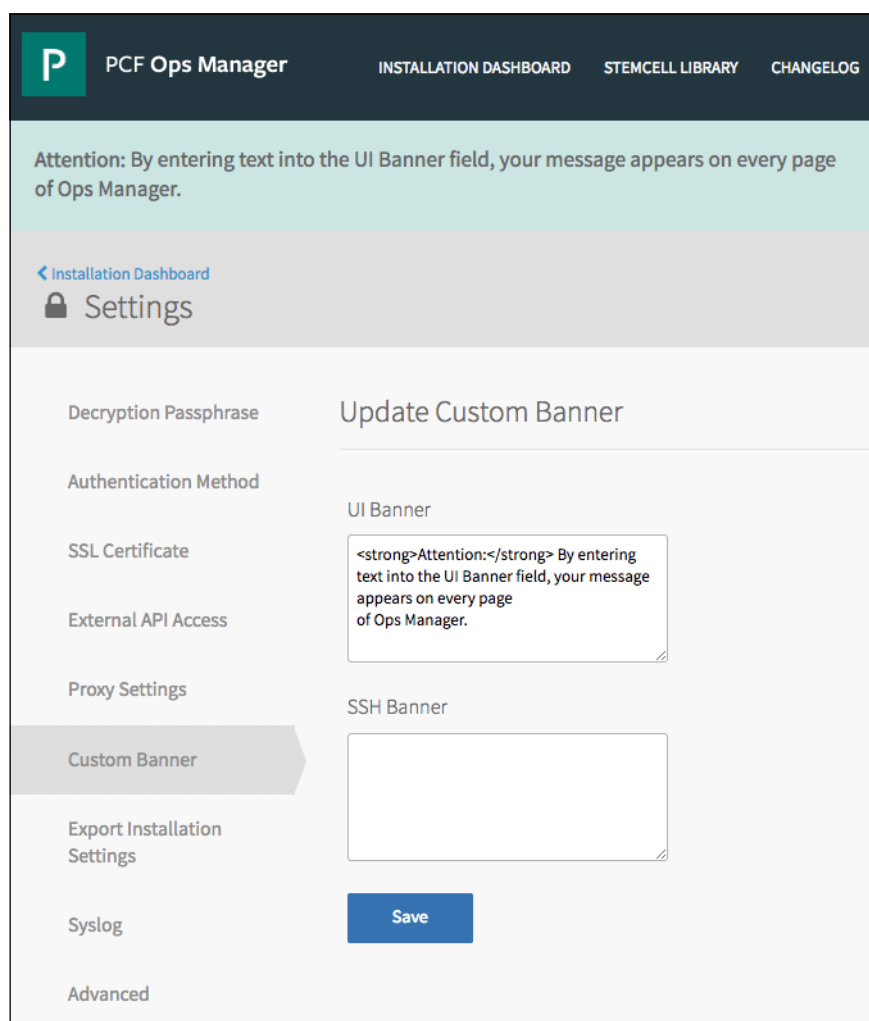
No proxy

Update

## Custom Banner

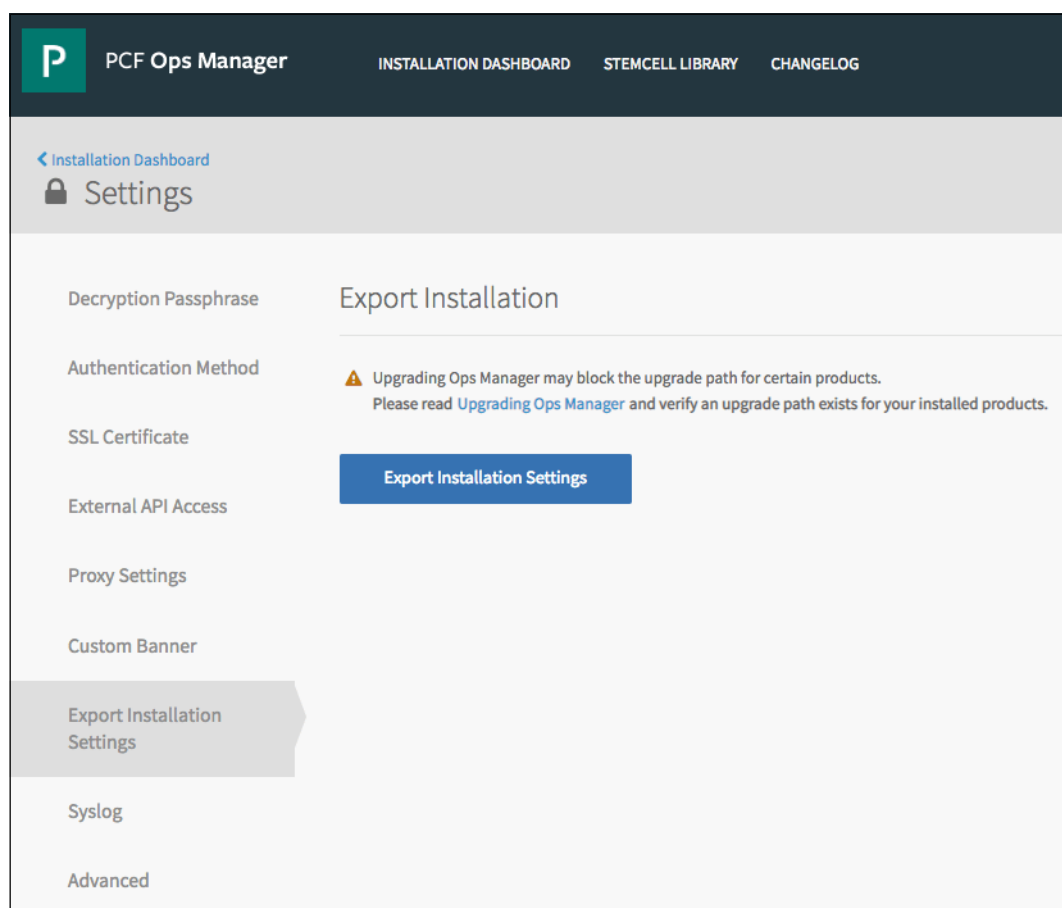
Create a custom text banner to convey your identity or important messages to operators. For **UI Banner**, enter the text you want to be shown on each page of the Ops Manager UI. For **SSH Banner**, enter the text that appears when an operator shells into Ops Manager.





## Export Installation Settings

Exports the current installation with all of its assets. When you export an installation, the exported file contains references to the base VM images, necessary packages, and configuration settings.



## Syslog

Viewable by administrators only. Configure a custom Syslog server for Ops Manager. When you select **Yes** and fill the following fields, Ops Manager produces and sends all Ops Manager logs to the configured Syslog endpoint.

1. Select **Syslog**.

## Syslog

Do you want to configure Syslog for Bosh Director?

☐ No

☒ Yes

Address\*

The address or host for the syslog server

Port\*

Transport Protocol\*

TCP

⬆⬇⬆

☒ Enable TLS

Permitted Peer\*

SSL Certificate\*

Queue Size

Save

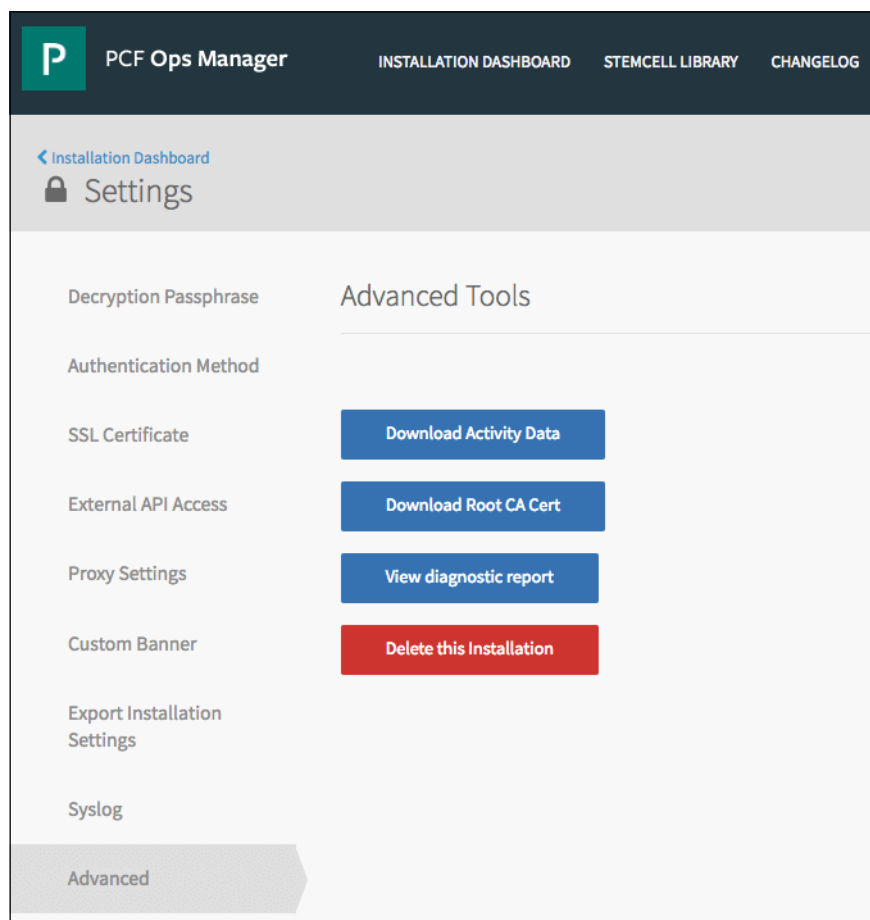
2. (Optional) Select **Yes** to send BOSH Director system logs to a remote server.

3. In the **Address** field, enter the IP address or DNS name for the remote server.
4. In the **Port** field, enter the port number that the remote server listens on.
5. In the **Transport Protocol** dropdown menu, select **TCP**, **UDP**, or **REL**. This selection determines which transport protocol is used to send the logs to the remote server.
6. (Optional) Pivotal strongly recommends that you enable TLS encryption when forwarding logs as they may contain sensitive information. For example, these logs may contain cloud provider credentials. To enable TLS, perform the following steps.
  - In the **Permitted Peer** field, enter either the name or SHA1 fingerprint of the remote peer.
  - In the **SSL Certificate** field, enter the SSL certificate for the remote server.
7. Click **Save**.

## Advanced

The **Advanced** settings pane has the following buttons:

- **Download Activity Data** - Downloads a directory containing the config file for the installation, the deployment history, and version information.
- **Download Root CA Cert** - Downloads the root CA certificate of your deployment as an alternative to curling the Ops Manager API.
- **View diagnostic report** - Displays information about your deployment configuration.
- **Delete this Installation**



## My Account Page

To change your email and password, navigate to the **My Account** page by clicking your user name located at the upper right corner of the screen and selecting **My Account**.

## Account Settings

### Profile

admin@test.org  
\*\*\*\*\*

[Change Email](#)  
[Change Password](#)

### Third Party Access

You have not yet authorized any third party applications.

## Adding and Deleting Products

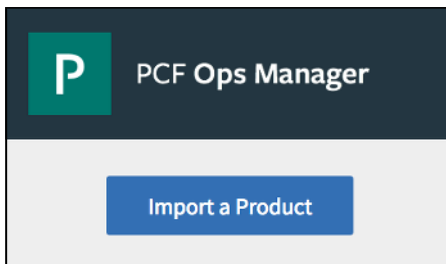
Page last updated:

Refer to this topic for help adding and deleting additional products from your [Pivotal Cloud Foundry](#) (PCF) installation, such as [Pivotal RabbitMQ® for PCF](#).

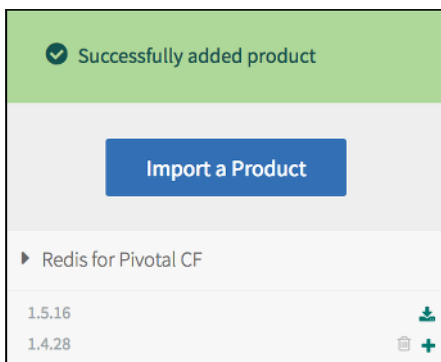
**Note:** In Ops Manager 2.2, all product tiles use floating stemcells by default. This increases the security of your deployment by enabling tiles to automatically use the latest patched version of a stemcell, but it may significantly increase the amount of time required by a tile upgrade. Review the [Floating Stemcells](#) topic for more information.

## Adding and Importing Products

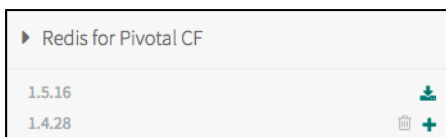
1. Download PCF-compatible products at [Pivotal Network](#). If you cannot download products from Pivotal Network due to restricted network connectivity, see [Installing PCF in Airgapped Environments](#).
2. Navigate to your Ops Manager **Installation Dashboard** and log in.
3. Click **Import a Product**.



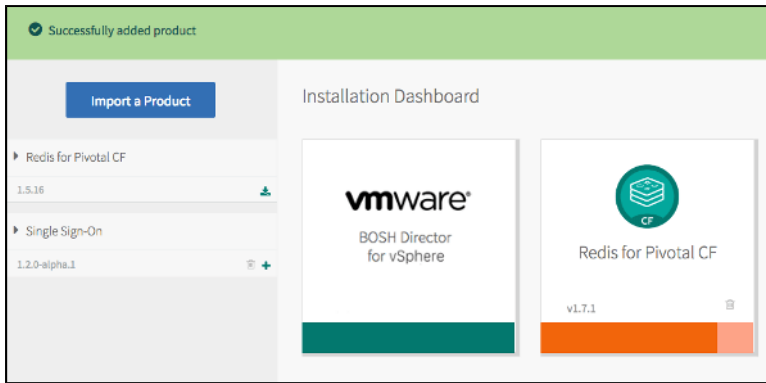
4. Select the .pivotal file that you downloaded from Pivotal Network or received from your software distributor, then click **Open**. If the product is successfully added, it appears in your product list. If the product you selected is not the latest version, the most up-to-date version will appear on your product list.



5. Add the product tile to the **Installation Dashboard** by clicking the green plus sign icon.

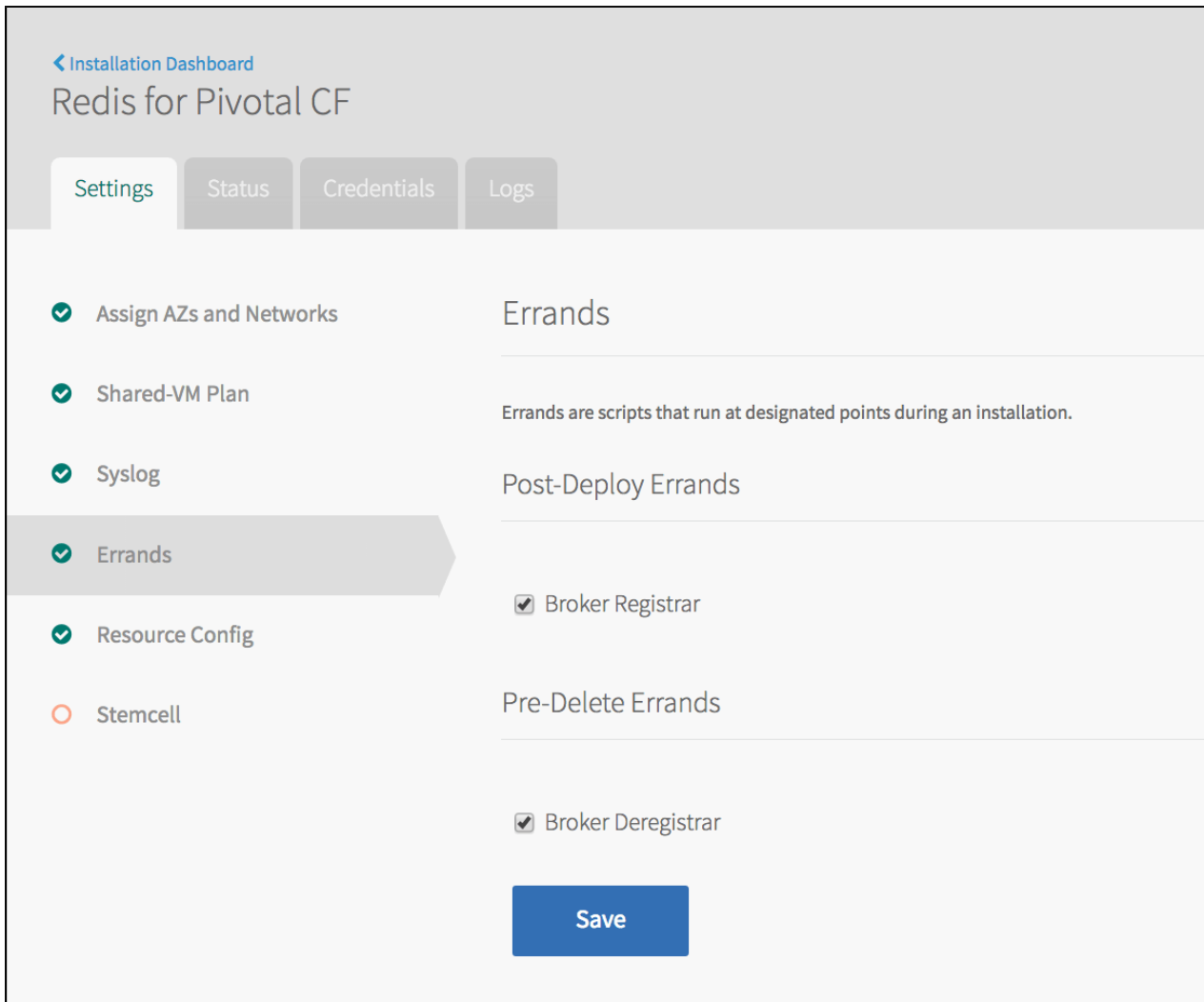


6. The product tile appears in the Installation Dashboard. If the product requires configuration, the tile appears orange. If necessary, configure the product.



7. **(Optional)** In the product configuration view, select the **Errands** pane to configure post-install errands or review the default settings. Post-install errands are scripts that automatically run after a product installs, before Ops Manager makes the product available for use. For more information about post-install errands, see the [Errands](#) topic.

**Note:** By default, Ops Manager reruns errands even if they are not necessary due to settings left from a previous install. Leaving errands checked at all times can cause updates and other processes to take longer. To prevent an errand from running, deselect the checkbox for the errand in the **Settings** tab on the product tile before installing the product.



The **Broker Registrar** checkbox is an example of an errand available for a product. When you select this checkbox, this errand registers service brokers with the Cloud Controller and also updates any broker URL and credential values that have changed since the previous registration.

8. In the Pending Changes view, click **Apply Changes** to start installation and run post-install lifecycle errands for the product.

## Using Pivotal Network API to Upgrade Products

Ops Manager provides a way to upgrade products by connecting your **Installation Dashboard** with Pivotal Network using a API token. Once you have uploaded a [product](#), all subsequent product upgrades appear automatically in your **Installation Dashboard**.

**Note:** Using the Pivotal Network API is only available if you have access to the Internet since communication between Ops Manager and the Pivotal Network is necessary to import your products. If you are on an isolated network, do not save your API token.

1. Navigate to [Pivotal Network](#) and log in.
2. Click your user name, located in the upper top right side of the page.
3. Select **Edit Profile**.

API TOKEN    JW[REDACTED]    [Regenerate](#)

4. In the **Edit Profile** tab, copy your **API Token**.
5. Navigate to your Ops Manager **Installation Dashboard** and log in.
6. Click your user name, located in the upper top right side of the page.
7. Select **Settings**.
8. In the **External API Access** tab, paste your **API Token**.

[Installation Dashboard](#)

**Settings**

Decryption Passphrase
Authentication Method

External API Access

Proxy Settings
Export Installation Settings
Advanced

Pivotal Network Settings

Configure your [Pivotal Network](#) API token to enable update checking.

Set API token

JW[REDACTED]

Save

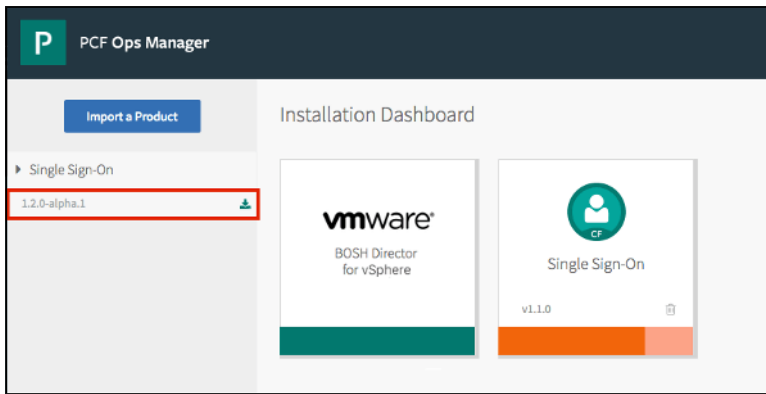
9. Click **Save**.

## Update Existing Products

Once you save the Pivotal Network **API Token** to the Ops Manager **Installation Dashboard**, the latest versions of your existing products will appear in your **Installation Dashboard**. Upgrade your product to the latest version by following these instructions.

1. Locate and download the product version you want to upgrade to by clicking on the green download icon.





2. When the download is complete, refresh the page to use the product.
3. If necessary, configure the product.
4. In the Pending Changes view, click **Apply Changes**.

## Applying Changes to BOSH Director

You can use the Ops Manager API to apply pending changes only to BOSH Director when you stage multiple products in a new installation or as part of an upgrade. For more information, see [Applying Changes to BOSH Director](#).

## Deleting a Product

1. From the Installation Dashboard, click the trash icon on a product tile to remove that product. In the **Delete Product** dialog box that appears, click **Confirm**.

**Note:** You cannot delete the BOSH Director product.

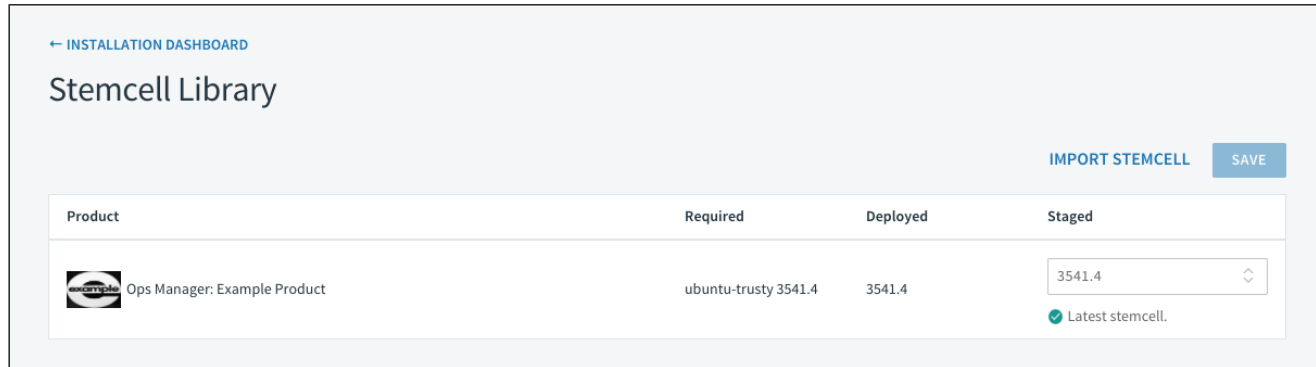
2. In the Pending Changes view, click **Apply Changes**.  
After you delete a product, the product tile is removed from the installation and the Installation Dashboard. However, the product appears in the Available Products view.

## Importing and Managing Stemcells

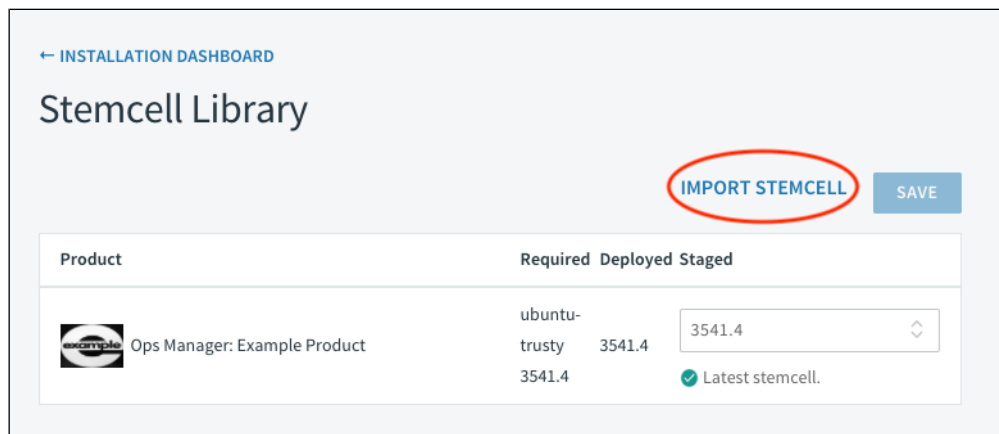
Page last updated:

This topic explains how to use the Stemcell Library introduced in Ops Manager v2.1 to import and stage stemcells to products.

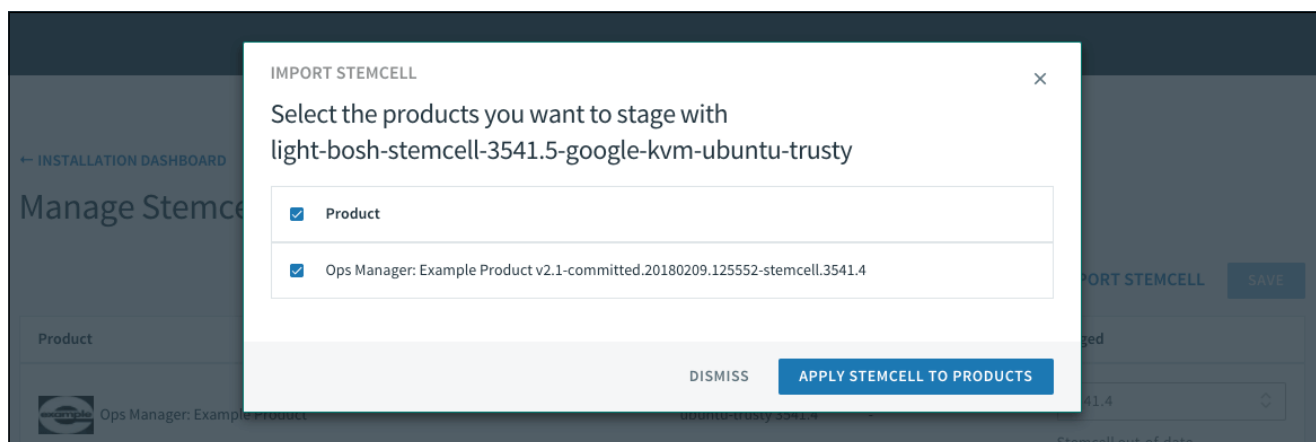
For more conceptual information about floating stemcells and stemcell upgrades, see [Floating Stemcells](#).



### Import and Stage a Stemcell



Download the appropriate .tgz stemcell file from [Pivotal Network](#), then click **Import Stemcell** to permanently import a stemcell into Ops Manager.



To stage your stemcell to compatible products, enable the products in the “Import Stemcell” dialog. Click **Apply Stemcell to Products** to save your selections. Click **Dismiss** to dismiss the “Import Stemcell” dialog.

## Choose a Stemcell Version

If you have uploaded multiple versions of a stemcell, you can use the dropdown menu in the **Staged** column to choose which version to use.

You can choose a different version until you deploy. After deployment, older stemcell versions are no longer available.

|                                                                                   |                                                  |         |         |         |
|-----------------------------------------------------------------------------------|--------------------------------------------------|---------|---------|---------|
|  | Pivotal Cloud Foundry Isolation Segments v1.12.8 | 3345.17 | 3345.17 | 3345.17 |
|  | Pivotal Cloud Foundry Metrics v1.4.2             | 3363.*  | 3363.0  |         |

Available Stemcells  
 3345.30  
 3345.22  
 ✓ 3345.17

If the stemcell displays with a green checkmark and the words “Latest stemcell” below the **Staged** dropdown, the stemcell is the latest available version on your host. An outdated stemcell displays “Stemcell out-of-date.”

|                                                                                   |                                      |        |        |        |
|-----------------------------------------------------------------------------------|--------------------------------------|--------|--------|--------|
|  | Spring Cloud Services for PCF v1.4.7 | 3445.* | 3445.0 | 3445.5 |
|-----------------------------------------------------------------------------------|--------------------------------------|--------|--------|--------|

✓ Latest stemcell.

## Applying Changes to BOSH Director


Page last updated:

This topic describes how to apply pending changes only to the BOSH Director when you stage multiple products in a new installation or as part of an upgrade.

### Overview

After you click **Apply Changes** on the Ops Manager Installation Dashboard, Ops Manager deploys the BOSH Director and all other products that have pending changes. You can optionally apply changes only to the BOSH Director using the Ops Manager API.

To deploy only the BOSH Director, you need to submit the `POST /api/v0/installations` API request. You must include the `deploy_products` parameter in this request and set the value of the parameter to `"none"`.

 **Note:** Submitting the `POST /api/v0/installations` API request is equivalent to clicking **Apply Changes** on the Ops Manager Installation Dashboard.

If you do not include `"deploy_products": "none"` in the `POST /api/v0/installations` request, Ops Manager deploys the BOSH Director and all other products with pending changes.

## Apply Pending Changes to BOSH Director

To apply pending changes only to the BOSH Director, perform the steps below:

1. Ensure your BOSH Director tile is configured. The tile must be green in the Ops Manager Installation Dashboard.
2. Retrieve your authorization token to access the Ops Manager API. Refer to [Using the Ops Manager API](#) for the authentication instructions.
3. Submit the `POST /api/v0/installations` request with the `deploy_products` parameter set to `"none"`. See the following example:

```
$ curl "https://example.com/api/v0/installations" \
-X POST \
-H "Authorization: Bearer UAA-ACCESS-TOKEN" \
-H "Content-Type: application/json" \
-d '{
 "deploy_products": "none",
 "ignore_warnings": true
}'
```

For more information about using the Ops Manager API, browse to the [Ops Manager API documentation](#).

## Creating UAA Clients for BOSH Director

Page last updated:

This topic assumes you are using [BOSH CLI v2+](#).

This topic describes the process of creating a UAA client for the BOSH Director. You must create an automation client to run BOSH from a script or set up a continuous integration pipeline.

To create an automation client, do one of the following:

- [Local Authentication](#): When using Internal Authentication, use the existing admin client to manually create an automation client with the correct privileges.
- [Provision Admin Client](#): When setting up SAML authentication, ensure Ops Manager provisions an admin client.

### Local Authentication

To perform this procedure, the UAAC client must be installed on the Ops Manager virtual machine (VM).


1. Open a terminal and SSH into the Ops Manager VM by following the instructions for your IaaS in the [SSH into Ops Manager](#) topic.
2. Navigate to the Ops Manager **Installation Dashboard** and select the **BOSH Director** tile. In BOSH Director, click the **Status** tab, and record the IP address.
3. Using the `uaac target` command, target BOSH Director UAA on port `8443` using the IP address you copied, and specify the location of the root certificate. The default location is `/var/tempest/workspaces/default/root_ca_certificate`.

```
$ uaac target https://BOSH-DIRECTOR-IP:8443 --ca-cert \
/var/tempest/workspaces/default/root_ca_certificate

Target: https://10.85.16.4:8443
```

Where:


- `BOSH-DIRECTOR-IP` is the IP you recorded in the **Status** tab of the BOSH Director.

 **Note:** You can also curl or point your browser to the following endpoint to obtain the root certificate: `https://OPS-MANAGER-FQDN/api/v0/security/root_ca_certificate`

4. Log in to the BOSH Director UAA and retrieve the owner token. Perform the following step to obtain the values for `UAA-LOGIN-CLIENT-PASSWORD` and `UAA-ADMIN-CLIENT-PASSWORD`:
  - a. Select the **BOSH Director** tile from the Ops Manager **Installation Dashboard**.
  - b. Click the **Credentials** tab, and record the entries for **Uaa Login Client Credentials** and **Uaa Admin User Credentials**.
  - c. For each entry, click **Link to Credential** to obtain the password.

```
$ uaac token owner get login -s UAA-LOGIN-CLIENT-PASSWORD
User name: admin
Password: UAA-ADMIN-CLIENT-PASSWORD

Successfully fetched token via owner password grant.
Target: https://10.85.16.4:8443
Context: admin, from client login
```

 **Note:** To obtain the password for the UAA login and admin clients, you can also curl or point your browser to the following endpoints: `https://OPS-MANAGER-FQDN/api/v0/deployed/director/credentials/uaa_login_client_credentials` and `https://OPS-MANAGER-FQDN/api/v0/deployed/director/credentials/uaa_admin_user_credentials`

5. Create a new UAA Client with `bosh.admin` privileges.

```
$ uaa client add ci --authorized_grant_types client_credentials \
--authorities bosh.admin --secret CI-SECRET
```

```
scope: uaa.none
client_id: ci
resource_ids: none
authorized_grant_types: client_credentials
autoapprove:
action: none
authorities: bosh.admin
name: ci
lastmodified: 1469727130702
id: ci
```

6. Set the client and secret as environment variables on the VM.

```
$ ubuntu@ip-10-0-0-12:~$ export BOSH_CLIENT=ci
$ ubuntu@ip-10-0-0-12:~$ export BOSH_CLIENT_SECRET=CI-SECRET
```

7. Set an alias for the BOSH Director environment.

```
$ bosh alias-env MY-ENVIRONMENT-NAME -e BOSH-DIRECTOR-IP \
--ca-cert /var/tempest/workspaces/default/root_ca_certificate
```

You can now use the UAA client you created to run BOSH in automated or scripted environments, such as continuous integration pipelines.

## Provision Admin Client

Pivotal does not support SAML authentication to the BOSH Director. Ops Manager provides an option to create UAA clients during SAML configuration so that BOSH can be automated using scripts and tooling.

1. Select **Provision an admin client in the Bosh UAA** when configuring Ops Manager for SAML.
2. Click the **Status** tab, and record the IP address, after deploying BOSH Director (BOSH).
3. Click the **Credentials** tab in the BOSH Director tile.
4. Click the link for the **Uaa Bosh Client Credentials** to record the client name and secret.
5. Open a terminal and SSH into the Ops Manager VM. Follow the instructions for your SSH in the [SSH into Ops Manager](#) topic.
6. Set the client and secret as environment variables on the Ops Manager VM. `export BOSH_CLIENT=bosh_admin_client export BOSH_CLIENT_SECRET=UAA-BOSH-CLIENT-SECRET` Where:

- `UAA-BOSH-CLIENT-SECRET` is the client secret you recorded in Step 4. For example:

```
$ ubuntu@ip-10-0-0-12:~$ export BOSH_CLIENT=bosh_admin_client
$ ubuntu@ip-10-0-0-12:~$ export BOSH_CLIENT_SECRET=aBcDeFGhijKabdsadfdfdf
```

7. Set an alias for the BOSH Director environment.

```
$ bosh alias-env MY-ENVIRONMENT-NAME -e BOSH-DIRECTOR-IP \
--ca-cert /var/tempest/workspaces/default/root_ca_certificate
```

Where:

- `BOSH-DIRECTOR-IP` is the IP you recorded in the **Status** tab of the BOSH Director.

## Using Your Own Load Balancer

This guide describes how to use your own load balancer and forward traffic to your Pivotal Application Service (PAS) router IP address.

[Pivotal Cloud Foundry](#) (PCF) includes a tier of reverse proxies that dynamically track the location of application containers and system components, enabling routing of requests to those endpoints even as IPs and ports change.


In order for the PCF Routers to be horizontally scalable and highly available, a load balancer must be deployed in front of them. The simplest solution is to use a layer-4 TCP load balancer, provided by your IaaS or IT team, which passes all HTTP and TLS handling to the PCF Routers. For details on TLS termination, see [Securing Traffic into Cloud Foundry](#). For a description of features supported by the PCF routing tier, see [HTTP Routing](#).

If you have requirements that are not fulfilled by the PCF Routers alone, you can choose to use your own layer-7 load balancer (provided by your IaaS or IT team), or the HAProxy load balancer included with PCF. If you choose to use HAProxy, you must use a layer-4 TCP load balancer in front of it, in order for HAProxy itself to be highly available. Singleton instances of HAProxy are only for use in lab and test environments.

If you choose to use your own layer-7 load balancer, it must fulfill the following requirements:

- Provides load balancing to each of the PCF Router IP addresses
- Supports TLS termination for wildcard hostnames
- Adds appropriate `x-forwarded-for` and `x-forwarded-proto` HTTP headers to incoming requests
- Sets an HTTP keepalive connection timeout greater than five seconds
- (Optional) Supports WebSockets

The choice to use HAProxy or your own load balancer depends on what features you need out of a load balancer, and whether you want the ability to configure it yourself.

 **Note:** Application logging with [Loggregator](#) requires WebSockets. To use another logging service, see the [Using Third-Party Log Management Services](#) topic.

For how to install an [F5 Local Traffic Manager \(LTM\)](#) as a load balancer for PCF and Pivotal Application Service (PAS), see [Configuring an F5 Load Balancer for PAS](#).

## Prerequisites

To integrate your own load balancer with PCF, you must ensure the following:

- WebSocket connections are not blocked for Loggregator functionality.
- The load balancer must be able to reach the Gorouter IP addresses.

Follow the instructions below to use your own load balancer.

## Step 1: Deploy PCF Installation VM

Deploy a PCF Installation virtual machine. See [Deploying Ops Manager on vSphere](#)(../customizing/..om/vsphere/deploy.html) for more information.

## Step 2: Register PCF IP Address

In your load balancer, register the IP addresses that you assigned to PCF.

## Step 3: Configure Pivotal Ops Manager and BOSH Director

Configure your Pivotal Operations Manager and BOSH Director as described in [Installing Pivotal Cloud Foundry](#), then add PAS.

Do not click **Install** after adding PAS.

## Step 4: Configure Networking

Complete the **Networking** configuration page in PAS. Load balancer configuration in PAS varies depending on which IaaS you are using for PCF. See the configuration procedure for your deployment IaaS:

- [AWS](#)
- [Azure](#)
- [GCP](#)
- [OpenStack](#)
- [vSphere](#)

## Step 5: Finalize Changes

1. Return to the **Ops Manager Installation Dashboard**
2. Click **Install**.




## Creating and Managing Ops Manager User Accounts

Page last updated:

[Pivotal Cloud Foundry](#) supports multiple user accounts in Ops Manager. A User Account and Authentication (UAA) module co-located on the Ops Manager VM manages access permissions to Ops Manager.

When Ops Manager boots for the first time, you create an admin user. However, you do not create additional users through the Ops Manager web interface. If you want to create additional users who can log into Ops Manager, you must use the UAA API, either through `curl` or the UAA Command Line Client (UAAC).

 **Note:** You can only manage users on the Ops Manager UAA module if you chose to use Internal Authentication instead of an external Identity Provider when configuring Ops Manager.

Follow these steps to add or remove users via the UAAC. If you do not already have the UAAC installed, run `gem install cf-uaac` from a terminal window.

### Adding Users to Ops Manager

1. Target your Ops Manager UAA:

```
$ uaac target https://YOUR-OPSMAN-FQDN/uaa/
```

2. Get your token:

```
$ uaac token owner get
Client ID: opsmn
Client Secret: [Press Enter]
Username: Admin
Password: *****

Successfully fetched token via client credentials grant.
Target https://YOUR-OPSMAN-FQDN/uaa/
```

3. Add a user:

```
$ uaac user add YOUR-USER-NAME -p YOUR-USER-PASSWORD --emails YOUR-USER-EMAIL@EXAMPLE.COM
```

4. (Optional) Set your user's Role-Based Access Control (RBAC) permissions. For more information, see [Configuring Role-Based Access Control \(RBAC\) in Ops Manager](#).

### Removing Users from Ops Manager

1. Target your Ops Manager UAA:

```
$ uaac target https://YOUR-OPSMAN-FQDN/uaa/
```

2. Get your token:

```
$ uaac token owner get
Client ID: opsmn
Client Secret: [Press Enter]
Username: Admin
Password: *****

Successfully fetched token via client credentials grant.
Target https://YOUR-OPSMAN-FQDN/uaa/
```

3. Delete a user:

```
$ uaac user delete YOUR-USER-NAME
```



## Configuring Role-Based Access Control (RBAC) in Ops Manager

Page last updated:

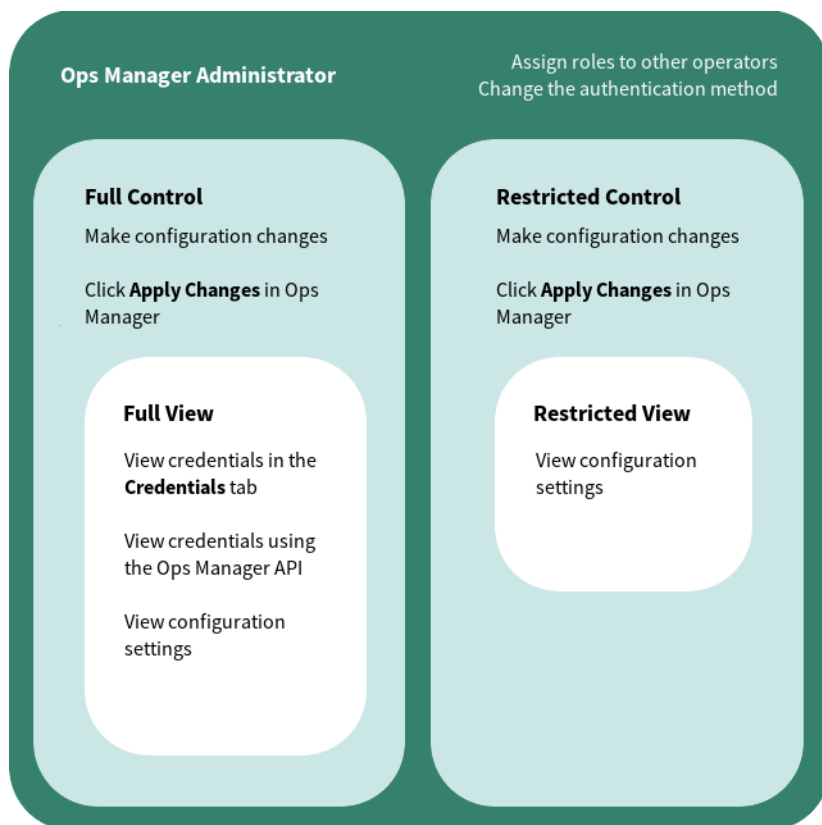
This topic describes how to customize role-based access control (RBAC) in Ops Manager. Use RBAC to manage which operators in your organization can make deployment changes, view credentials, and manage user roles in Ops Manager.

For information about configuring Ops Manager to use internal authentication or SAML authentication, refer to the Ops Manager configuration topic for your IaaS:

- [Configuring BOSH Director on AWS](#)
- [Configuring BOSH Director on Azure Manually](#)
- [Configuring BOSH Director on GCP](#)
- [Configuring BOSH Director on OpenStack](#)
- [Configuring BOSH Director on vSphere](#)

## Understand Roles in Ops Manager

You can assign the following roles to determine which operators in your organization make deployment changes, view credentials, and manage user roles in Ops Manager:



Ops Manager administrators can use the roles defined in the diagram above to meet the security needs of their organization. The roles provide a range of privileges that are appropriate for different types of users. For example, assign either **Restricted Control** or **Restricted View** to an operator to prevent access to all Ops Manager credentials.

See the following table for more information about each role:

| Ops Manager Role          | Role Definition                                                                                                                                                                                                                                   | UAA Scope    |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Ops Manager Administrator | Administrators can make configuration changes and click <b>Apply Changes</b> in Ops Manager, view credentials in the <b>Credentials</b> tab and Ops Manager API endpoints, change the authentication method, and assign roles to other operators. | opsman.admin |

| Ops Manager Role   | Role Definition                                                                                                                                                                                | UAA Scope                 |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Full Control       | Operators can make configuration changes and click <b>Apply Changes</b> in Ops Manager, and view credentials in the <b>Credentials</b> tab and Ops Manager API endpoints.                      | opsman.full_control       |
| Restricted Control | Operators can make configuration changes and click <b>Apply Changes</b> in Ops Manager. They cannot view credentials in the <b>Credentials</b> tab or Ops Manager API endpoints.               | opsman.restricted_control |
| Full View          | Operators can view Ops Manager configuration settings and view credentials in the <b>Credentials</b> tab and Ops Manager API endpoints. They cannot make configuration changes in Ops Manager. | opsman.full_view          |
| Restricted View    | Operators can view Ops Manager configuration settings. They cannot make configuration changes or view credentials in the <b>Credentials</b> tab or Ops Manager API endpoints.                  | opsman.restricted_view    |

When you install a new Ops Manager instance, all existing users have the Ops Manager Administrator role by default.

To assign one of the above roles to an operator, follow the procedure for granting access using either [internal authentication](#) or [SAML authentication](#).

**Note:** Multiple **Restricted View** and **Full View** operators can be logged in to Ops Manager at the same time. However, other roles with write access cannot be logged in simultaneously.

## Enable RBAC in Ops Manager After Upgrade

When you install a new instance of Ops Manager, RBAC is permanently enabled by default.

If your organization has operators who are devoted to managing certain services like MySQL for PCF, you can use RBAC to assign those services operators a more restricted role.

If you upgrade from an older Ops Manager instance, you must enable RBAC and assign roles to users before they can access Ops Manager. If you do not assign any roles to a user, they cannot log in to Ops Manager.

**Warning:** Do not assign roles before you enable RBAC.

## Enable RBAC with Internal Authentication

If you are upgrading from an older version of Ops Manager and use internal authentication, do the following to enable RBAC:

1. Log in to the Ops Manager dashboard.
2. Click **Settings** from the user account menu.
3. Click **Advanced**.
4. Click **Enable RBAC**. When the confirmation dialog box appears, click **Confirm and Logout**.

### Notes:

- Enabling RBAC is permanent. You cannot undo this action. When you upgrade Ops Manager, your RBAC settings remain configured.
- You will not see this dialog box if RBAC is already configured. With new instances of Ops Manager, RBAC is permanently configured by default.

## Enable RBAC with SAML Authentication

If you are upgrading from an older version of Ops Manager and use SAML authentication, perform the steps in this section to enable RBAC. To enable RBAC in Ops Manager when using SAML authentication, you must configure groups in SAML for admins and non-admins and then map the admin group to Ops Manager.


### Step 1: Configure SAML Groups

To gather information from your SAML dashboard, do the following:

1. Log in to your SAML provider dashboard.
2. Create or identify the name of the SAML group that contains Ops Manager admin users.
3. Identify the groups attribute tag you configured for your SAML server.

## Step 2: Enable RBAC in Ops Manager

Perform the steps above in [Enable RBAC with Internal Authentication](#) to configure Ops Manager to recognize your SAML admin user group.

 **Note:** When RBAC is enabled, only users with the Ops Manager Administrator role can edit SAML configuration.

## Create User Accounts in Ops Manager

To assign RBAC roles to operators, you must first create user accounts for them. For more information about creating user accounts in Ops Manager with the User Account and Authentication (UAA) module, see [Creating and Managing Ops Manager User Accounts](#).

## Manage RBAC Roles in Ops Manager

You can assign the roles defined in [Understanding Roles in Ops Manager](#) to determine which operators in your organization make deployment changes, view credentials, and manage user roles in Ops Manager.

## Manage Roles with Internal Authentication

If you configured Ops Manager to use internal authentication, do the following to configure roles using the [UAA Command Line Interface \(UAAC\)](#):

1. Target your UAA server and log in as an admin:

```
uaac target https://YOUR-OPSMAN-DOMAIN/uaa
uaac token owner get
```

2. When prompted, enter the following credentials. Enter `opsman` for **Client ID** and leave **Client secret** blank, then enter your username and password:

```
Client ID: opsman
Client secret:
User name: USERNAME
Password: YOUR-PASSWORD
```

3. Assign one of the following roles to a user, replacing `USERNAME` with their username.

- **Ops Manager Administrator:**

```
uaac member add opsman.admin USERNAME
```

- **Full Control:**

```
uaac member add opsman.full_control USERNAME
```

- **Restricted Control:**

```
uaac member add opsman.restricted_control USERNAME
```

- **Full View:**

```
uaac member add opsman.full_view USERNAME
```

- **Restricted View:**

```
uaac member add opsman.restricted_view USERNAME
```

## Manage Roles with SAML Authentication

If you configured Ops Manager with SAML authentication, do the following to assign non-admin user roles using UAAC:

1. Target your UAA server and log in as an admin:

```
uaac target https://YOUR-OPSMAN-DOMAIN/uaa
uaac token sso get
```

2. When prompted, enter **Client ID** and **Passcode**, leaving **Client secret** blank:

```
Client ID: opsman
Client secret:
Passcode (from http://YOUR-OPSMAN-DOMAIN/uaa/passcode): YOUR-UAA-PASSCODE
```

3. Run the following command:

```
uaac group map SAML-GROUP --name 'OPSMAN-SCOPE' --origin 'saml'
```

Replace the placeholder text as follows:

- **SAML-GROUP** : Replace with name of the SAML group the user belongs to.
- **OPSMAN-SCOPE** : Replace with an Ops Manager UAA scope. Refer to the table in [Understand Roles in Ops Manager](#) to determine which UAA scope to use.

4. Add new and existing users to the appropriate SAML groups in the SAML provider dashboard. Users must log out of both Ops Manager and the SAML provider for role changes to take effect.

# Logging In to Apps Manager

Page last updated:

## Log In as Admin User

Complete the following steps to log in to Apps Manager as the Admin user:

- 1. If you do not know the system domain for the deployment, then select Pivotal Application Service (PAS) **Settings > Domains** to locate the configured system domain.
- 2. Open a browser and navigate to `apps.YOUR-SYSTEM-DOMAIN`. For example, if the system domain is `system.example.com`, then point your browser to `apps.system.example.com`.
- 3. Log in using UAA credentials for the Admin user. To obtain these credentials, refer to PAS **Credentials > UAA > Admin Credentials**.

|     |                   |                                    |
|-----|-------------------|------------------------------------|
| UAA | VM Credentials    | <a href="#">Link to Credential</a> |
|     | Admin Credentials | <a href="#">Link to Credential</a> |

## Adding Existing SAML or LDAP Users to a PCF Deployment

This topic describes the procedure for adding existing SAML or LDAP users to a [Pivotal Cloud Foundry](#) (PCF) deployment enabled with SAML or LDAP.

The following two ways exist to add existing SAML or LDAP users to your PCF deployment:

- [Option 1: Import Users in Bulk](#)
- [Option 2: Add Users Manually](#)

### Prerequisites

You must have the following to perform the procedures in this topic:

- Admin access to the Ops Manager Installation Dashboard for your PCF deployment
- The [Cloud Foundry Command Line Interface](#) (cf CLI) v6.23.0 or later

### Option 1: Import Users in Bulk

You can import SAML or LDAP users in bulk by using the UAA Bulk Import Tool. See [the UAA Users Import README](#) for instructions about installing and using the tool.

### Option 2: Add Users Manually

Perform the procedures below to add existing SAML or LDAP users to your PCF deployment manually.

#### Step 1: Create User

Perform the following steps to add a SAML or LDAP user:

1. Run `cf target https://api.YOUR-SYSTEM-DOMAIN` to target the API endpoint for your PCF deployment. Replace `YOUR-SYSTEM-DOMAIN` with your system domain. For example:

```
$ cf target https://api.example.com
```

2. Run `cf login` and provide credentials for an account with the [Admin user role](#):

```
$ cf login
```

3. Run `cf create-user EXAMPLE-USERNAME --origin YOUR-PROVIDER-NAME` to create the user in UAA. Replace `EXAMPLE-USERNAME` with the username of the SAML or LDAP user you wish to add, and select one of the options below:

- For LDAP, replace `YOUR-PROVIDER-NAME` with `ldap`. For example:

```
$ cf create-user j.smith@example.com --origin ldap
```

- For SAML, replace `YOUR-PROVIDER-NAME` with the name of the SAML provider you provided when configuring Ops Manager. For example:

```
$ cf create-user j.smith@example.com --origin example-saml-provider
```

#### Step 2: Associate User with Org or Space Role

After creating the SAML or LDAP user, you must associate the user with either an Org or Space role.

For more information about roles, see the [Roles and Permissions](#) section of the *Orgs, Spaces, Roles, and Permissions* topic.



## Associate User with Org Role

Run `cf set-org-role USERNAME YOUR-ORG ROLE` to associate the SAML or LDAP user with an Org role. Replace `USERNAME` with the name of the SAML or LDAP user, and replace `YOUR-ORG` with the name of your Org.

For `ROLE`, enter one of the following:

- `OrgManager`: Org Managers can invite and manage users, select and change plans, and set spending limits.
- `BillingManager`: Billing Managers can create and manage the billing account and payment information.
- `OrgAuditor`: Org Auditors have read-only access to Org information and reports.

Example:

```
$ cf set-org-role j.smith@example.com my-org OrgManager
```

## Associate User with Space Role

Run `cf set-space-role USERNAME YOUR-ORG YOUR-SPACE ROLE` to associate the SAML or LDAP user with a Space role. Replace `USERNAME` with the name of the SAML or LDAP user, replace `YOUR-ORG` with the name of your Org, and `YOUR-SPACE` with the name of a Space in your Org.

For `ROLE`, enter one of the following:

- `SpaceManager`: Space Managers can invite and manage users, and enable features for a given Space.
- `SpaceDeveloper`: Space Developers can create and manage apps and services, and see logs and reports.
- `SpaceAuditor`: Space Auditors can view logs, reports, and settings on this Space.

Example:

```
$ cf set-space-role j.smith@example.com my-org my-space SpaceDeveloper
```

## Modifying Your Ops Manager Installation and Product Template Files

Page last updated:

This topic describes how to modify your Ops Manager installation by decrypting and editing the YAML files that Ops Manager uses to store configuration data. Operators can use these procedures to view and change values that they cannot access through the Ops Manager web interface. They can also modify the product templates that Ops Manager uses to create forms and obtain user input.

Operators may want to modify the Ops Manager installation and product template files for a number of reasons, including the following:

- To change the User Account and Authentication (UAA) admin password of their deployment
- To retrieve key values
- To migrate content across different Pivotal Cloud Foundry (PCF) releases

**⚠ warning:** Be careful when making changes to your Ops Manager installation and product template files. Use spaces instead of tabs, and remember that YAML files use whitespace as a delimiter. Finally, Pivotal does not officially support these procedures, so use them at your own risk.

## Understand Installation and Product Template Files

During the installation process, Ops Manager combines information from the installation and product template files to generate the manifests that define your deployment.

- **Installation files:** PCF stores user-entered data and automatically generated values for Ops Manager in installation YAML files on the Ops Manager virtual machine (VM). PCF encrypts and stores these files in the directory `/var/tempest/workspaces/default`. You must decrypt the files to view their contents, edit them as necessary, then re-encrypt them.
- **Product templates:** Ops Manager uses product templates to create forms and obtain user input. The `job_types` and `property_blueprint` key-value pairs in a product template determine how the `jobs` and `properties` sections display in the installation file. Ops Manager stores product templates as YAML files in the directory `/var/tempest/workspaces/default/metadata` on the Ops Manager VM. These files are not encrypted, so you can edit them without decrypting. User input does not alter these files.

**💡 Note:** Upgrading Ops Manager may eliminate your changes to the installation and product template files.

## Modify the Installation Files

Perform the following steps to locate, decrypt, and edit the Ops Manager installation files `installation.yml` and `actual-installation.yml`.

1. SSH into the Ops Manager VM by following the steps in the [SSH into Ops Manager](#) section of the *Advanced Troubleshooting with the BOSH CLI* topic.
2. On the command line, navigate to the scripts directory:

```
$ cd /home/tempest-web/tempest/web/scripts/
```

3. Run the following command to decrypt the installation YAML file and make a temporary copy of the decrypted file. When prompted for a passphrase, enter the decryption passphrase you created when you launched Ops Manager for the first time:

```
$ sudo -u tempest-web ./decrypt /var/tempest/workspaces/default/installation.yml /tmp/installation.yml
```

4. Open `/tmp/installation.yml` to view or edit values.
5. If you plan to make changes, make a backup of the original installation YAML file:

```
$ cp /var/tempest/workspaces/default/installation.yml ~/installation-orig.yml
```

6. If you have made changes to your copy of the installation YAML file, you must encrypt it and overwrite the original with it:

```
$ sudo -u tempest-web RAILS_ENV=production /home/tempest-web/tempest/web/scripts/encrypt /tmp/installation.yml /var/tempest/workspaces/default/installation.yml
```

When prompted, enter a passphrase.

7. Delete the temporary copy of the decrypted file:

```
$ rm /tmp/installation.yml
```

8. Repeat steps 2 through 7 for `/tmp/actual-installation.yml`. Each step you see `installation.yml`, replace with `actual-installation.yml`. For example, for step 3 you run:

```
$ sudo -u tempest-web ./decrypt /var/tempest/workspaces/default/actual-installation.yml /tmp/actual-installation.yml
```

9. Restart the Ops Manager web interface:

```
$ sudo service tempest-web stop && sudo service tempest-web start
```

10. Navigate to Ops Manager in a browser and enter your decryption passphrase.
11. Log in to Ops Manager and click **Apply Changes**.
12. If Ops Manager cannot load your changes, see the [Revert To Your Backup](#) section of this topic to restore your previous settings.

## Modify Product Template Files

Perform the following steps to locate and edit your Ops Manager product template files:

1. SSH into the Ops Manager VM by following the steps in the [SSH into Ops Manager](#) section of the *Advanced Troubleshooting with the BOSH CLI* topic.
2. On the Ops Manager VM, navigate to the `/var/tempest/workspaces/default/metadata` directory.

```
$ cd /var/tempest/workspaces/default/metadata
```

3. The `/var/tempest/workspaces/default/metadata` directory contains the product templates as YAML files. If you plan to make changes, make a backup of the original product template YAML file:

```
$ cp /var/tempest/workspace/default/metadata/YOUR-PRODUCT-TEMPLATE.yml ~/YOUR-PRODUCT-TEMPLATE-orig.yml
```

4. Open and edit the product template YAML file as necessary. For more information about product templates, see the [Product Template Reference](#) [↗](#) topic.
5. Navigate to Ops Manager to see your changes.
6. If Ops Manager cannot load your changes, see the [Revert To Your Backup](#) section of this to restore your previous settings.

## Revert to Your Backup

Perform the following steps to revert to your backup of an installation or product template file:

1. SSH into the Ops Manager VM by following the steps in the [SSH into Ops Manager](#) section of the *Advanced Troubleshooting with the BOSH CLI* topic.
2. Overwrite the modified file with the backup:

- For the installation file, run the following command:

```
$ cp ~/installation-orig.yml /var/tempest/workspaces/default/installation.yml
```

- For a product template file, run the following command:

```
$ cp ~/YOUR-PRODUCT-TEMPLATE-orig.yml /var/tempest/workspaces/default/metadata/YOUR-PRODUCT-TEMPLATE.yml
```

3. Restart the Ops Manager web interface:

```
$ sudo service tempest-web stop && sudo service tempest-web start
```

4. Navigate to Ops Manager in a browser and enter your decryption passphrase.
5. Log in to Ops Manager and click **Apply Changes**.

## Managing Errands in Ops Manager

Page last updated:

This topic describes product errands and how to configure them in Pivotal Cloud Foundry (PCF) Ops Manager.

Errands are scripts that can run at the beginning and at the end of an installed product's availability time. You can use Ops Manager to adjust whether and when these errands run.

Product tiles include two types of errands:

- **Post-deploy errands** run after the product installs but before Ops Manager makes the product available for use. One example is an errand that publishes a newly-installed service to the Services Marketplace.
- **Pre-delete errands** run after an operator chooses to delete the product but before Ops Manager actually deletes it. One example is a clean-up task that removes all data objects used by the errand.

When you click **Apply Changes** in Ops Manager, BOSH either creates a VM for each errand that runs or co-locates errands on existing VMs. Tile developers determine where BOSH deploys the errands for their product.

Pivotal Application Service (PAS) provides several post-deploy errands including smoke tests, Apps Manager, notification, Pivotal Account, and autoscaling errands. For more information about PAS errands, see the *Deploying PAS* topic for the platform where you are deploying PAS. For example, if you are deploying PAS on GCP, see [Deploying PAS on GCP](#).

For information about the errands associated with any other PCF product, see the documentation provided with the product tile.

## Errand Run Rules

Operators can configure two different run rules for errands: **On** and **Off**. These rules control when Ops Manager executes the errand.

When the errand is configured to be **On**, then it always runs, even if there are no changes to the product manifest. When the errand is configured to be **Off**, it never runs.

## Ops Manager Defaults and Tile Defaults

By default, Ops Manager applies the **On** rule to all errands.

For any errand, the tile developer can override these Ops Manager defaults with their own tile-specific defaults defined in the tile [property blueprints](#).

## Configure Run Rules in Ops Manager

You can configure the run rules for errands in two places in Ops Manager. The [Errands](#) pane saves your configuration and applies the configuration to future installations. The [Pending Changes](#) view applies the rules only to the next time you run an Ops Manager install, without saving them.

## Errands Pane: Persistent Rules

Product tiles for PAS and other PCF products have an **Errands** pane that configures the run rules for the product's errands and saves the settings for later.

The **Errands** pane lists all errands for the product and lets you select **On** or **Off**. The [default](#) option differs depending on the errand, and reflects the default setting used by Ops Manager for the errand or any tile-specific default that overrides it.

## Errands

Errands are scripts that run at designated points during an installation.

### Post-Deploy Errands

|                                             |                                                                                                                                          |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Smoke Test Errand                           | Runs Smoke Tests against your Application Service installation                                                                           |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| Usage Service Errand                        | Pushes the Pivotal Usage Service application to your Application Service installation. Pivotal Apps Manager depends on this application. |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| Apps Manager Errand                         | Pushes the Pivotal Apps Manager application to your Application Service installation                                                     |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| Notifications Errand                        | Pushes the Pivotal Notifications application to your Application Service installation                                                    |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| Notifications UI Errand                     | Pushes the Notifications UI component to your Application Service installation                                                           |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| App Autoscaler Errand                       | Pushes the Pivotal App Autoscaler application to your Application Service installation                                                   |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| App Autoscaler Smoke Test Errand            | Runs Smoke Tests against the App Autoscaling Service.                                                                                    |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| NFS Broker Errand                           | Pushes the NFS Broker application to your Application Service installation                                                               |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |
| Delete Pivotal Account Application          | Deletes the Pivotal Account Application from your Application Service installation                                                       |
| <input type="button" value="Default (On)"/> |                                                                                                                                          |

There are no pre-delete errands for this product.

Save

To configure the run rules for a tile, do the following:

1. Navigate to Ops Manager and click the tile to open it.
2. Under the **Settings** tab, open the **Errands** pane.
3. Use the dropdowns to configure the run rule choice for each errand: **On** or **Off**.
4. Click **Save** to save the configuration values and return to the Installation Dashboard.
5. Click **Apply Changes** to redeploy the tile with the new settings.

## Pending Changes: One-Time Rules

Ops Manager lets you quickly configure one-time errand run rules for any product queued up for installation:

1. Navigate to Ops Manager. The **Pending Changes** section at top right shows products that Ops Manager has yet to install or update.

- Under **Pending Changes**, click the product you wish to configure. A list of errands associated with the product appears.

## Pending Changes

Revert

INSTALL Ops Manager Director

▼ INSTALL Pivotal Elastic Runtime

Smoke Test Errand

Usage Service Errand

Apps Manager Errand

Notifications Errand

Notifications UI Errand

Pivotal Account Errand

Autoscaling Errand

Autoscaling Registration Errand

NFS Broker Errand

Default

Default

Default

Default

Default

Default

Default

Default

Default

INSTALL PCF Isolation Segment

▶ INSTALL PCF Runtime For Windows

Apply changes

Changelog

- Use the dropdowns to configure the [run rule](#) choice for each errand: **On** or **Off**. Ops Manager applies these settings once you click **Apply changes** to install the product, but does not save the settings for future installations.
- Click **Apply Changes** to redeploy the tile.

## Related Links

If you are a product developer and want to learn more about adding errands to your product tile for PCF, see the [Errands](#) topic in the *PCF Tile Developer Guide*.

## Monitoring PCF VMs from Ops Manager

Page last updated:

This topic describes how to check current VM status in Pivotal Cloud Foundry (PCF) Ops Manager.

For a complete guide to monitoring PCF, see [Monitoring Pivotal Cloud Foundry](#).

## Monitoring VMs Using the Ops Manager Interface

Click any product tile and select the **Status** tab to view monitoring information.

| JOB     | INDEX | IPS        | CID                                     | LOAD AVG15 | CPU  | MEMORY | SWAP | SYSTEM DISK | EPHEM. DISK | PERS. DISK | LOGS |
|---------|-------|------------|-----------------------------------------|------------|------|--------|------|-------------|-------------|------------|------|
| HAProxy | 0     | 10.0.0.254 | vm-9985a13c-106a-48d1-a3de-d0e0e816c857 | 0.06%      | 0.1% | 9.6%   | 0.0% | 41%         | 5%          | N/A        |      |
| NATS    | 0     | 10.0.0.5   | vm-dee49615-aea8-4f4f-bf0f-b1060083ddef | 0.12%      | 0.1% | 9.7%   | 0.0% | 41%         | 21%         | N/A        |      |
|         |       |            | vm-6d43e59e-                            |            |      |        |      |             |             |            |      |


The columns display the following information:

| VM Data Point | Details                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job           | Each job represents a component running on one or more VMs that Ops Manager deployed.                                                                                                                                    |
| Index         | For jobs that run across multiple VMs, the <code>index</code> value indicates the order in which the job VMs were deployed. For jobs that run on only one VM, the VM has an <code>index</code> value of <code>0</code> . |
| IPs           | IP address of the job VM.                                                                                                                                                                                                |
| CID           | Uniquely identifies the VM.                                                                                                                                                                                              |
| Load Avg15    | CPU load average over 15 minutes.                                                                                                                                                                                        |
| CPU           | Current CPU usage.                                                                                                                                                                                                       |
| Memory        | Current memory usage.                                                                                                                                                                                                    |
| Swap          | Swap file percentage.                                                                                                                                                                                                    |
| System Disk   | System disk space usage.                                                                                                                                                                                                 |
| Ephem. Disk   | Ephemeral disk space usage.                                                                                                                                                                                              |
| Pers. Disk    | Persistent disk space usage.                                                                                                                                                                                             |
| Logs          | Download link for the most recent log files.                                                                                                                                                                             |

## Operations Manager VM Disk Space

The Ops Manager stores its logs on the Ops Manager VM in the `/tmp` directory.



 **Note:** The logs collect over time and do not self-delete. To prevent the VM from running out of disk space, restart the VM to clear the log entries from `/tmp`.

## PAS Concepts

Pivotal Application Service (PAS) is based on Cloud Foundry, which is an open source cloud application platform, providing a choice of clouds, developer frameworks, and application services. Cloud Foundry makes it faster and easier to build, test, deploy, and scale applications. It is an [open source project](#) and is available through a variety of private cloud distributions and public cloud instances.

This guide presents an overview of how Cloud Foundry works and a discussion of key concepts. Refer to this guide to learn more about Cloud Foundry fundamentals.

## General Concepts

- [Cloud Foundry Overview](#)
- [How Apps Are Staged](#)
- [High Availability in Cloud Foundry](#)
- [Orgs, Spaces, Roles, and Permissions](#)
- [Application Security Groups](#)
- [Cloud Foundry Security](#)
- [Container Security](#)
- [Container-to-Container Networking](#)
- [GrootFS Disk Usage](#)

## Architecture

- [Cloud Foundry Components](#)
- [Cloud Controller](#)
- [Messaging \(NATS\)](#)
- [Gorouter](#)
- [User Account and Authentication \(UAA\) Server](#)
- [Garden](#)
- [HTTP Routing](#) [↗](#)

## Diego

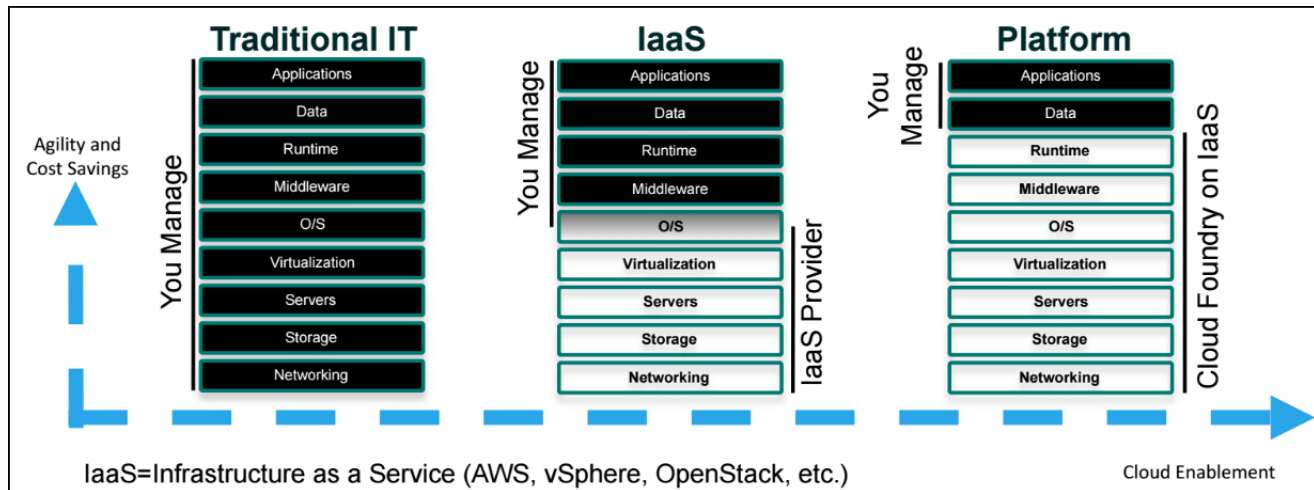
- [Diego Architecture](#)
- [Application SSH Components and Processes](#)
- [How the Diego Auction Allocates Jobs](#)

## Cloud Foundry Overview

Page last updated:

### The Industry-Standard Cloud Platform

Cloud platforms let anyone deploy network apps or services and make them available to the world in a few minutes. When an app becomes popular, the cloud easily scales it to handle more traffic, replacing with a few keystrokes the build-out and migration efforts that once took months. Cloud platforms represent the next step in the evolution of IT, enabling you to focus exclusively on your applications and data without worrying about underlying infrastructure.



Not all cloud platforms are created equal. Some have limited language and framework support, lack key app services, or restrict deployment to a single cloud. Cloud Foundry (CF) has become the industry standard. It is an [open source](#) platform that you can deploy to run your apps on your own computing infrastructure, or deploy on an IaaS like AWS, vSphere, or OpenStack. You can also use a PaaS deployed by a commercial [CF cloud provider](#). A broad [community](#) contributes to and supports Cloud Foundry. The platform's openness and extensibility prevent its users from being locked into a single framework, set of app services, or cloud.

Cloud Foundry is ideal for anyone interested in removing the cost and complexity of configuring infrastructure for their apps. Developers can deploy their apps to Cloud Foundry using their existing tools and with zero modification to their code.

### How Cloud Foundry Works

To flexibly serve and scale apps online, Cloud Foundry has subsystems that perform specialized functions. Here's how some of these main subsystems work.

#### How the Cloud Balances Its Load

Clouds balance their processing loads over multiple machines, optimizing for efficiency and resilience against point failure. A Cloud Foundry installation accomplishes this at three levels:

1. [BOSH](#) creates and deploys virtual machines (VMs) on top of a physical computing infrastructure, and deploys and runs Cloud Foundry on top of this cloud. To configure the deployment, BOSH follows a manifest document.
2. The CF [Cloud Controller](#) runs the apps and other processes on the cloud's VMs, balancing demand and managing app lifecycles.
3. The [router](#) routes incoming traffic from the world to the VMs that are running the apps that the traffic demands, usually working with a customer-provided load balancer.

#### How Apps Run Anywhere

Cloud Foundry designates two types of VMs: the component VMs that constitute the platform's infrastructure, and the host VMs that host apps for the

outside world. Within CF, the Diego system distributes the hosted app load over all of the host VMs, and keeps it running and balanced through demand surges, outages, or other changes. Diego accomplishes this through an auction algorithm.

To meet demand, multiple host VMs run duplicate instances of the same app. This means that apps must be portable. Cloud Foundry distributes app source code to VMs with everything the VMs need to compile and run the apps locally. This includes the OS [stack](#) that the app runs on, and a [buildpack](#) containing all languages, libraries, and services that the app uses. Before sending an app to a VM, the Cloud Controller [stages](#) it for delivery by combining stack, buildpack, and source code into a droplet that the VM can unpack, compile, and run. For simple, standalone apps with no dynamic pointers, the droplet can contain a pre-compiled executable instead of source code, language, and libraries.

## How CF Organizes Users and Workspaces

CF manages user accounts through two [User Authentication and Authorization](#) (UAA) servers, which support access control as [OAuth2](#) services and can store user information internally, or connect to external user stores through LDAP or SAML.

One UAA server grants access to BOSH, and holds accounts for the CF operators who deploy runtimes, services, and other software onto the BOSH layer directly. The other UAA server controls access to the Cloud Controller, and determines who can tell it to do what. The Cloud Controller UAA defines different user roles, such as admin, developer, or auditor, and grants them different sets of privileges to run CF commands. The Cloud Controller UAA also scopes the roles to separate, compartmentalized [Orgs and Spaces](#) within an installation, to manage and track use.

## Where CF Stores Resources

Cloud Foundry uses the git system on [GitHub](#) to version-control source code, buildpacks, documentation, and other resources. Developers on the platform also use GitHub for their own apps, custom configurations, and other resources. To store large binary files, such as droplets, CF maintains an internal or external blobstore. To store and share temporary information, such as internal component states, CF uses MySQL and [Consul](#).

## How CF Components Communicate

Cloud Foundry components communicate in two of the following ways:

- By sending messages internally using HTTP and HTTPS protocols
- By sending [NATS](#) messages to each other directly

BOSH Director colocates a BOSH DNS server on every deployed VM. All VMs keep up-to-date DNS records for all the other VMs in the same foundation. This enables service discovery between VMs.

BOSH DNS allows deployments to continue communicating with VMs even when the VMs' IP addresses change. It also provides client-side load-balancing by randomly selecting a healthy VM when multiple VMs are available.

For more information about BOSH DNS, see [Native DNS Support](#) in the BOSH documentation.

## How to Monitor and Analyze a CF Deployment

Cloud Foundry generates system logs from Cloud Foundry components and app logs from hosted apps.

As Cloud Foundry runs, its component and host VMs generate logs and metrics. Cloud Foundry apps also typically generate logs. The [Loggregator](#) system aggregates the component metrics and app logs into a structured, usable form, the *Firehose*. You can use all of the output of the Firehose, or direct the output to specific uses, such as monitoring system internals, triggering alerts, or analyzing user behavior, by applying *nozzles*.

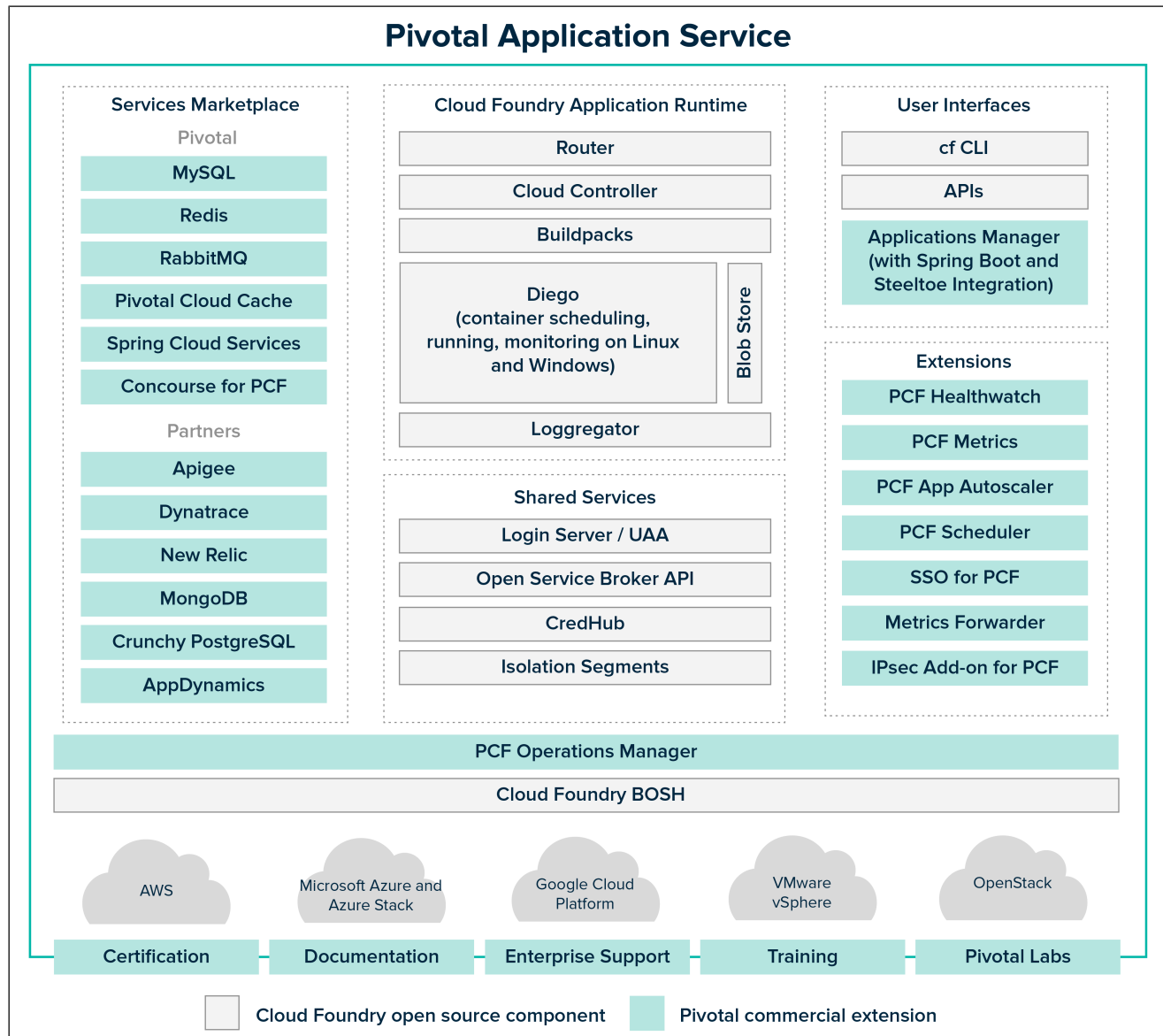
The component logs follow a different path. They stream from rsyslog agents, and the cloud operator can configure them to stream out to a syslog drain.

## Using Services with CF

Typical apps depend on free or metered [services](#) such as databases or third-party APIs. To incorporate these into an app, a developer writes a Service Broker, an API that publishes to the Cloud Controller the ability to list service offerings, provision the service, and enable apps to make calls out to it.

## How Pivotal Cloud Foundry Differs from Open Source Cloud Foundry

Open source software provides the basis for the Pivotal Cloud Foundry platform. Pivotal Application Service (PAS) is the Pivotal distribution of Cloud Foundry software for hosting apps. Pivotal offers additional commercial features, enterprise services, support, documentation, certificates, and others value-adds.



## How Apps Are Staged

This topic describes how Diego stages buildpack apps and Docker images.

### Overview

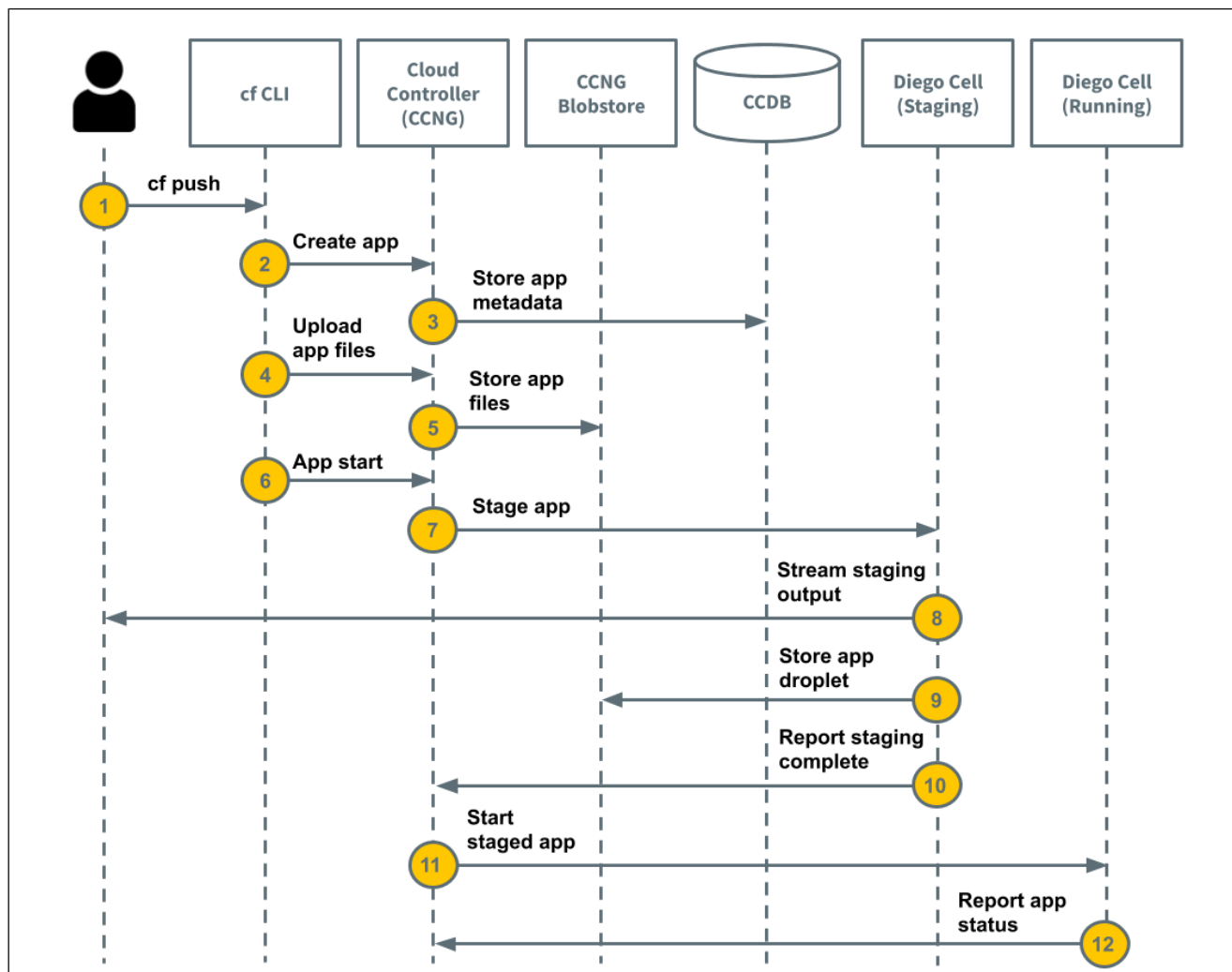
Cloud Foundry uses Diego to manage app containers. It is a self-healing system that attempts to keep the correct number of instances running in Diego Cells to avoid network failures and crashes. For more information about Diego, see [Diego Components and Architecture](#).

This topic references tasks and long-running processes (LRPs). For more information about these, see [Tasks and Long-Running Processes](#).

## How Diego Stages Buildpack Apps

This section describes how Diego stages buildpack apps.

The following diagram illustrates the steps and components involved in the process of staging a buildpack app.



For a description of each step in the process of staging a buildpack app, see the following:

1. A developer runs `cf push`.
2. The Cloud Foundry Command Line Interface (cf CLI) tells the Cloud Controller to create a record for the app. See the [Cloud Controller](#) topic for more information about the Cloud Controller.
3. The Cloud Controller stores the app metadata. App metadata can include the app name, number of instances, buildpack, and other information

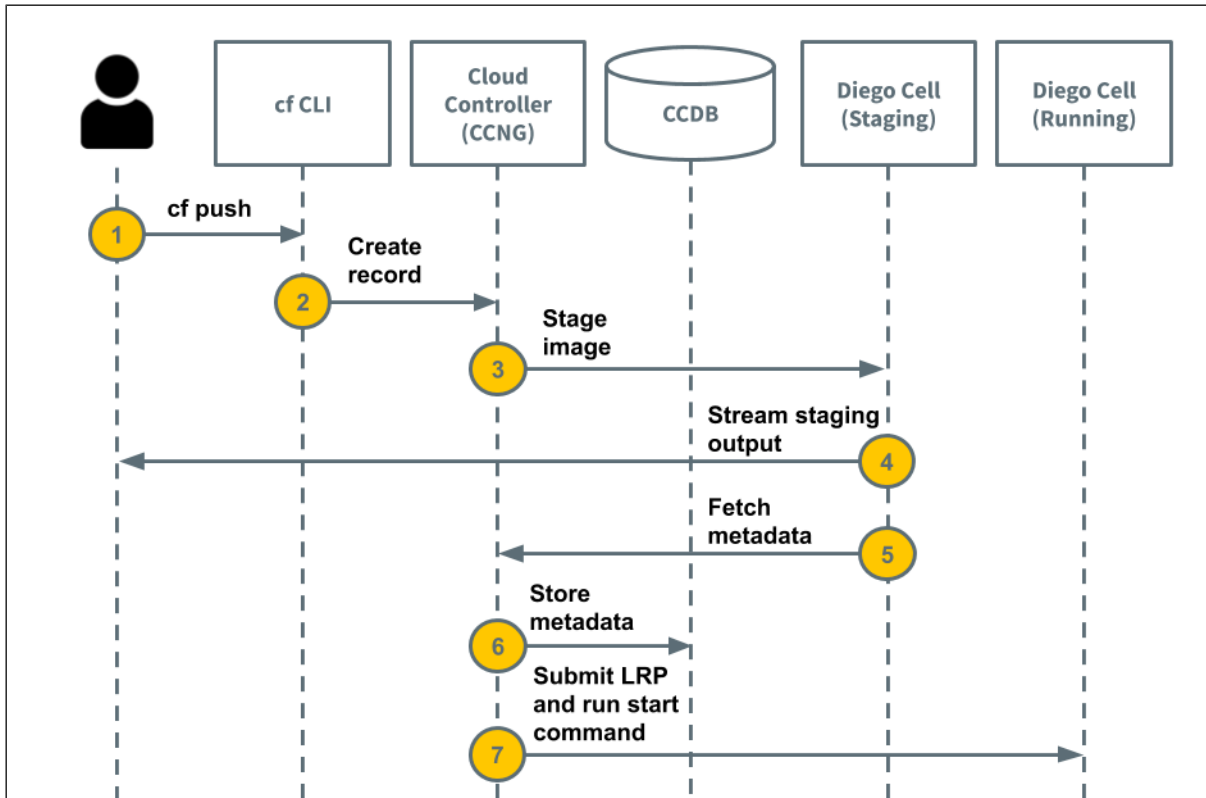
about the app.

4. This step includes the following:
  - a. The cf CLI requests a resource match from the Cloud Controller.
  - b. The cf CLI uploads the app source files, omitting any app files that already exist in the resource cache.
  - c. The Cloud Controller combines the uploaded app files with files from the resource cache to create the app package.
5. The Cloud Controller stores the app package in the blobstore. For more information, see the [Blobstore](#) section in the *Cloud Foundry Components* topic.
6. The cf CLI issues a request to start the app.
7. This step includes the following:
  - a. The Cloud Controller issues a staging request to Diego.
  - b. Diego schedules a Diego Cell to run the staging task.
  - c. The task downloads buildpacks and the app buildpack cache, if present.
  - d. The task uses the buildpack to compile and stage the app.
8. The Diego Cell streams the output of the staging process. A developer may need to view the output to troubleshoot staging problems.
9. This step includes the following:
  - a. The task creates a tarball, or droplet, with the compiled and staged app.
  - b. The Diego Cell stores the droplet in the blobstore.
  - c. The task uploads the buildpack cache to the blobstore for use the next time the app is staged.
10. The Diego Bulletin Board System (BBS) reports to the Cloud Controller that staging is complete. If staging does not complete within 15 minutes, it fails.
11. Diego schedules the app as a LRP on one or more Diego Cells.
12. The Diego Cells report the status of the app to the Cloud Controller.

## How Diego Stages Docker Images

This section describes how Diego stages Docker images.

The following diagram illustrates the steps and components involved in the process of staging a Docker image.



For a description of each step in the process of staging a Docker image, see the following:

1. A developer runs `cf push` and includes the name of a Docker image in an accessible Docker Registry.
2. The cf CLI tells the Cloud Controller to create a record for the Docker image.
3. This step includes the following:
  - a. The Cloud Controller issues a staging request to Diego.
  - b. Diego schedules a Diego Cell to run the task.
4. The Diego Cell streams the output of the staging process. A developer may need to view the output to troubleshoot staging problems.
5. The task fetches the metadata associated with the Docker image and returns a portion of it to the Cloud Controller.
6. The Cloud Controller stores the metadata in the Cloud Controller database (CCDB).
7. This step includes the following:
  - a. The Cloud Controller uses the Docker image metadata to construct a LRP that runs the start command specified in the Dockerfile.
  - b. The Cloud Controller submits the LRP to Diego.
  - c. Diego schedules the LRP on one or more Diego Cells.
  - d. The Cloud Controller instructs Diego and the Gorouter to route traffic to the Docker image.



**Note:** The Cloud Controller takes into account any user-specified overrides specified in the Dockerfile, such as environment variables.



## Application Container Lifecycle


Page last updated:

This topic describes the lifecycle of an application container for Cloud Foundry (CF) deployments running on the Diego architecture.

### Deployment

The application deployment process involves uploading, staging, and starting the app in a container. Your app must successfully complete each of these phases within certain time limits. The default time limits for the phases are as follows:

- Upload: 15 minutes
- Stage: 15 minutes
- Start: 60 seconds

 **Note:** Your administrator can change these defaults. Check with your administrator for the actual time limits set for app deployment.

Developers can change the time limit for starting apps through an application manifest or on the command line. For more information, see [The timeout attribute](#) section of the Deploying with Application Manifests topic and [Using Application Health Checks](#).

### Crash Events

If an app instance crashes, CF automatically restarts it by rescheduling the instance on another container three times. After three failed restarts, CF waits thirty seconds before attempting another restart. The wait time doubles each restart until the ninth restart, and remains at that duration until the 200th restart. After the 200th restart, CF stops trying to restart the app instance.

### Evacuation

Certain operator actions require restarting VMs with containers hosting app instances. For example, an operator who updates stemcells or installs a new version of CF must restart all the VMs in a deployment.

CF automatically relocates the instances on VMs that are shutting down through a process called evacuation. CF recreates the app instances on another VM, waits until they are healthy, and then shuts down the old instances. During an evacuation, developers may see their app instances in a duplicated state for a brief period.


During this app duplication process, singleton app instances may become temporarily unavailable if the replacement instance does not become healthy within the cell's evacuation timeout, which defaults to 10 minutes. Because of this, app developers with a low tolerance for brief downtime may prefer to run several instances of their app. See [Run Multiple Instances to Increase Availability](#).

### Shutdown

PCF requests a shutdown of your app instance in the following scenarios:

- When a user runs `cf scale`, `cf stop`, `cf push`, `cf delete`, or `cf restart-app-instance`
- As a result of a system event, such as the replacement procedure during Diego cell evacuation or when an app instance stops because of a failed health-check probe

To shut down the app, CF sends the app process in the container a SIGTERM. The process has ten seconds to shut down gracefully. If the process has not exited after ten seconds, CF sends a SIGKILL.

 **Note:** One exception to the cases mentioned above is when monit restarts a crashed Diego cell rep or Garden server. In this case, CF immediately stops the apps that are still running using SIGKILL.



## High Availability in Cloud Foundry

Page last updated:

This topic describes the components used to ensure high availability in Cloud Foundry, vertical and horizontal scaling, and the infrastructure required to support scaling component VMs for high availability.

### Components of a High Availability Deployment

This section describes the system components needed to ensure high availability.

#### Availability Zones

During product updates and platform upgrades, the VMs in a deployment restart in succession, rendering them temporarily unavailable. During outages, VMs go down in a less orderly way. Spreading components across Availability Zones (AZs) and scaling them to a sufficient level of redundancy maintains high availability during both upgrades and outages and can ensure zero downtime.

Deploying Cloud Foundry across three or more AZs and assigning multiple component instances to different AZ locations lets a deployment operate uninterrupted when entire AZs become unavailable. Cloud Foundry maintains its availability as long as a majority of the AZs remain accessible. For example, a three-AZ deployment stays up when one entire AZ goes down, and a five-AZ deployment can withstand an outage of up to two AZs with no impact on uptime.

#### External Load Balancers

Production environments should use a highly-available customer-provided load balancing solution that does the following:

- Provides load balancing to each of the Cloud Foundry Router IP addresses
- Supports SSL termination with wildcard DNS location
- Adds appropriate x-forwarded-for and x-forwarded-proto HTTP headers to incoming requests
- (Optional) Supports WebSockets

If you are deploying in lab and test environments, the `use-haproxy.yml` ops file enables HAProxy for your foundation.

For more information, see [Using Your Own Load Balancer](#).

#### Blob Storage

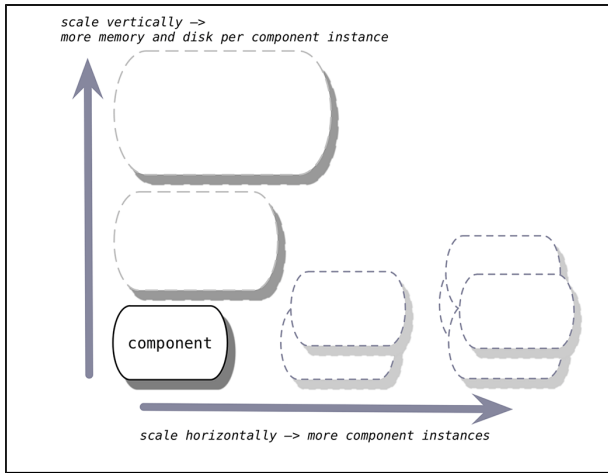
For storing blobs, large binary files, the best approach for high availability is to use external storage such as Amazon S3 or an S3-compatible service.

If you store blobs internally using WebDAV or NFS, these components run as single instances and you cannot scale them. For these deployments, use the high availability features of your IaaS to immediately recover your WebDAV or NFS server VM if it fails. Contact [Pivotal Support](#) if you need assistance.

The singleton compilation components do not affect platform availability.

### Vertical and Horizontal Scaling for High Availability

You can scale platform capacity vertically by adding memory and disk, or horizontally by adding more VMs running instances of Cloud Foundry components. The nature of the applications you host on Cloud Foundry should determine whether you should scale vertically or horizontally.



For more information about scaling applications and maintaining app uptime, see [Scaling an Application Using cf scale](#) and [Using Blue-Green Deployment to Reduce Downtime and Risk](#).

## Scale Vertically

Scaling vertically means adding memory and disk to your component VMs.

To scale vertically, ensure that you allocate and maintain enough of the following:

- Free space on host Diego cell VMs so that apps expected to deploy can successfully be staged and run.
- Disk space and memory in your deployment such that if one host VM is down, all instances of apps can be placed on the remaining Host VMs.
- Free space to handle one AZ going down if deploying in multiple AZs.

## Scale Horizontally

Scaling horizontally means increasing the number of VM instances dedicated to running a functional component of the system.

You can horizontally scale most Cloud Foundry components to multiple instances to achieve the redundancy required for high availability.

You should also distribute the instances of multiply-scaled components across different AZs to minimize downtime during ongoing operation, product updates, and platform upgrades. If you use more than three AZs, ensure that you use an odd number of AZs.

For more information regarding zero downtime deployment, see [Scaling Instances in PAS](#).

The following table provides recommended instance counts for a high-availability deployment and the minimum instances for a functional deployment:

| Pivotal Application Service (PAS) Job | Recommended Instance Number for HA | Minimum Instance Number | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Diego Cell                            | ≥ 3                                | 1                       | The optimal balance between CPU/memory sizing and instance count depends on the performance characteristics of the apps that run on Diego cells. Scaling vertically with larger Diego cells makes for larger points of failure, and more apps go down when a cell fails. On the other hand, scaling horizontally decreases the speed at which the system rebalances apps. Rebalancing 100 cells takes longer and demands more processing overhead than rebalancing 20 cells. |
| Diego Brain                           | ≥ 2                                | 1                       | For high availability, use at least one per AZ, or at least two if only one AZ.                                                                                                                                                                                                                                                                                                                                                                                              |
| Diego BBS                             | ≥ 2                                | 1                       | For high availability in a multi-AZ deployment, use at least one instance per AZ. Scale Diego BBS to at least two instances for high availability in a single-AZ deployment.                                                                                                                                                                                                                                                                                                 |
| Consul                                | ≥ 3                                | 1                       | Set this to an odd number equal to or one greater than the number of AZs you have, in order to maintain quorum. Distribute the instances evenly across the AZs, at least one instance per AZ.                                                                                                                                                                                                                                                                                |
| MySQL Internal Load Balancer          | 1                                  | 0                       | A load balancer distributes SQL traffic across two redundant MySQL proxies.                                                                                                                                                                                                                                                                                                                                                                                                  |
| MySQL Proxy                           | 2                                  | 1                       | If you use an <a href="#">external database</a> in your deployment, then you can set the MySQL Proxy instance count to <code>0</code> .                                                                                                                                                                                                                                                                                                                                      |

|                               |               |        |                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|---------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MySQL Server                  | 3             | 1      | If you use an <a href="#">external database</a> in your deployment, then you can set the MySQL Server instance count to <code>0</code> . For instructions about scaling down an internal MySQL cluster, see <a href="#">Scaling Down Your MySQL Cluster</a> .                                                                                                                                      |
| NATS Server                   | $\geq 2$      | 1      | In a high availability deployment, you might run a single NATS instance if your deployment lacks the resources to deploy two stable NATS servers. Components using NATS are resilient to message failures and the BOSH resurrector recovers the NATS VM quickly if it becomes non-responsive.                                                                                                      |
| Cloud Controller              | $\geq 2$      | 1      | Scale the Cloud Controller to accommodate the number of requests to the API and the number of apps in the system.                                                                                                                                                                                                                                                                                  |
| Clock Global                  | $\geq 2$      | 1      | For a high availability deployment, scale the Clock Global job to a value greater than 1 or to the number of AZs you have.                                                                                                                                                                                                                                                                         |
| Router                        | $\geq 2$      | 1      | Scale the router to accommodate the number of incoming requests. Additional instances increase available bandwidth. In general, this load is much less than the load on Diego cells.                                                                                                                                                                                                               |
| HAProxy                       | 0 or $\geq 2$ | 0 or 1 | For environments that require high availability, you can scale HAProxy to <code>0</code> and then configure a high-availability load balancer (LB) to point directly to each Gorouter instance. Alternately, you can also configure the high availability LB to point to HAProxy instance scaled at $\geq 2$ . Either way, an LB is required to host Cloud Foundry domains at a single IP address. |
| UAA                           | $\geq 2$      | 1      |                                                                                                                                                                                                                                                                                                                                                                                                    |
| Doppler Server                | $\geq 2$      | 1      | Deploying additional Doppler servers splits traffic across them. For a high availability deployment, Pivotal recommends at least two per Availability Zone.                                                                                                                                                                                                                                        |
| Loggregator Trafficcontroller | $\geq 2$      | 1      | Deploying additional Loggregator Traffic Controllers allows you to direct traffic to them in a round-robin manner. For a high availability deployment, Pivotal recommends at least two per Availability Zone.                                                                                                                                                                                      |
| Syslog Scheduler              | $\geq 2$      | 1      | The Syslog Scheduler is a scalable component. For high availability, use at least one instance per AZ, or at least two instances if only one AZ is present.                                                                                                                                                                                                                                        |

## Configure Support for High Availability Components

This section describes the surrounding infrastructure required to support scaling component VMs for high availability.

### BOSH Resurrector

The BOSH Resurrector increases Pivotal Application Service (PAS) availability in the following ways:

- Reacts to hardware failure and network disruptions by recreating virtual machines on active, stable hosts
- Detects operating system failures by continuously monitoring virtual machines and recreating them as required
- Continuously monitors the BOSH Agent running on each virtual machine and recreates the VMs as required

The BOSH Resurrector continuously monitors the status of all virtual machines in an PAS deployment. The Resurrector also monitors the BOSH Agent on each VM. If either the VM or the BOSH Agent fail, the Resurrector recreates the virtual machine on another active host. To enable the BOSH Resurrector, see [Enable BOSH Resurrector](#).

### Resource Pools

To configure your resource pools according to the requirements of your deployment, see the [Ops Manager configuration topic for your IaaS](#).

Each IaaS has different ways of limiting resource consumption for scaling VMs. Consult with your IaaS administrator to ensure additional VMs and related resources, like IPs and storage, will be available when scaling.

For information about configuring resource pools for Amazon Web Services, see [Amazon EC2 FAQs](#) in the Amazon documentation. For information about configuring resource pools for OpenStack, see [Manage projects and users](#) in the OpenStack documentation. For information about configuring resource pools for vSphere, see [Configuring BOSH Director on vSphere](#).

### Databases

For database services deployed outside Cloud Foundry, plan to leverage your infrastructure's high availability features and to configure backup and

restore where possible. For more information about scaling internal database components, see the [Scaling Instances in PAS](#) topic.



**Note:** Data services may have single points of failure depending on their configuration.

Contact [Pivotal Support](#) [↗](#) if you need assistance.

## How Cloud Foundry Maintains High Availability

Page last updated:

This topic explains how Pivotal Cloud Foundry (PCF) deployments include several layers of high availability to keep applications running during system failure. These layers include AZs, application health management, process monitoring, and VM resurrection.

### Availability Zones

PCF supports deploying application instances across multiple AZs. This level of high availability requires that you define AZs in your IaaS. PCF balances the applications you deploy across the AZs you defined. If an AZ goes down, you still have application instances running in another.

You can configure your deployment so that Diego cells are created across these AZs. Follow the configuration for your specific IaaS: [AWS](#), [GCP](#), [OpenStack](#), or [vSphere](#).

### Health Management for App Instances

If you lose application instances for any reason, such as a bug in the app or an AZ going down, PCF restarts new instances to maintain capacity. Under Diego architecture, the nsync, BBS, and Cell Rep components track the number of instances of each application that are running across all of the Diego cells. When these components detect a discrepancy between the actual state of the app instances in the cloud and the desired state as known by the Cloud Controller, they advise the Cloud Controller of the difference and the Cloud Controller initiates the deployment of new application instances.

For more information about the nsync, BBS, and Cell Rep components, see the [nsync, BBS, and Cell Rep](#) section of the *Cloud Foundry Components* topic.

### Process Monitoring

PCF uses a BOSH agent, *monit*, to monitor the processes on the component VMs that work together to keep your applications running, such as nsync, BBS, and Cell Rep. If *monit* detects a failure, it restarts the process and notifies the BOSH agent on the VM. The BOSH agent notifies the BOSH Health Monitor, which triggers responders through plugins such as email notifications or paging.

### Resurrection for VMs

BOSH detects if a VM is present by listening for heartbeat messages that are sent from the BOSH agent every 60 seconds. The BOSH Health Monitor listens for those heartbeats. When the Health Monitor finds that a VM is not responding, it passes an alert to the Resurrector component. If the Resurrector is enabled, it sends the IaaS a request to create a new VM instance to replace the one that failed.

To enable the Resurrector, see the following pages for your particular IaaS: [AWS](#), [Azure](#), [GCP](#), [OpenStack](#), or [vSphere](#).

## Orgs, Spaces, Roles, and Permissions

PCF uses a role-based access control (RBAC) system to grant Pivotal Application Service users permissions appropriate to their role within an org or a space. This topic describes how orgs and spaces work within a PCF deployment, and how different Pivotal Application Service User roles operate within those contexts.

Admins, Org Managers, and Space Managers can assign user roles using the [cf CLI](#) or [Apps Manager](#).



**Note:** Before you assign a **space role** to a user, you must assign an **org role** to the user.

## Orgs

An org is a development account that an individual or multiple collaborators can own and use. All collaborators access an org with user accounts. Collaborators in an org share a resource quota plan, applications, services availability, and custom domains.

By default, an org has the status of *active*. An admin can set the status of an org to *suspended* for various reasons such as failure to provide payment or misuse. When an org is suspended, users cannot perform certain activities within the org, such as push apps, modify spaces, or bind services. For details on what activities are allowed for suspended orgs, see [Roles and Permissions for Suspended Orgs](#).

## User Accounts

A user account represents an individual person within the context of a PCF installation. A user can have different roles in different spaces within an org, governing what level and type of access they have within that space.

Before you assign a space role to a user, you must assign an org role to the user. The error message

```
Server error, error code: 1002, message: cannot set space role because user is not part of the org
```

occurs when you try to set a space role before setting an org role for the user.

## Spaces

Every application and service is scoped to a space. An org can contain multiple spaces. A space provides users with access to a shared location for application development, deployment, and maintenance. Each space role applies only to a particular space.

## Roles and Permissions

A user can have one or more roles. The combination of these roles defines the user's overall permissions in the org and within specific spaces in that org. Roles can be assigned different scopes of User Account and Authentication (UAA) privileges. For more information about UAA scopes, see [Scopes](#) in *Component: User Account and Authentication (UAA) Server*.

For non-admin users, the `cloud_controller.read` scope is required to view resources, and the `cloud_controller.write` scope is required to create, update, and delete resources.

- **Admin** is a user role that has been assigned the `cloud_controller.admin` scope in UAA. An admin user has permissions on all orgs and spaces and can perform operational actions using the [Cloud Controller API](#). To create an account with `cloud_controller.admin` scope for your installation, see [Create an Admin User](#).
- **Admin Read-Only** is a user role that has been assigned the `cloud_controller.admin_read_only` scope in UAA. This role has read-only access to all Cloud Controller API resources.
- **Global Auditor** is a user role that has been assigned the `cloud_controller.global_auditor` scope in UAA. This role has read-only access to all Cloud Controller API resources except for secrets such as environment variables. The Global Auditor role cannot access those values.
- **Org Managers** are managers or other users who need to administer the org.
- **Org Auditors** view but cannot edit user information and org quota usage information.
- **Org Users** can view the list of other org users and their roles. When an Org Manager gives a person an Org or Space role, that person automatically receives Org User status in that Org.
- **Space Managers** are managers or other users who administer a space within an org.



- **Space Developers** are application developers or other users who manage applications and services in a space.
- **Space Auditors** view but cannot edit the space.

## Roles and Permissions for Active Orgs

The following table describes the permissions for various PCF roles.

| Activity                                                                                           | Admin          | Admin Read-Only | Global Auditor | Org Manager    | Org Auditor    | Space Manager  | Space Developer | Space Auditor  |
|----------------------------------------------------------------------------------------------------|----------------|-----------------|----------------|----------------|----------------|----------------|-----------------|----------------|
| Scope of operation                                                                                 | Org            | Org             | Org            | Org            | Org            | Space          | Space           | Space          |
| Add and edit users and roles                                                                       | ✓              |                 |                | 1              |                | 1              |                 |                |
| View users and roles                                                                               | ✓              | ✓               | ✓              | ✓              | ✓              | ✓              | ✓               | ✓              |
| Create and assign org quota plans                                                                  | ✓              |                 |                |                |                |                |                 |                |
| View org quota plans                                                                               | ✓              | ✓               | ✓              | ✓              | ✓              | ✓              | ✓               | ✓              |
| Create orgs                                                                                        | ✓              |                 |                | 2              | 2              | 2              | 2               | 2              |
| View all orgs                                                                                      | ✓              | ✓               | ✓              |                |                |                |                 |                |
| View orgs where user is a member                                                                   | ✓ <sup>3</sup> | ✓ <sup>3</sup>  | ✓ <sup>3</sup> | ✓              | ✓              | ✓              | ✓               | ✓              |
| Edit, rename, and delete orgs                                                                      | ✓              |                 |                | ✓ <sup>4</sup> |                |                |                 |                |
| Suspend or activate an org                                                                         | ✓              |                 |                |                |                |                |                 |                |
| Create and assign space quota plans                                                                | ✓              |                 |                | ✓              |                |                |                 |                |
| Create spaces                                                                                      | ✓              |                 |                | ✓              |                |                |                 |                |
| View spaces                                                                                        | ✓              | ✓               | ✓              | ✓              |                | ✓              | ✓               | ✓              |
| Edit spaces                                                                                        | ✓              |                 |                | ✓              |                | ✓              |                 |                |
| Delete spaces                                                                                      | ✓              |                 |                | ✓              |                |                |                 |                |
| Rename spaces                                                                                      | ✓              |                 |                | ✓              |                | ✓              |                 |                |
| View the status, number of instances, service bindings, and resource use of applications           | ✓              | ✓               | ✓              | ✓              |                | ✓              | ✓               | ✓              |
| Add private domains <sup>5</sup>                                                                   | ✓              |                 |                | ✓              |                |                |                 |                |
| Deploy, run, and manage applications                                                               | ✓              |                 |                |                |                |                | ✓               |                |
| Use application SSH <sup>6</sup>                                                                   | ✓              |                 |                |                |                |                | ✓               |                |
| Instantiate and bind services to applications                                                      | ✓              |                 |                |                |                |                | ✓               |                |
| Associate routes <sup>5</sup> , instance counts, memory allocation, and disk limit of applications | ✓              |                 |                |                |                |                | ✓               |                |
| Rename applications                                                                                | ✓              |                 |                |                |                |                | ✓               |                |
| Create and manage <a href="#">Application Security Groups</a>                                      | ✓              |                 |                |                |                |                |                 |                |
| Create, update, and delete an <a href="#">Isolation Segment</a>                                    | ✓              |                 |                |                |                |                |                 |                |
| List all <a href="#">Isolation Segments</a> for an Org                                             | ✓              | ✓               | ✓ <sup>7</sup> | ✓ <sup>7</sup> | ✓ <sup>7</sup> | ✓ <sup>7</sup> | ✓ <sup>7</sup>  | ✓ <sup>7</sup> |
| Entitle or revoke an <a href="#">Isolation Segment</a>                                             | ✓              |                 |                |                |                |                |                 |                |
| List all Orgs entitled to an <a href="#">Isolation Segment</a>                                     | ✓              | ✓               | ✓ <sup>7</sup> | ✓ <sup>7</sup> | ✓ <sup>7</sup> | ✓ <sup>7</sup> | ✓ <sup>7</sup>  | ✓ <sup>7</sup> |
| Assign a default <a href="#">Isolation Segment</a> to an Org                                       | ✓              |                 |                | ✓              |                |                |                 |                |
| List and manage <a href="#">Isolation Segments</a> for spaces                                      | ✓              |                 |                | ✓              |                |                |                 |                |
| List entitled <a href="#">Isolation Segment</a> for a space                                        | ✓              | ✓               | ✓              | ✓              |                | ✓              | ✓               | ✓              |
| List which <a href="#">Isolation Segment</a> an app runs on                                        | ✓              | ✓               | ✓              | ✓              |                | ✓              | ✓               | ✓              |

<sup>1</sup>Not by default, unless [feature flag](#) `set_roles_by_username` is set to `true`.

<sup>2</sup>Not by default, unless [feature flag](#) `user_org_creation` is set to `true`.

<sup>3</sup>Admin, admin read-only, and global auditor roles do not need to be added as members of orgs or spaces to view resources.

<sup>4</sup>Org Managers can rename their orgs and edit some fields; they cannot delete orgs.

<sup>5</sup>Unless disabled by [feature flags](#).

<sup>6</sup>This assumes that SSH is enabled for the platform, space, and app. For more information, see [SSH Access Control Hierarchy](#).

<sup>7</sup>Applies only to orgs they belong to.

## Roles and Permissions for Suspended Orgs

The following table describes roles and permissions applied after an operator sets the status of an org to *suspended*.

| Activity                                                                                           | Admin | Admin Read-Only | Global Auditor | Org Manager | Org Auditor | Space Manager | Space Developer | Space Auditor |
|----------------------------------------------------------------------------------------------------|-------|-----------------|----------------|-------------|-------------|---------------|-----------------|---------------|
| Scope of operation                                                                                 | Org   | Org             | Org            | Org         | Org         | Space         | Space           | Space         |
| Add and edit users and roles                                                                       | ✓     |                 |                |             |             |               |                 |               |
| View users and roles                                                                               | ✓     | ✓               | ✓              | ✓           | ✓           | ✓             | ✓               | ✓             |
| Create and assign org quota plans                                                                  | ✓     |                 |                |             |             |               |                 |               |
| View org quota plans                                                                               | ✓     | ✓               | ✓              | ✓           | ✓           | ✓             | ✓               | ✓             |
| Create orgs                                                                                        | ✓     |                 |                |             |             |               |                 |               |
| View all orgs                                                                                      | ✓     | ✓               | ✓              |             |             |               |                 |               |
| View orgs where user is a member                                                                   | ✓     | ✓               | ✓              | ✓           | ✓           | ✓             | ✓               | ✓             |
| Edit, rename, and delete orgs                                                                      | ✓     |                 |                |             |             |               |                 |               |
| Suspend or activate an org                                                                         | ✓     |                 |                |             |             |               |                 |               |
| Create and assign space quota plans                                                                | ✓     |                 |                |             |             |               |                 |               |
| Create spaces                                                                                      | ✓     |                 |                |             |             |               |                 |               |
| View spaces                                                                                        | ✓     | ✓               | ✓              | ✓           |             | ✓             | ✓               | ✓             |
| Edit spaces                                                                                        | ✓     |                 |                |             |             |               |                 |               |
| Delete spaces                                                                                      | ✓     |                 |                |             |             |               |                 |               |
| Rename spaces                                                                                      | ✓     |                 |                |             |             |               |                 |               |
| View the status, number of instances, service bindings, and resource use of applications           | ✓     | ✓               | ✓              | ✓           |             | ✓             | ✓               | ✓             |
| Add private domains <sup>†</sup>                                                                   | ✓     |                 |                |             |             |               |                 |               |
| Deploy, run, and manage applications                                                               | ✓     |                 |                |             |             |               |                 |               |
| Instantiate and bind services to applications                                                      | ✓     |                 |                |             |             |               |                 |               |
| Associate routes <sup>†</sup> , instance counts, memory allocation, and disk limit of applications | ✓     |                 |                |             |             |               |                 |               |
| Rename applications                                                                                | ✓     |                 |                |             |             |               |                 |               |
| Create and manage <a href="#">Application Security Groups</a>                                      | ✓     |                 |                |             |             |               |                 |               |

## Cloud Foundry Security

Page last updated:


This topic provides an overview of Cloud Foundry (CF) security. For an overview of container security, see the [Container Security](#) topic.

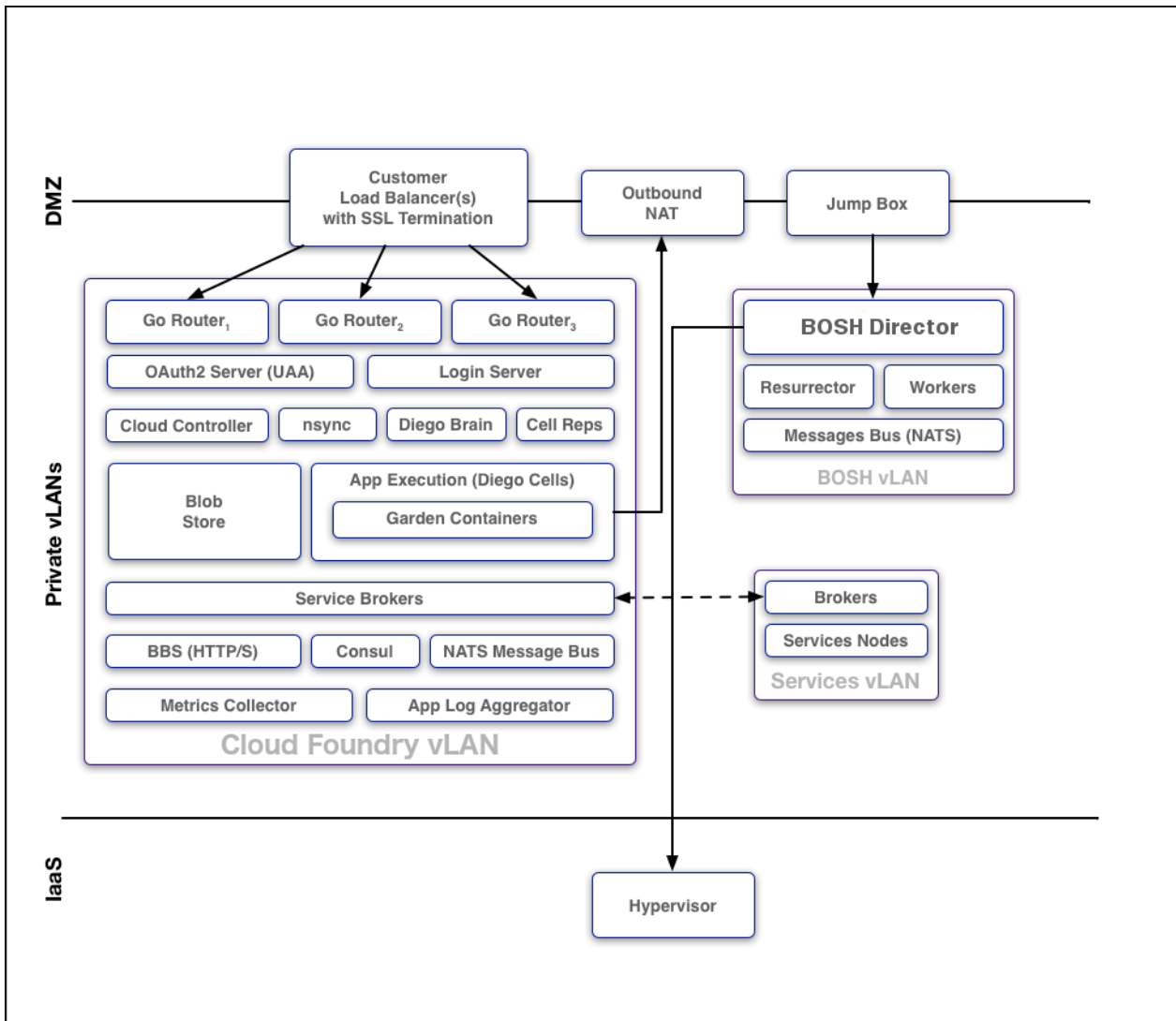
Cloud Foundry implements the following measures to mitigate against security threats:

- Minimizes network surface area
- Isolates customer applications and data in containers
- Encrypts connections
- Uses role-based access controls, applying and enforcing roles and permissions to ensure that users can only view and affect the spaces for which they have been granted access
- Ensures security of application bits in a multi-tenant environment
- Prevents possible denial of service attacks through resource starvation

## System Boundaries and Access

As the image below shows, in a typical deployment of Cloud Foundry, the components run on virtual machines (VMs) that exist within a VLAN. In this configuration, the only access points visible on a public network are a load balancer that maps to one or more Cloud Foundry routers and, optionally, a NAT VM and a jumpbox. Because of the limited number of contact points with the public internet, the surface area for possible security vulnerabilities is minimized.

 **Note:** Pivotal recommends that you also install a NAT VM for outbound requests and a Jumpbox to access the BOSH Director, though these access points are optional depending on your network configuration.



## Protocols

All traffic from the public internet to the Cloud Controller and UAA happens over HTTPS. Inside the boundary of the system, components communicate over a publish-subscribe (pub-sub) message bus [NATS](#), HTTP, and SSL/TLS.

## BOSH

Operators deploy Cloud Foundry with BOSH. The BOSH Director is the core orchestrating component in BOSH: it controls VM creation and deployment, as well as other software and service lifecycle events. You use HTTPS to ensure secure communication to the BOSH Director.

**Note:** Pivotal recommends that you deploy the BOSH Director on a subnet that is not publicly accessible, and access the BOSH Director from a Jumpbox on the subnet or through VPN.

BOSH includes the following functionality for security:

- Communicates with the VMs it launches over NATS. Because NATS cannot be accessed from outside Cloud Foundry, this ensures that published messages can only originate from a component within your deployment.
- Provides an audit trail through the `bosh tasks --all` and `bosh tasks --recent=VALUE` commands. `bosh tasks --all` returns a table that shows all BOSH actions taken by an operator or other running processes. `bosh tasks --recent=VALUE` returns a table of recent tasks, with `VALUE` being the number of recent tasks you want to view.
- Allows you to set up individual login accounts for each operator. BOSH operators have root access.

**Note:** BOSH does not encrypt data stored on BOSH VMs. Your IaaS might encrypt this data.

## Isolation Segments

Isolation segments provide dedicated pools of resources to which apps can be deployed to isolate workloads. Using isolation segments separates app resources as completely as if they were in different CF deployments but avoids redundant management components and unneeded network complexity.

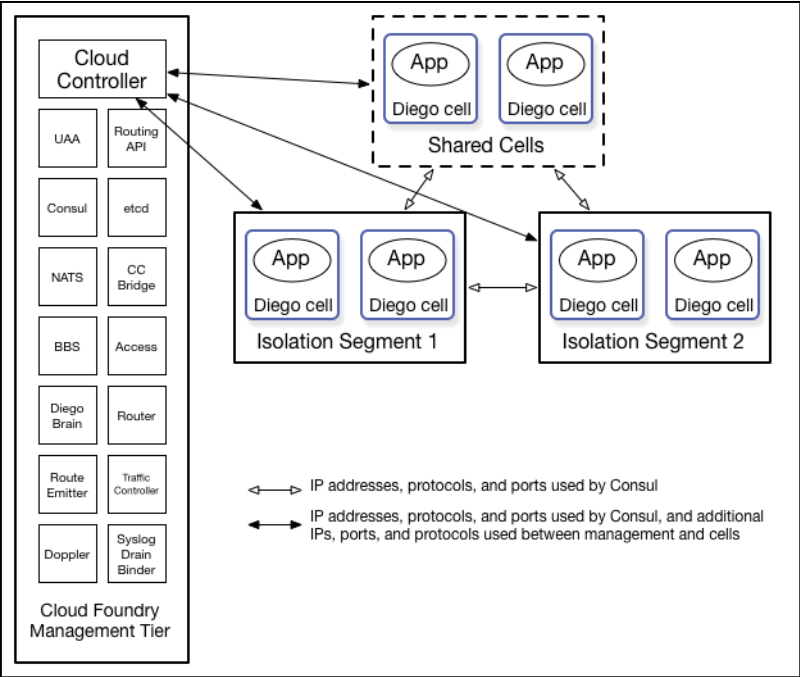
You can designate isolation segments for exclusive use by [orgs and spaces](#) within CF. This guarantees that apps within the org or space use resources that are not also used by other orgs or spaces.

Customers can use isolation segments for different reasons, including the following:

- To follow regulatory restrictions that require separation between different types of applications. For example, a health care company may not be able to host medical records and billing systems on the same machines.
- To dedicate specific hardware to different isolation segments. For example, to guarantee that high-priority apps run on a cluster of high-performance hosts.
- To separate data on multiple clients, to strengthen a security story, or offer different hosting tiers.

In CF, the Cloud Controller Database (CCDB) identifies isolation segments by name and GUID, for example `30dd879c-ee2f-11db-8314-0800200c9a66`. The isolation segment object has no internal structure beyond these two properties at the Cloud Foundry level, but BOSH associates the name of the isolation segment with Diego cells, through their `placement_tag` property.

This diagram shows how isolation segments keep apps running on different pools of cells, and how the cells communicate with each other and with the management components:



See the [Installing PCF Isolation Segment](#) and [Managing Isolation Segments](#) topics for more information about how to create and manage isolation segments in a PCF deployment.

See the [Isolation Segments](#) section of the *Cloud Controller API (CAPI) Reference* for API commands related to isolation segments.

## Authentication and Authorization

[User Account and Authentication](#) (UAA) is the central identity management service for Cloud Foundry and its various components.

UAA acts as an [OAuth2](#) Authorization Server and issues access tokens for applications that request platform resources. The tokens are based on the [JSON Web Token](#) and are digitally signed by UAA.

Operators can configure the identity store in UAA. If users register an account with the Cloud Foundry platform, UAA acts as the user store and stores user passwords in the UAA database using [bcrypt](#). UAA also supports connecting to external user stores through LDAP and SAML. Once an operator has

configured the external user store, such as a corporate Microsoft Active Directory, users can use their LDAP credentials to gain access to the Cloud Foundry platform instead of registering a separate account. Alternatively, operators can use SAML to connect to an external user store and enable single sign-on for users into the Cloud Foundry platform.

## Managing User Access with Role-Based Access Control


Applications that users deploy to Cloud Foundry exist within a space. Spaces exist within orgs. To view and access an org or a space, a user must be a member of it. Cloud Foundry uses role-based access control (RBAC), with each role granted permissions to either an org or a specified space. For more information about roles and permissions, refer to the [Orgs, Spaces, Roles, and Permissions](#) topic.

For more information, see [Getting Started with the Apps Manager](#) and [Managing User Accounts and Permissions Using the Apps Manager](#).

## Security for Service Broker Integration

The Cloud Controller authenticates every request with the Service Broker API using HTTP or HTTPS, depending on which protocol that you specify during broker registration. The Cloud Controller rejects any broker registration that does not contain a username and password.

Service instances bound to an app contain credential data. Users specify the binding credentials for [user-provided service instances](#), while third-party brokers specify the binding credentials for managed service instances. The `VCAP_SERVICES` environment variable contains credential information for any service bound to an app. Cloud Foundry constructs this value from encrypted data that it stores in the Cloud Controller Database (CCDB).

 **Note:** The selected third-party broker controls how securely to communicate managed service credentials.

A third-party broker might offer a dashboard client in its catalog. Dashboard clients require a text string defined as a `client_secret`. Cloud Foundry does not store this secret in the CCDB. Instead, Cloud Foundry passes the secret to the UAA component for verification using HTTP or HTTPS.

## Software Vulnerability Management

Cloud Foundry manages software vulnerability using releases and BOSH stemcells. New Cloud Foundry releases are created with updates to address code issues, while new stemcells are created with patches for the latest security fixes to address any underlying operating system issues.

## Ensuring Security for Application Artifacts

Cloud Foundry secures both the code and the configuration of an application using the following functionality:

- Application developers push their code using the [Cloud Foundry API](#). Cloud Foundry secures each call to the CF API using the [UAA](#) and SSL.
- The Cloud Controller uses [RBAC](#) to ensure that only authorized users can access a particular application.
- The Cloud Controller stores the configuration for an application in an encrypted database table. This configuration data includes user-specified environment variables and service credentials for any services bound to the app.
- Cloud Foundry runs the app inside a secure container. For more information, see the [Container Security](#) topic.
- Cloud Foundry operators can configure network traffic rules to control inbound communication to and outbound communication from an app. For more information, see the [Network Traffic Rules](#) section of the [Container Security](#) topic.

## Security Event Logging and Auditing

For operators, Cloud Foundry provides an audit trail through the `bosh tasks` command. This command shows all actions that an operator has taken with the platform. Additionally, operators can redirect Cloud Foundry component logs to a standard syslog server using the `syslog_daemon_config` [property](#) in the `metron_agent` job of `cf-release`.

For users, Cloud Foundry records an audit trail of all relevant API invocations of an app. The Cloud Foundry Command Line Interface (cf CLI) command `cf events` returns this information.

## Recommendations for Running a Secure Deployment

To help run a secure deployment, Pivotal recommends the following:

- Configure UAA clients and users using a BOSH manifest. Limit and manage these clients and users as you would any other kind of privileged account.
- Deploy within a VLAN that limits network traffic to individual VMs. This reduce the possibility of unauthorized access to the VMs within your BOSH-managed cloud.
- Enable HTTPS for applications and SSL database connections to protect sensitive data transmitted to and from applications.
- Ensure that the Jumpbox is secure, along with the load balancer and NAT VM.
- Encrypt stored files and data within databases to meet your data security requirements. Deploy using industry standard encryption and the best practices for your language or framework.
- Prohibit promiscuous network interfaces on the trusted network.
- Review and monitor data sharing and security practices with third-party services that you use to provide additional functionality to your application.
- Store SSH keys securely to prevent disclosure, and promptly replace lost or compromised keys.
- Use Cloud Foundry's RBAC model to restrict your users' access to only what is necessary to complete their tasks.
- Use a strong passphrase for both your Cloud Foundry user account and SSH keys.
- Use the [IPsec add-on](#) to encrypt IP data traffic within your deployment.

## Container Security

Page last updated:

This topic describes how Cloud Foundry (CF) secures the containers that host application instances on Linux. For an overview of other CF security features, see the [Cloud Foundry Security](#) topic.

- [Container Mechanics](#) provides an overview of container isolation.
- [Inbound and Outbound Traffic from CF](#) provides an [overview](#) of container networking and describes how CF administrators [customize](#) container network traffic rules for their deployment.
- [Container Security](#) describes how CF secures containers by running application instances in [unprivileged](#) containers and by [hardening](#) them.

## Container Mechanics


Each instance of an app deployed to CF runs within its own self-contained environment, a [Garden container](#). This container isolates processes, memory, and the filesystem using operating system features and the characteristics of the virtual and physical infrastructure where CF is deployed.

CF achieves container isolation by namespacing kernel resources that would otherwise be shared. The intended level of isolation is set to prevent multiple containers that are present on the same host from detecting each other. Every container includes a private root filesystem, which includes a Process ID (PID), namespace, network namespace, and mount namespace.

CF creates container filesystems using the [Garden Rootfs](#) (GrootFS) tool. It stacks the following using OverlayFS:

- A **read-only base filesystem**: This filesystem has the minimal set of operating system packages and Garden-specific modifications common to all containers. Containers can share the same read-only base filesystem because all writes are applied to the read-write layer.
- A **container-specific read-write layer**: This layer is unique to each container and its size is limited by XFS project quotas. The quotas prevent the read-write layer from overflowing into unallocated space.

Resource control is managed using Linux control groups. Associating each container with its own cgroup or job object limits the amount of memory that the container may use. Linux cgroups also require the container to use a fair share of CPU compared to the relative CPU share of other containers.

 **Note:** CF does not support a RedHat Enterprise Linux OS stemcell. This is due to an inherent security issue with the way RedHat handles user namespacing and container isolation.

## CPU

Each container is placed in its own cgroup. Cgroups make each container use a fair share of CPU relative to the other containers. This prevents oversubscription on the host VM where one or more containers hog the CPU and leave no computing resources to the others.

The way cgroups allocate CPU time is based on shares. CPU shares do not work as direct percentages of total CPU usage. Instead, a share is relative in a given time window to the shares held by the other containers. The total amount of CPU that can be overall divided among the cgroups is what is left by other processes that may run in the host VM.

Generally, cgroups offers two possibilities for limiting the CPU usage: *CPU affinity* and *CPU bandwidth*, the latter of which is used in Cloud Foundry.

- CPU affinity: It consists of binding a cgroup to certain CPU cores. The actual amount of CPU cycles that can be consumed by the cgroup is thus limited to what is available on the bound CPU cores.
- CPU bandwidth: Sets the weight of a cgroup with the process scheduler. The process scheduler divides the available CPU cycles among cgroups depending on the shares held by each cgroup, relative to the shares held by the others.  
For example, consider two cgroups, one holding two shares and one holding four. Assuming the process scheduler gets to administer 60 CPU cycles, the first cgroup with two shares will get one third of those available CPU cycles, as it holds one third of the overall shares. Similarly, the second cgroup will get 40 cycles, as it holds two thirds of the collective shares.

The calculation of the CPU usage based on the percentage of the total CPU power available is quite sophisticated and is performed regularly as the CPU demands of the various containers fluctuates. Specifically, the percentage of CPU cycles a cgroup gets can be calculated by dividing the `cpu.shares` it holds by the sum of the `cpu.shares` of all the cgroups that are currently doing CPU activity:

```
process_cpu_share_percent = cpu.shares / sum_cpu_shares *
100
```

In Cloud Foundry, cgroup shares range from 10 to 1024, with 1024 being the default. The actual amount of shares a cgroup gets can be read from the



`cpu.shares` file of the cgroup configurations pseudo-file-system available in the container at `/sys/fs/cgroup/cpu`.

The amount of shares given to an applications cgroup depends on the amount of memory the application declares to need in the manifest. Cloud Foundry scales the number of allocated shares linearly with the amount of memory, with an app instance requesting 8G of memory getting the upper limit of 1024 shares.

```
process_cpu.shares = max((application_memory / 8),
1024)
```

The next example helps to illustrate this better. Consider three processes. P1, P2 and P3, which are assigned `cpu.shares` of 5, 20 and 30, respectively.

P1 is active, while P2 and P3 require no CPU. Hence, P1 may use the whole CPU. When P2 joins in and is doing some actual work (e.g. a request comes in), the CPU share between P1 and P2 will be calculated as follows:

- P1 ->  $5 / (5+20) = 0.2 = 20\%$
- P2 ->  $20 / (5+20) = 0.8 = 80\%$
- P3 (idle)

At some point process P3 joins in as well. Then the distribution will be recalculated again:

- P1 ->  $5 / (5+20+30) = 0.0909 = \sim 9\%$
- P2 ->  $20 / (5+20+30) = 0.363 = \sim 36\%$
- P3 ->  $30 / (5+20+30) = 0.545 = \sim 55\%$

Should P1 become idle, the following recalculation between P2 and P3 takes place:

- P1 (idle)
- P2 ->  $20 / (20+30) = 0.4 = 40\%$
- P3 ->  $30 / (20+30) = 0.6 = 60\%$

If P3 finishes or becomes idle then P2 can consume all the CPU as another recalculation will be performed.

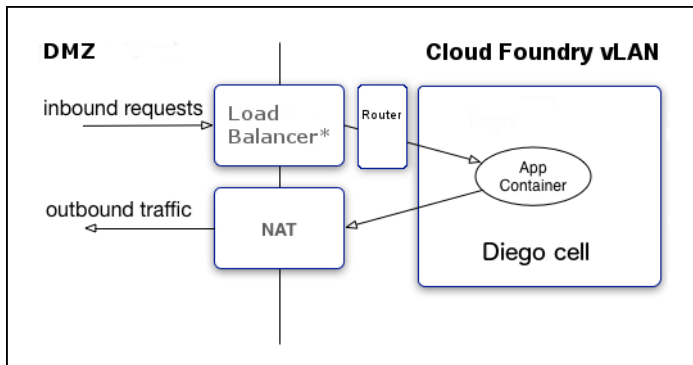
**Summary:** The cgroup shares are the minimum guaranteed CPU share that the process can get. This limitation becomes effective only when processes on the same host compete for resources.

## Inbound and Outbound Traffic from CF

### Networking Overview

A host VM has a single IP address. If you configure the deployment with the cluster on a VLAN, as recommended, then all traffic goes through the following levels of network address translation, as shown in the diagram below.

- **Inbound** requests flow from the load balancer through the router to the host cell, then into the application container. The router determines which application instance receives each request.
- **Outbound** traffic flows from the application container to the cell, then to the gateway on the cell's virtual network interface. Depending on your IaaS, this gateway may be a NAT to external networks.



## Network Traffic Rules

Administrators configure rules to govern container network traffic. This is how containers send traffic outside of CF and receive traffic from outside, the Internet. These rules can prevent system access from external networks and between internal components and determine if apps can establish connections over the virtual network interface.

Administrators configure these rules at two levels:

- Application Security Groups (ASGs) apply network traffic rules at the container level. For information about creating and configuring ASGs, see [Application Security Groups](#).
- Container-to-Container networking policies determine app-to-app communication. Within CF, apps can communicate directly with each other, but the containers are isolated from outside CF. For information about administering container-to-container network policies, see [Administering Container-to-Container Networking](#).

## Container Security

CF secures containers through the following measures:

- Running application instances in [unprivileged](#) containers by default
- [Hardening](#) containers by limiting functionality and access rights
- Allowing administrators to configure ASGs to block outbound connections from application containers. For information about creating and configuring ASGs, see [Application Security Groups](#).

## Types

Garden has two container types: unprivileged and privileged. Currently, CF runs all application instances and staging tasks in unprivileged containers by default. This measure increases security by eliminating the threat of root escalation inside the container.

Formerly, CF ran apps based on Docker images in unprivileged containers, and buildpack-based apps and staging tasks in privileged containers. CF ran apps based on Docker images in unprivileged containers because Docker images come with their own root filesystem and user, so CF could not trust the root filesystem and could not assume that the container user process would never be root. CF ran build-pack based apps and staging tasks in privileged containers because they used the cflinuxfs2 root filesystem and all processes were run as the unprivileged user `vcap`.

## Hardening

CF mitigates against container breakout and denial of service attacks in the following ways:

- CF uses the full set of [Linux namespaces](#) [↗](#) (IPC, Network, Mount, PID, User, UTS) to provide isolation between containers running on the same host. The User namespace is not used for privileged containers.
- In unprivileged containers, CF maps UID/GID 0 (root) inside the container user namespace to a different UID/GID on the host to prevent an app from inheriting UID/GID 0 on the host if it breaks out of the container.
  - CF uses the same UID/GID for all containers.
  - CF maps all UIDs except UID 0 to themselves. CF maps UID 0 inside the container namespace to `MAX_UID-1` outside of the container namespace.
  - Container Root does not grant Host Root permissions.
- CF mounts `/proc` and `/sys` as read-only inside containers.
- CF disallows `dmesg` access for unprivileged users and all users in unprivileged containers.
- CF uses `chroot` when importing docker images from docker registries.
- CF establishes a container-specific overlay filesystem mount. CF uses `pivot_root` [↗](#) to move the root filesystem into this overlay, in order to isolate the container from the host system's filesystem.
- CF does not call any binary or script inside the container filesystem, in order to eliminate any dependencies on scripts and binaries inside the root filesystem.
- CF avoids side-loading binaries in the container through bind mounts or other methods. Instead, it re-executes the same binary by reading it from `/proc/self/exe` whenever it needs to run a binary in a container.
- CF establishes a virtual Ethernet pair for each container for network traffic. See the [Container Network Traffic](#) section above for more information. The virtual Ethernet pair has the following features:

- One interface in the pair is inside the container's network namespace, and is the only non-loopback interface accessible inside the container.
  - The other interface remains in the host network namespace and is bridged to the container-side interface.
  - Egress whitelist rules are applied to these interfaces according to Application Security Groups (ASGs) configured by the administrator.
  - First-packet logging rules may also be enabled on TCP whitelist rules.
  - DNAT rules are established on the host to enable traffic ingress from the host interface to whitelisted ports on the container-side interface.
- CF applies disk quotas using container-specific XFS quotas with the specified disk-quota capacity.
  - CF applies a total memory usage quota through the memory cgroup and destroys the container if the memory usage exceeds the quota.
  - CF applies a fair-use limit to CPU usage for processes inside the container through the `cpu.shares` control group.
  - CF limits access to devices using cgroups but explicitly whitelists the following safe device nodes:
    - `/dev/full`
    - `/dev/fuse`
    - `/dev/null`
    - `/dev/ptmx`
    - `/dev/pts/*`
    - `/dev/random`
    - `/dev/tty`
    - `/dev/tty0`
    - `/dev/tty1`
    - `/dev/urandom`
    - `/dev/zero`
    - `/dev/tap`
    - `/dev/tun`
  - CF drops the following [Linux capabilities](#) for all container processes. Every dropped capability limits the actions the root user can perform.
    - `CAP_DAC_READ_SEARCH`
    - `CAP_LINUX_IMMUTABLE`
    - `CAP_NET_BROADCAST`
    - `CAP_NET_ADMIN`
    - `CAP_IPC_LOCK`
    - `CAP_IPC_OWNER`
    - `CAP_SYS_MODULE`
    - `CAP_SYS_RAWIO`
    - `CAP_SYS_PTRACE`
    - `CAP_SYS_PACCT`
    - `CAP_SYS_BOOT`
    - `CAP_SYS_NICE`
    - `CAP_SYS_RESOURCE`
    - `CAP_SYS_TIME`
    - `CAP_SYS_TTY_CONFIG`
    - `CAP_LEASE`
    - `CAP_AUDIT_CONTROL`
    - `CAP_MAC_OVERRIDE`
    - `CAP_MAC_ADMIN`
    - `CAP_SYSLOG`
    - `CAP_WAKE_ALARM`
    - `CAP_BLOCK_SUSPEND`
    - `CAP_SYS_ADMIN` (for unprivileged containers)

## Container-to-Container Networking

This topic provides an overview of how Container-to-Container Networking works.

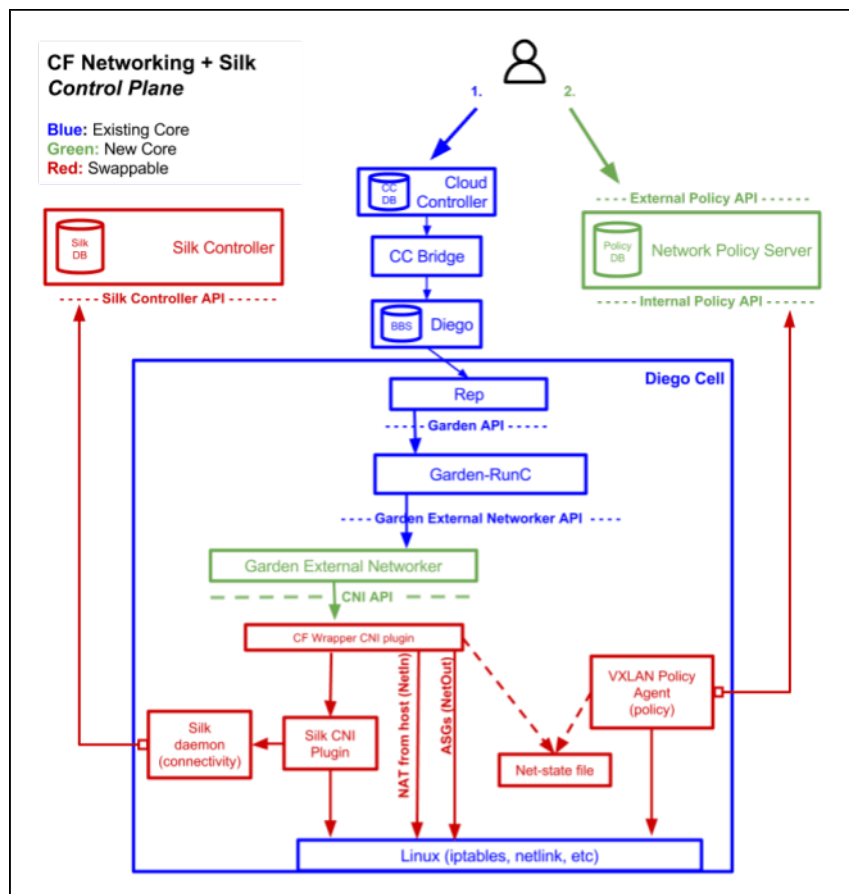
The Container-to-Container Networking feature enables app instances to communicate with each other directly. Container-to-Container Networking is always enabled in PAS. For more information about how to configure Container-to-Container Networking, see the [Administering Container-to-Container Networking](#) topic.

## Architecture

### Overview

Container-to-Container Networking integrates with [Garden-runC](#) in a [Diego](#) deployment. The [Container-to-Container Networking BOSH release](#) includes several core components, as well as swappable components.

To understand the components and how they work, see the diagram and tables below. The diagram highlights Pivotal Application Service components in blue and green. The diagram also highlights swappable components in red.



### Core Components

The Container-to-Container Networking BOSH release includes the following core components:

| Part                                                 | Function                                                                                                                                                                                                             |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Foundry Command Line Interface (CF CLI) plugin | A plugin that you download to control network access policies between apps.                                                                                                                                          |
|                                                      | A central management node that does the following: <ul style="list-style-type: none"> <li>Maintains a database of policies for traffic between apps. The CF CLI plugin calls an API to create or update a</li> </ul> |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Server             | record in the policy database whenever you create or remove a policy. <ul style="list-style-type: none"> <li>Exposes a JSON REST API used by the CF CLI plugin</li> </ul>                                                                                                                                                                                                                                                                    |
| Garden External Networker | A Garden-runC add-on deployed to every Diego cell that does the following: <ul style="list-style-type: none"> <li>Invokes the CNI plugin component to set up the network for each app</li> <li>Forwards ports to support incoming connections from the Gorouter, TCP Router, and Diego SSH Proxy. This keeps apps externally reachable.</li> <li>Installs outbound whitelist rules to support Application Security Groups (ASGs).</li> </ul> |

## Swappable Components

The Container-to-Container Networking BOSH release includes the following swappable components:

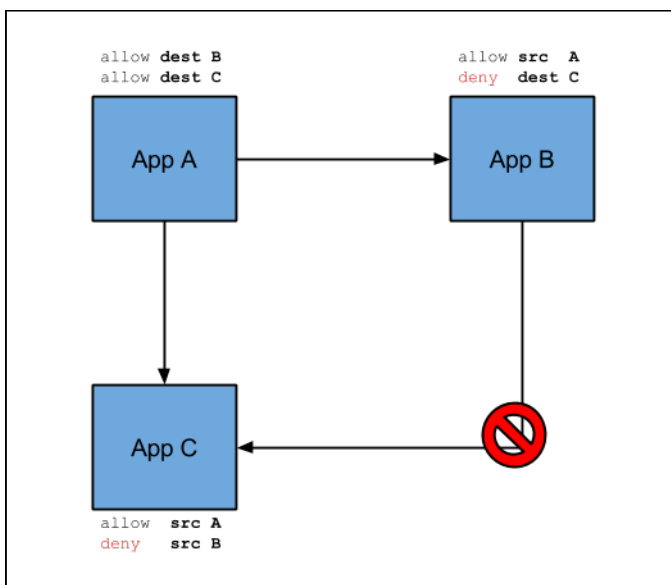
| Part               | Function                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Silk CNI plugin    | A plugin that provides IP address management and network connectivity to app instances as follows: <ul style="list-style-type: none"> <li>Uses a shared VXLAN overlay network to assign each container a unique IP address</li> <li>Installs network interface in container using the Silk VXLAN backend. This is a shared, flat L3 network.</li> </ul>                                                  |
| VXLAN Policy Agent | Enforces network policy for traffic between apps as follows: <ul style="list-style-type: none"> <li>Discovers desired network policies from the Policy Server Internal API</li> <li>Updates iptables rules on the Diego cell to allow whitelisted inbound traffic</li> <li>Tags outbound traffic with the unique identifier of the source app using the VXLAN Group-Based Policy (GBP) header</li> </ul> |

## App Instance Communication

The diagram below illustrates how app instances communicate in a deployment with Container-to-Container Networking enabled. In this example, the operator creates two policies to regulate the flow of traffic between **App A**, **App B**, and **App C**.

- Allow traffic from **App A** to **App B**
- Allow traffic from **App A** to **App C**

If traffic and its direction is not explicitly allowed, it is denied. For example, **App B** cannot send traffic to **App C**.



## Overlay Network

Container-to-Container Networking uses an overlay network to manage communication between app instances.


Overlay networks are not externally routable, and traffic sent between containers does not exit the overlay. You can use the same overlay network range for different Cloud Foundry deployments in your environment.


The overlay network range defaults to `10.255.0.0/16`. You can modify the default to any [RFC 1918](#) range that meets the following requirements:

- The range is not used by services that app containers access.
- The range is not used by the underlying Cloud Foundry infrastructure.

All Diego cells in your Cloud Foundry deployment share this overlay network. By default, each cell is allocated a /24 range that supports 254 containers per cell, one container for each of the usable IP addresses, `.1` through `.254`. To modify the number of Diego cells your overlay network supports, see [Overlay Network](#) in *Configuring Container-to-Container Networking*.

Cloud Foundry container networking is currently supported only on Linux.

 **warning:** The overlay network IP address range must not conflict with any other IP addresses in the network. If a conflict exists, Diego cells cannot reach any endpoint that has a conflicting IP address.

 **Note:** Traffic to app containers from the Gorouter or from app containers to external services uses cell IP addresses and NAT, not the overlay network.

## Policies

Enabling Container-to-Container Networking for your deployment allows you to create policies for communication between app instances. The Container-to-Container Networking feature also provides a unique IP address to each app container and provides direct IP reachability between app instances.

The policies you create specify a source app, destination app, protocol, and port so that app instances can communicate directly without going through the Gorouter, a load balancer, or a firewall. Container-to-Container Networking supports UDP and TCP, and you can configure policies for multiple ports. These policies apply immediately without having to restart the app.

Additionally, policies use and track the GUIDs of the apps. The policies continue to work when apps redeploy, or if they crash and Diego places them in a new container. Pushing a brand new app requires a new policy, but not updates to an existing app because an app always retains its GUID.

## App Service Discovery

The Pivotal Application Service platform supports DNS-based service discovery that lets apps find each others' internal addresses. For example, a front end app instance can use the service discovery mechanism to establish communications with a back end app instance. See the [Developer Guide](#) for how to set up and use app service discovery.

Container-to-Container app service discovery does not provide client-side load balancing or circuit-breaking, and it does not apply to `cf marketplace` services or require [application binding](#). It just lets apps publish service endpoints to each other, unbrokered and unmediated.

## Alternative Network Stacks

The BOSH release that contains the Container-to-Container Networking feature is composed of a pluggable network stack. Advanced users or third-party vendors can integrate a different network stack. For more information about third-party plugins, see the [Container-to-Container Networking BOSH release](#) documentation.

## Container-to-Container Networking versus ASGs

Both application security groups (ASGs) and Container-to-Container Networking policies affect traffic from app instances. The following table highlights differences between ASGs and Container-to-Container Networking policies.

|                    | ASGs                                | Container-to-Container Networking Policies                   |
|--------------------|-------------------------------------|--------------------------------------------------------------|
| Policy granularity | From a space to an IP address range | From a source app to a destination app                       |
| Scope              | For a space, org, or deployment     | For app to app only                                          |
| Traffic direction  | Outbound control                    | Policies apply for incoming packets from other app instances |

|                      |                   |                                                |
|----------------------|-------------------|------------------------------------------------|
| Source app           | Is not known      | Is identified because of direct addressability |
| Policies take affect | After app restart | Immediately                                    |

## Application Security Groups

Page last updated:

This topic provides an overview of Application Security Groups (ASGs), and describes how to manage and administer them. Many of the steps below require the [Cloud Foundry Command Line Interface](#) (cf CLI) tool.



**Note:** If you are creating ASGs for the first time, see [Restricting App Access to Internal PCF Components](#).

## About Application Security Groups

Application Security Groups (ASGs) are a collections of egress rules that specify the protocols, ports, and IP address ranges where app or task instances send traffic.

ASGs define **allow** rules, and their order of evaluation is unimportant when multiple ASGs apply to the same space or deployment. The platform sets up rules to filter and log outbound network traffic from app and task instances. ASGs apply to both buildpack-based and Docker-based apps and tasks.

## Staging and Running ASGs

Administrators can define a `staging` ASG for app and task staging, and a `running` ASG for app and task runtime.

When apps or tasks begin staging, they require traffic rules permissive enough to allow them to pull resources from the network. A running app or task no longer needs to pull resources, so traffic rules can be more restrictive and secure. To distinguish between these two security requirements, administrators can define a `staging` ASG for app and task staging with more permissive rules, and a `running` ASG for app and task runtime with less permissive rules.

## Platform-Wide and Space-Scoped ASGs

To provide granular control when securing a deployment, administrators can assign platform-wide ASGs that apply to all app and task instances for the entire deployment, or space-scoped ASGs that apply only to apps and tasks in a particular space.

In environments with both platform-wide and space-specific ASGs, the ASGs for a particular space combine with the platform ASGs to determine the rules for that space.

## Simplifying ASGs with a Services Subnet

ASGs can be complicated to configure correctly, especially when the specific IP addresses listed in a group change.

To simplify securing a deployment while still allowing apps reach external services, operators can deploy the services into a subnet that is separate from their Cloud Foundry deployment, then create ASGs for the apps that whitelist those service subnets, while denying access to any virtual machine (VM) hosting other apps.

For examples of typical ASGs, see the [Typical Application Security Groups](#) section of this topic.

## Default ASGs

Pivotal Application Service (PAS) defines one default ASG, `default_security_group`. This group allows all outbound traffic from application containers on public and private networks except for the link-local range, `169.254.0.0/16`, which is blocked.



**warning:** For security, PAS administrators must [modify the default ASGs](#) so that outbound network traffic cannot access internal components.

The ASG is defined in the Cloud Controller configuration as follows:

```
security_group_definitions:
- name: default_security_group
 rules:
 - protocol: all
```



```
destination: 0.0.0.0-169.253.255.255
- protocol: all
destination: 169.255.0.0-255.255.255.255
```

## ASG Sets

ASGs are applied by configuring ASG sets differentiated by *scope*, platform-wide or space specific, and *lifecycle*, staging or running.

Currently, four ASG sets exist in Cloud Foundry:

- Platform-wide staging ASG set, also called “default-staging”
- Platform-wide running ASG set, also called “default-running”
- Space-scoped staging ASG set
- Space-scoped running ASG set


In environments with both platform-wide and space-specific ASG sets, combine the ASG sets for a particular space with the platform ASG sets to determine the rules for that space.

The following table indicates the differences between the four sets.

| When an ASG is bound to the... | the ASG rules are applied to...                                         |
|--------------------------------|-------------------------------------------------------------------------|
| Platform-wide staging ASG set  | the staging lifecycle for all apps and tasks.                           |
| Platform-wide running ASG set  | the running lifecycle for all app and task instances.                   |
| Space-scoped staging ASG set   | the staging lifecycle for apps and tasks in a particular space.         |
| Space-scoped running ASG set   | the running lifecycle for app and task instances in a particular space. |

Typically, ASGs applied during the staging lifecycle are more permissive than the ASGs applied during the running lifecycle. This is because staging often requires access to different resources, such as dependencies.

You use different commands to apply an ASG to each of the four sets. For more information, see the [Procedures](#) section of this topic.

 **Note:** To apply a staging ASG to apps within a space, you must use cf CLI 6.28.0 or later.

## The Structure and Attributes of ASGs


ASG rules are specified as a JSON array of ASG objects. An ASG object has the following attributes:

| Attribute                | Description                                                                                                                                                                                    | Notes                                                                                                   |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| <code>protocol</code>    | <code>tcp</code> , <code>udp</code> , <code>icmp</code> , or <code>all</code>                                                                                                                  | Required                                                                                                |
| <code>destination</code> | A single IP address, an IP address range like <code>192.0.2.0-192.0.2.50</code> , or a CIDR block that can receive traffic                                                                     |                                                                                                         |
| <code>ports</code>       | A single port, multiple comma-separated ports, or a single range of ports that can receive traffic. Examples: <code>443</code> , <code>80,8080,8081</code> , <code>8080-8081</code>            | Only possible if <code>protocol</code> is <code>tcp</code> or <code>udp</code> .                        |
| <code>code</code>        | ICMP code                                                                                                                                                                                      | Required when <code>protocol</code> is <code>icmp</code> . A value of <code>-1</code> allows all codes. |
| <code>type</code>        | ICMP type                                                                                                                                                                                      | Required when <code>protocol</code> is <code>icmp</code> . A value of <code>-1</code> allows all types. |
| <code>log</code>         | Set to <code>true</code> to enable logging. For more information about how to configure system logs to be sent to a syslog drain, see the <a href="#">Using Log Management Services</a> topic. | Logging is only supported with protocol type <code>tcp</code>                                           |
| <code>description</code> | An optional text field for operators managing security group rules                                                                                                                             |                                                                                                         |

## Process for Administering ASGs

The following table outlines the flow of tasks that the administrator carries out over the lifecycle of ASGs. Procedures for each of these tasks are given in

Managing ASGs with the `cf` CLI below.

 **Note:** If you are creating ASGs for the first time, see [Restricting App Access to Internal PCF Components](#).

|    | Task                                                                                                            | For more information, see                                  |
|----|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| 1. | Review the existing ASGs. If this is a new deployment, these consist of only the <a href="#">Default ASGs</a> . | <a href="#">View ASGs</a>                                  |
| 2. | Create new ASGs.                                                                                                | <a href="#">Create ASGs</a>                                |
| 3. | Update the existing ASGs.                                                                                       | <a href="#">Update ASGs</a>                                |
| 4. | Bind ASGs to an ASG set.                                                                                        | <a href="#">Bind ASGs</a>                                  |
| 5. | If you need to delete an ASG, first unbind it, then delete it.                                                  | <a href="#">Unbind ASGs</a><br><a href="#">Delete ASGs</a> |


## Managing ASGs with the `cf` CLI

This section provides the commands you need to create and manage ASGs.

### View ASGs

Run the following `cf` CLI commands to view information about existing ASGs:

| Command                                       | Output                                                                                                   |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <code>cf security-groups</code>               | All ASGs                                                                                                 |
| <code>cf staging-security-groups</code>       | All ASGs applied to the platform-wide staging ASG set                                                    |
| <code>cf running-security-groups</code>       | All ASGs applied to the platform-wide running ASG set                                                    |
| <code>cf security-group SECURITY-GROUP</code> | All rules in the ASG named <code>SECURITY-GROUP</code> , for example, <code>cf security-group dns</code> |

 **Note:** You can also view ASGs in Apps Manager under the **Settings** tab of a space or an app.

### Create ASGs

To create an ASG, perform the following steps:

1. Create a rules file: a JSON-formatted single array containing objects that describe the rules. See the following example, which allows ICMP traffic of code `1` and type `0` to all destinations, and TCP traffic to `10.0.11.0/24` on ports `80` and `443`. Also see [The Structure and Attributes of ASGs](#).

```
[
 {
 "protocol": "icmp",
 "destination": "0.0.0.0/0",
 "type": 0,
 "code": 0
 },
 {
 "protocol": "tcp",
 "destination": "10.0.11.0/24",
 "ports": "80,443",
 "log": true,
 "description": "Allow http and https traffic from ZoneA"
 }
]
```



2. Run `cf create-security-group SECURITY-GROUP PATH-TO-RULES-FILE`. Replace `SECURITY-GROUP` with the name of your security group, and `PATH-TO-RULES-FILE` with the absolute or relative path to a rules file.

In the following example, `my-asg` is the name of a security group, and `~/workspace/my-asg.json` is the path to a rules file.

```
$ cf create-security-group my-asg ~/workspace/my-asg.json
```

After the ASG is created, you must bind it to an ASG set before it takes effect. See [Bind ASGs](#) below.

## Bind ASGs

 **Note:** Binding an ASG does not affect started apps until you restart them. To restart all of the apps in an org or a space, use the [app-restarter](#)  cf CLI plugin.

To apply an ASG, you must first bind it to an ASG set.

To bind an ASG to the platform-wide staging ASG set, run `cf bind-staging-security-group SECURITY-GROUP`. Replace `SECURITY-GROUP` with the name of your security group.

Example:

```
$ cf bind-staging-security-group my-asg
```

To bind an ASG to the platform-wide running ASG set, run `cf bind-running-security-group SECURITY-GROUP` command. Replace `SECURITY-GROUP` with the name of your security group.

Example:

```
$ cf bind-running-security-group my-asg
```

To bind an ASG to a space-scoped running ASG set, run `cf bind-security-group SECURITY-GROUP ORG SPACE`. Replace `SECURITY-GROUP` with the name of your security group. Replace `ORG` and `SPACE` with the org and space where you want to bind the ASG set.

Example:

```
$ cf bind-security-group my-asg my-org my-space
```

To bind an ASG to a space-scoped staging ASG set, run `cf bind-security-group SECURITY-GROUP ORG SPACE --lifecycle staging`. Replace `SECURITY-GROUP` with the name of your security group. Replace `ORG` and `SPACE` with the org and space where you want to bind the ASG set.



## Update ASGs

To update an existing ASG, perform the following steps.



1. Edit the ASG rules in the JSON file.
2. Run `cf update-security-group SECURITY-GROUP PATH-TO-RULES-FILE`. Replace `SECURITY-GROUP` with the name of the existing ASG you want to change, and `PATH-TO-RULES-FILE` with the absolute or relative path to a rules file.

In the following example, `my-asg` is the name of a security group, and `~/workspace/my-asg-v2.json` is the path to a rules file.

```
$ cf update-security-group my-asg ~/workspace/my-asg-v2.json
```

 **Note:** Updating an ASG does not affect started apps until you restart them. To restart all of the apps in an org or a space, use the [app-restarter](#)  cf CLI plugin.

## Unbind ASGs

 **Note:** Unbinding an ASG does not affect started apps until you restart them. To restart all of the apps in an org or a space, use the [app-restarter](#)  cf CLI plugin.

To unbind an ASG from the platform-wide staging ASG set, run `cf unbind-staging-security-group SECURITY-GROUP`. Replace `SECURITY-GROUP` with the name of your security group.

Example:

```
$ cf unbind-staging-security-group my-asg
```

To unbind an ASG from the platform-wide running ASG set, run `cf unbind-running-security-group SECURITY-GROUP`. Replace `SECURITY-GROUP` with the name of your security group.

Example:


```
$ cf unbind-running-security-group my-asg
```

To unbind an ASG from a specific space, run `cf unbind-security-group SECURITY-GROUP ORG SPACE --lifecycle running`. Replace `SECURITY-GROUP` with the name of your security group. Replace `ORG` and `SPACE` with the org and space where you want to unbind the ASG set, and replace `running` with `staging` if you want to unbind from the staging ASG set.

Example:

```
$ cf unbind-security-group my-asg my-org my-space --lifecycle staging
```

## Delete ASGs

 **Note:** You can only delete unbound ASGs. To unbind ASGs, see [Unbind ASGs](#) above.


To delete an ASG, run `cf delete-security-group SECURITY-GROUP`. Replace `SECURITY-GROUP` with the name of your security group.

Example:

```
$ cf delete-security-group my-asg
```

## Typical ASGs

Below are examples of typical ASGs. Configure your ASGs in accordance with your organization's network access policy for untrusted apps.

| ASG                             | For access to                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>dns</code>                | DNS, either public or private                                                                                                                    |
| <code>public-networks</code>    | Public networks, excluding IaaS metadata endpoints                                                                                               |
| <code>private-networks</code>   | Private networks in accordance with <a href="#">RFC-1918</a>  |
| <code>load-balancers</code>     | The internal Pivotal Application Service load balancer and others                                                                                |
| <code>internal-proxies</code>   | Internal proxies                                                                                                                                 |
| <code>internal-databases</code> | Internal databases                                                                                                                               |

## DNS


To resolve hostnames to IP addresses, apps require DNS server connectivity, which typically use port 53. Administrators should create or update a `dns` ASG with appropriate rules. Administrators may further restrict the DNS servers to specific IP addresses or ranges of IP addresses.

Example `dns` ASG:

```
[
 {
 "protocol": "tcp",
 "destination": "0.0.0.0/0",
 "ports": "53"
 },
 {
 "protocol": "udp",
 "destination": "0.0.0.0/0",
 "ports": "53"
 }
]
```

## Public Networks

Apps often require public network connectivity to retrieve app dependencies, or to integrate with services available on public networks. Example app dependencies include public Maven repositories, NPM, RubyGems, and Docker registries.

 **Note:** You should exclude IaaS metadata endpoints, such as `169.254.169.254`, because the metadata endpoint can expose sensitive environment information to untrusted apps. The `public_networks` example below accounts for this recommendation.

Example `public_networks` ASG:

```
[
 {
 "destination": "0.0.0.0-9.255.255.255",
 "protocol": "all"
 },
 {
 "destination": "11.0.0.0-169.253.255.255",
 "protocol": "all"
 },
 {
 "destination": "169.255.0.0-172.15.255.255",
 "protocol": "all"
 },
 {
 "destination": "172.32.0.0-192.167.255.255",
 "protocol": "all"
 },
 {
 "destination": "192.169.0.0-255.255.255.255",
 "protocol": "all"
 }
]
```

## Private Networks

Network connections that are commonly allowable in private networks include endpoints such as proxy servers, Docker registries, load balancers, databases, messaging servers, directory servers, and file servers. Configure appropriate private network ASGs as appropriate. You may find it helpful to use a naming convention with `private_networks` as part of the ASG name, such as `private_networks_databases`.

 **Note:** You should exclude any private networks and IP addresses that app and task instances should not have access to.

Example `private_networks` ASG:

```
[
 {
 "protocol": "tcp",
 "destination": "10.0.0.0-10.255.255.255",
 "ports": "443"
 },
 {
 "protocol": "tcp",
 "destination": "172.16.0.0-172.31.255.255",
 "ports": "443"
 },
 {
 "protocol": "tcp",
 "destination": "192.168.0.0-192.168.255.255",
 "ports": "443"
 }
]
```

## Marketplace Services

Each installed Marketplace Service requires its own set of ASG rules to function properly. See the installation instructions for each installed Marketplace Service to determine which ASG rules it requires. For more information about how to provision and integrate services, see the [Services Overview](#) topics.

## About the ASG Creator Tool

The ASG Creator is a command line tool that you can use to create JSON rules files. The ASG Creator lets you specify IP addresses, CIDRs, and IP address ranges that you want to disallow traffic to, as well as the addresses that you want to allow traffic to. Based on these disallow/allow (exclude/include) lists that you provide as input, the ASG Creator formulates a JSON file of allow rules.

In turn, the JSON file is the input for the `cf create-security-group` command that creates an ASG.

You can download the latest release of the ASG Creator from the Cloud Foundry incubator repository on Github: <https://github.com/cloudfoundry-incubator/asg-creator/releases/latest>

## ASG Logging

The KB article [How to use Application Security Group \(ASG\) logging](#) describes how you can use ASGs to correlate emitted logs back to an app.

## GrootFS Disk Usage

Page last updated:

This topic explains the concepts related to GrootFS disk space management in Pivotal Application Service.

## GrootFS Stores

GrootFS is the container root filesystem management component for Garden. A container root filesystem or *rootfs* is often referred to as an **image**.

A **GrootFS store** is the directory in which rootfs layers and container images are cached. This directory is configured by GrootFS and mounted on an XFS-formatted volume by the Garden job during BOSH VM creation.

Individual container root filesystems are provided via OverlayFS mounts.

Supplying GrootFS with an already formatted XFS volume for its store is not yet supported for BOSH-controlled deployments.

## General Garbage Collection Behavior in GrootFS Stores

GrootFS stores are initialized to use the entirety of `/var/vcap/data`. If the `reserved_space_for_other_jobs_in_mb` is not set high enough, or if there are many images with few shared volumes, the store can use up all available space.

The thresholder component calculates and sets a value so that GrootFS's garbage collector can attempt to ensure that a small reserved space is kept free for other jobs. GrootFS only tries to garbage collect when that threshold is reached. However, if all the rootfs layers are actively in use by images, then garbage collection cannot occur and that space is used up.

## Volumes

Underlying layers in rootfs images are known as `volumes` in GrootFS. They are read-only and their changesets are layered together through an **OverlayFS** mount to create the root filesystems for containers.

When GrootFS writes each filesystem volume to disk, it also stores the number of bytes written to a file in a `meta` directory. The size of an individual volume is available in its corresponding metadata file. GrootFS also stores the SHA of each underlying volume used by an image in the `meta` folder.

For each container, GrootFS mounts the underlying `volumes` using overlay to a point in the `images` directory. This mount point is the rootfs for the container and is read-write.

On disk, the read-write layer for each container can be found at `/var/vcap/data/grootfs/store/unprivileged/images/CONTAINER-ID/diff` (or `/var/vcap/data/grootfs/store/privileged/images/CONTAINER-ID/diff` for privileged containers.)

When GrootFS calls on the built-in XFS quota tooling to get disk usage for a container, it takes into account data written to those `diff` directories and not the data in the read-only volumes.

## Volume Cleanup Example

When `clean` is called in GrootFS, any layers that are not being used by an existing rootfs are deleted from the store. The cleanup only takes into account the `volumes` folders in the store.

For example, imagine that there are two rootfs images from different base images, Image A and Image B:

```
- Image A
Layers:
- layer-1
- layer-2
- layer-3
```

```
- Image B
Layers:
- layer-1
- layer-4
- layer-5
```

They have a layer in common, layer-1. And after deleting Image B, layer-4 and layer-5 can be collected by clean, but not layer-1 because Image A still uses that layer.

For more information on how to calculate GrootFS disk usage in your deployment, see [Examining GrootFS Disk Usage](#).

## Additional Information

For more information, see the following sections of `garden-runc-release` :

- [overlay-xfs-setup](#) [↗](#)
- [grootfs-utils](#) [↗](#)
- [threshold](#) [↗](#)

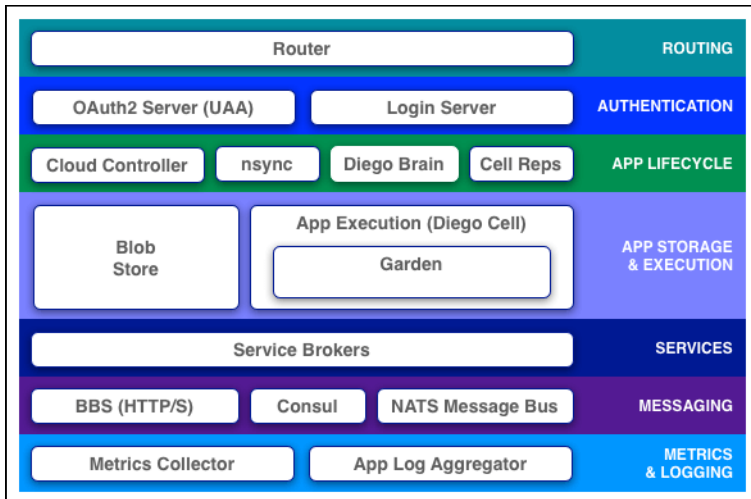


## Cloud Foundry Components

Page last updated:

Cloud Foundry components include a self-service application execution engine, an automation engine for application deployment and lifecycle management, and a scriptable command line interface (CLI), as well as integration with development tools to ease deployment processes. Cloud Foundry has an open architecture that includes a buildpack mechanism for adding frameworks, an application services interface, and a cloud provider interface.

See the descriptions below for more information about Cloud Foundry components. Some descriptions include links to more detailed documentation.



## Routing

### Router

The [router](#) routes incoming traffic to the appropriate component, either a Cloud Controller component or a hosted application running on a Diego Cell.

The router periodically queries the Diego Bulletin Board System (BBS) to determine which cells and containers each app currently runs on. Using this information, the router recomputes new routing tables based on the IP addresses of each cell virtual machine (VM) and the host-side port numbers for the cell's containers.

## Authentication

### OAuth2 Server (UAA) and Login Server

The OAuth2 server (the [UAA](#)) and Login Server work together to provide identity management.

## App Lifecycle

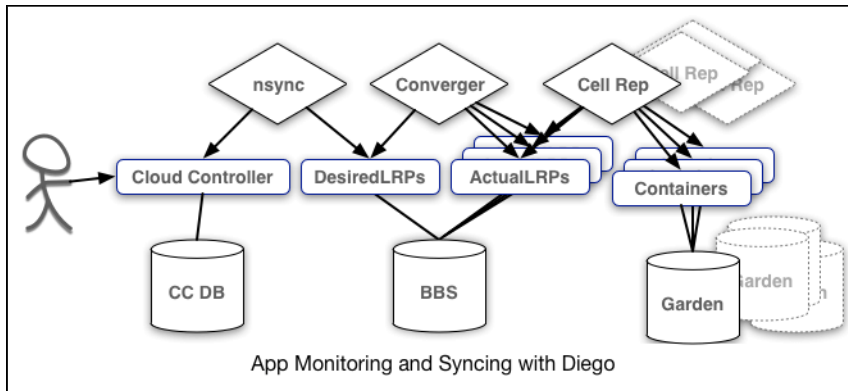
### Cloud Controller and Diego Brain

The [Cloud Controller](#) (CC) directs the deployment of apps. To push an app to Cloud Foundry, you target the Cloud Controller. The Cloud Controller then directs the Diego Brain through the CC-Bridge components to coordinate individual [Diego cells](#) to stage and run apps.

The Cloud Controller also maintain records of [orgs](#), [spaces](#), [user roles](#), [services](#) [↗](#), and more.

## nsync, BBS, and Cell Reps

To keep apps available, cloud deployments must constantly monitor their states and reconcile them with their expected states, starting and stopping processes as required.



The nsync, BBS, and Cell Rep components work together along a chain to keep apps running. At one end is the user. At the other end are the instances of apps running on widely-distributed VMs, which may crash or become unavailable.

Here is how the components work together:

- **nsync** receives a message from the Cloud Controller when the user scales an app. It writes the number of instances into a `DesiredLRP` structure in the Diego BBS database.
- **BBS** uses its convergence process to monitor the `DesiredLRP` and `ActualLRP` values. It launches or kills app instances as appropriate to ensure the `ActualLRP` count matches the `DesiredLRP` count.
- **Cell Rep** monitors the containers and provides the `ActualLRP` value.

## App Storage and Execution

### Blobstore

The blobstore is a repository for large binary files, which GitHub cannot easily manage because GitHub is designed for code. The blobstore contains the following:

- Application code packages
- Buildpacks
- Droplets

You can configure the blobstore as either an internal server or an external S3 or S3-compatible endpoint. See this [Knowledge Base article](#) for more information about the blobstore.

### Diego Cell

App instances, app tasks, and staging tasks all run as [Garden](#) containers on the Diego Cell VMs. The Diego cell rep component manages the lifecycle of those containers and the processes running in them, reports their status to the Diego BBS, and emits their logs and metrics to [Loggregator](#).

## Services

### Service Brokers

Apps typically depend on [services](#) such as databases or third-party SaaS providers. When a developer provisions and binds a service to an app, the service broker for that service is responsible for providing the service instance.

## Messaging

### Internal HTTPS and BBS

Cloud Foundry component VMs communicate with each other internally through HTTP and HTTPS protocols, sharing temporary messages and data stored in Diego's [Bulletin Board System \(BBS\)](#).

- BOSH Director colocates a [BOSH DNS](#) server on every deployed VM. All VMs keep up-to-date DNS records for all the other VMs in the same foundation, enabling service discovery between VMs. BOSH DNS also provides client-side load-balancing by randomly selecting a healthy VM when multiple VMs are available.
- Diego's [Bulletin Board System](#) (BBS) stores more frequently updated and disposable data such as cell and app status, unallocated work, and heartbeat messages, as well as longer-lived distributed locks. The BBS stores data in MySQL, using the [Go MySQL Driver](#).

The route-emitter component uses the NATS protocol to broadcast the latest routing tables to the routers.

## Metrics and Logging

### Loggregator

The [Loggregator](#) (log aggregator) system streams application logs to developers.

## Cloud Controller

Page last updated:

The Cloud Controller provides REST API endpoints for clients to access the system. The Cloud Controller maintains a database with tables for orgs, spaces, services, user roles, and more.

## Diego Auction

The Cloud Controller uses the [Diego Auction](#) to balance application processes over the [cells](#) in a Cloud Foundry installation.

## Database (CC\_DB)

The Cloud Controller database has been tested with MySQL.

## Blobstore

To stage and run apps, Cloud Foundry manages and stores the following types of binary large object (blob) files:

| Blob Type       | Description                                                                                                                                                                                                                                                                   | Location in Blobstore       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| App Packages    | Full contents of app directories, including source code and resource files, zipped into single blob files.                                                                                                                                                                    | /cc-packages                |
| Buildpacks      | Buildpack directories, which Diego cells download to compile and stage apps with.                                                                                                                                                                                             | /cc-buildpacks              |
| Resource Cache  | Large files from app packages that the Cloud Controller stores with a SHA for later re-use. To save bandwidth, the Cloud Foundry Command Line Interface (cf CLI) only uploads large application files that the Cloud Controller has not already stored in the resource cache. | /cc-resources               |
| Buildpack Cache | Large files that buildpacks generate during staging, stored for later re-use. This cache lets buildpacks run more quickly when staging apps that have been staged previously.                                                                                                 | cc-droplets/buildpack_cache |
| Droplets        | Staged apps packaged with everything needed to run in a container.                                                                                                                                                                                                            | /cc-droplets                |

Cloud Foundry blobstores use the [Fog](#) Ruby gem to store blobs in services like Amazon S3, WebDAV, or the NFS filesystem. The file system location of an internal blobstore is `/var/vcap/store/shared`.

A single blobstore typically stores all five types of blobs, but you can configure the Cloud Controller to use separate blobstores for each type.

## Automatic Blob Cleanup

After a blob deletion fails silently or something else goes wrong, the blobstore may contain blobs that the Cloud Controller no longer needs or lists in its database. These are called orphan blobs, and they waste blobstore capacity.

The Cloud Controller detects and removes orphan blobs by scanning part of the blobstore daily and checking for any blobs that its database does not account for. The process scans through the entire blobstore every week, and only removes blobs that show as orphans for three consecutive days.

The Cloud Controller performs this automatic cleanup when the `cloud_controller_worker` job property `cc.perform_blob_cleanup` is set to `true`.

## Manual Blob Cleanup

The Cloud Controller does not track resource cache and buildpack cache [blob types](#) in its database, so it does not [clean them up automatically](#) as it does with app package, buildpack, and droplet type blobs.

To clean up the buildpack cache, admin users can run `cf curl -X DELETE /v2/blobstores/buildpack_cache`. This empties the buildpack cache completely, which is a safe operation.

To clean up the resource cache, delete it as follows:

- **Internal blobstore:** Run `bosh ssh` to connect to the blobstore VM (NFS or WebDav) and `rm *` the contents of the `/var/vcap/store/shared/cc-resources` directory.
- **External blobstore:** Use the file store's API to delete the contents of the `resources` bucket.

Do not manually delete app package, buildpack, or droplet blobs from the blobstore. To free up resources from those locations, run `cf delete-buildpack` for buildpacks or `cf delete` for app packages and droplets.

## Testing

By default `rspec` runs a test suite with the SQLite in-memory database. Specify a connection string using the `DB_CONNECTION` environment variable to test against MySQL. For example:

```
DB_CONNECTION="mysql2://root:password@localhost:3306/ccng" rspec
```

## Cloud Controller Blobstore

This topic describes how Cloud Controllers and Diego interact with the CC's blobstore.

### Overview

Cloud Foundry uses a blobstore to store the source code that developers push, stage, and run.

This topic references staging and treats all blobstores as generic (S3-style) object stores.

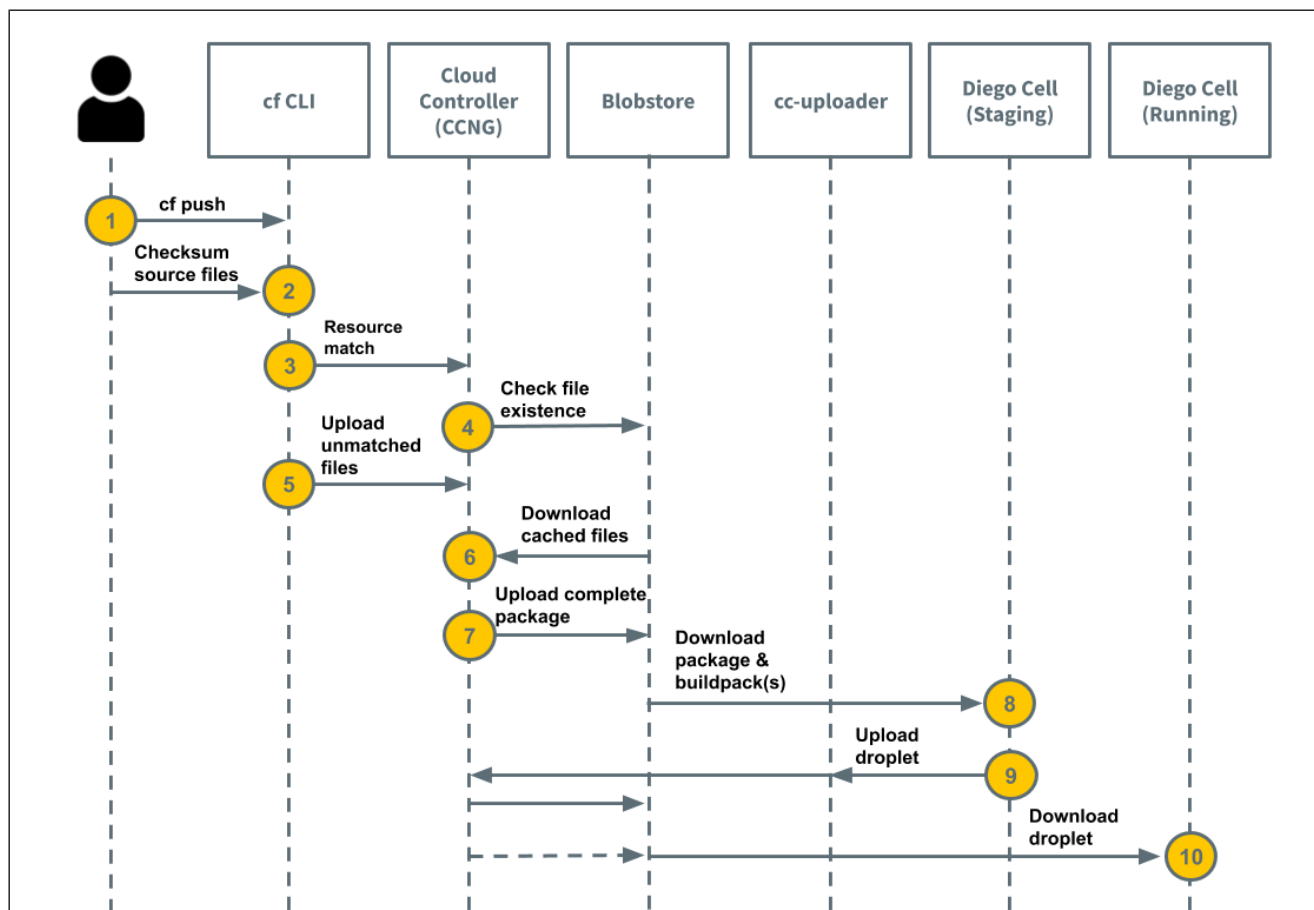
For more general information about staging, see [How Apps Are Staged](#).

For more information about how specific 3rd party blobstores can be configured, see .

### How staging uses the blobstore

This section describes how staging buildpack apps utilizes the blobstore.

The following diagram illustrates, in-depth, how the staging process uses the blobstore:



For a description of each step where staging a buildpack app interacts with the blobstore, see the following:

1. A developer runs `cf push`.
2. The cf CLI gets all the developers local source code files and computes a checksum of each.
3. The cf CLI makes a "Resource Match" request to the cloud controller, listing those files and their checksums.
4. This step, "Check file existence", includes the following:

- a. The Cloud Controller makes a series of “HEAD”-type requests to the blobstore to find out which files it has cached.
  - b. Cloud Controller content-addresses its cached files so that changes to a file result in it being stored as a different object.
  - c. Eventually Cloud Controller is able to compute which files it has and which it needs the CLI to upload.
  - d. In response to the resource match request, Cloud Controller lists the files the CLI needs to upload .
5. The CLI compresses and uploads the unmatched files to the Cloud Controller.
6. Asynchronously, The Cloud Controller downloads the matched files from the blobstore to its local disk.
7. This step includes the following:
  - a. The Cloud Controller zips together the freshly uploaded files with the downloaded cached files.
  - b. The Cloud Controller uploads the complete package to the blobstore.
8. The Diego Cell downloads the package and its buildpack(s) into a container and stages the app.
9. This step includes the following:
  - a. After the app has been staged, the Diego Cell uploads the complete droplet to the cc-uploader.
  - b. The cc-uploader makes a multipart upload request to upload the droplet to the Cloud Controller.
  - c. The Cloud Controller enqueues an asynchronous job to upload the blobstore.
10. This step includes the following:
  - a. The Diego Cell attempts to download the droplet from the Cloud Controller into the app’s container so it can run it.
  - b. The Cloud Controller redirects the Cell’s droplet download request to the blobstore.
  - c. The Diego Cell downloads the app’s droplet from the blobstore and runs it.

## Blobstore load

The shape of the load CC generates on its blobstore is a bit unusual because of resource matching. Many blobstores that perform very well under normal read, write, and delete load are overwhelmed by CC’s heavy usage of HEAD requests during resource matching.

Pushing an app with large number of files will cause the CC to check the blobstore for the existence of each and every one of those files.

Parallel BOSH deploys of Diego Cells can also generate significant read load on CC’s Blobstore as the cells perform [evacuation](#).

## How CC reaps expired packages, droplets, and buildpacks

As new droplets and packages are created, the oldest ones associated with an app are marked as “EXPIRED” if they exceed the configured limits for packages and droplets stored per app.

Nightly, starting at midnight, the Cloud Controller runs a series of jobs to delete the data associated with expired packages, droplets, and buildpacks.

Enabling the native [versioning](#) feature on your blobstore will increase the number of resources stored and increase costs.

## Blobstore Interaction timeouts

The Cloud Controller inherits its default blobstore operation timeouts from [excon](#). Excon defaults to a 60 second read, write, and connect timeouts.

## Messaging (NATS)

Page last updated:

This information was adapted from the [NATS](#) README. NATS is a lightweight publish-subscribe and distributed queueing messaging system written in Ruby. Ops Manager sends all NATS traffic using Transport Layer Security (TLS) encryption by default.

## Install NATS

```
$ gem install nats
or
$ rake geminstall

$ nats-sub foo &
$ nats-pub foo 'Hello World!'
```

## Basic Usage

```
require "nats/client"

NATS.start do

 # Simple Subscriber
 NATS.subscribe('foo') { |msg| puts "Msg received : '#{msg}'" }

 # Simple Publisher
 NATS.publish('foo.bar.baz', 'Hello World!')

 # Unsubscribing
 sid = NATS.subscribe('bar') { |msg| puts "Msg received : '#{msg}'" }
 NATS.unsubscribe(sid)

 # Requests
 NATS.request('help') { |response| puts "Got a response: '#{response}'" }

 # Replies
 NATS.subscribe('help') { |msg, reply| NATS.publish(reply, "I'll help!") }

 # Stop using NATS.stop, exits EM loop if NATS.start started the loop
 NATS.stop

end
```

## Wildcard Subscriptions

```
"*" matches any token, at any level of the subject.
NATS.subscribe('foo.*.baz') { |msg, reply, sub| puts "Msg received on [{sub}] : '#{msg}'" }
NATS.subscribe('foo.bar.*') { |msg, reply, sub| puts "Msg received on [{sub}] : '#{msg}'" }
NATS.subscribe('*.bar.*') { |msg, reply, sub| puts "Msg received on [{sub}] : '#{msg}'" }

">" matches any length of the tail of a subject and can only be the last token
E.g. 'foo.>' will match 'foo.bar', 'foo.bar.baz', 'foo.foo.bar.baz.22'
NATS.subscribe('foo.>') { |msg, reply, sub| puts "Msg received on [{sub}] : '#{msg}'" }
```

## Queues Groups

```
All subscriptions with the same queue name will form a queue group
Each message will be delivered to only one subscriber per queue group, queueing semantics
You can have as many queue groups as you want
Normal subscribers will continue to work as expected.
NATS.subscribe(subject, :queue => 'job.workers') { |msg| puts "Received '#{msg}'" }
```



## Advanced Usage

```
Publish with closure, callback fires when server has processed the message
NATS.publish('foo', 'You done?') { puts 'msg processed!' }

Timeouts for subscriptions
sid = NATS.subscribe('foo') { received += 1 }
NATS.timeout(sid, TIMEOUT_IN_SECS) { timeout_recvd = true }

Timeout unless a certain number of messages have been received
NATS.timeout(sid, TIMEOUT_IN_SECS, :expected => 2) { timeout_recvd = true }

Auto-unsubscribe after MAX_WANTED messages received
NATS.unsubscribe(sid, MAX_WANTED)

Multiple connections
NATS.subscribe('test') do |msg|
 puts "received msg"
 NATS.stop
end

Form second connection to send message on
NATS.connect { NATS.publish('test', 'Hello World!') }
```

## Gorouter

Page last updated:

Gorouter routes traffic coming into Cloud Foundry to the appropriate component, whether the request comes from an operator addressing the [Cloud Controller](#) or from an application user accessing an app running on a Diego Cell. Handling both platform and app requests with the same process centralizes routing logic and simplifies support for WebSockets and other types of traffic (for example, through HTTP CONNECT).

Refer to the following instructions for help getting started with Gorouter in a standalone environment.

## Setup

```
$ git clone https://github.com/cloudfoundry/gorouter.git
$ cd gorouter
$ git submodule update --init
$./bin/go install gorouter/gorouter
$ gem install nats
```

## Start

```
Start NATS server in daemon mode
$ nats-server -d

Start gorouter
$./bin/gorouter
```

## Usage

Gorouter receives route updates through [NATS](#). By default, routes that have not been updated in two minutes are pruned. Therefore, to maintain an active route, you must ensure that the route is updated at least every two minutes. The format of these route updates is as follows:

```
{
 "host": "127.0.0.1",
 "port": 4567,
 "uris": [
 "my_first_url.vcap.me",
 "my_second_url.vcap.me"
],
 "tags": {
 "another_key": "another_value",
 "some_key": "some_value"
 }
}
```

Such a message can be sent to both the `gorouter.register` subject to register URIs, and to the `gorouter.unregister` subject to unregister URIs, respectively.

```
$ nohup ruby -rsinatra -e 'get("/") { "Hello!" }' &
$ nats-pub 'gorouter.register' '{"host":"127.0.0.1","port":4567,
 "uris":["my_first_url.vcap.me","my_second_url.vcap.me"],
 "tags":{"another_key":"another_value","some_key":"some_value"}}'
Published [gorouter.register] : '{"host":"127.0.0.1","port":4567,
 "uris":["my_first_url.vcap.me","my_second_url.vcap.me"],
 "tags":{"another_key":"another_value","some_key":"some_value"}}'
$ curl my_first_url.vcap.me:8080
Hello!
```

## Instrumentation

Gorouter provides `/varz` and `/healthz` http endpoints for monitoring.

The `/routes` endpoint returns the entire routing table as JSON. Each route has an associated array of `host:port` entries.

All of the endpoints require http basic authentication, credentials for which you can acquire through NATS. You can explicitly set the `port`, `user` and `password` (`pass` is the config attribute) in the `gorouter.yml` config file `status` section.

```
status:
 port: 8080
 user: some_user
 pass: some_password
```

Example interaction with `curl`:

```
$ curl -vvv "http://someuser:somepass@127.0.0.1:8080/routes"
* About to connect() to 127.0.0.1 port 8080 (#0)
* Trying 127.0.0.1...
* Connected
* Connected to 127.0.0.1 (127.0.0.1) port 8080 (#0)
* Server auth using Basic with user 'someuser'
> GET /routes HTTP/1.1
> Authorization: Basic c29tZXVzZXI6c29tZXBhc3M=
> User-Agent: curl/7.24.0 (x86_64-apple-darwin12.0) libcurl/7.24.0 OpenSSL/0.9.8r zlib/1.2.5
> Host: 127.0.0.1:8080
> Accept: */*
>
< HTTP/1.1 200 OK
< Content-Type: application/json
< Date: Mon, 25 Mar 2013 20:31:27 GMT
< Transfer-Encoding: chunked
<
{"0295dd314aaf582f201e655cbd74ade5.cloudfoundry.me":["127.0.0.1:34567"],
"03e316d6aa375d1dc1153700da5f1798.cloudfoundry.me":["127.0.0.1:34568"]}
```

## Logs

This section provides details about Gorouter logging.

### Levels

The following table describes the log levels supported by Gorouter. The log level is set to `debug` and is not configurable.

| Message            | Description                                                     | Examples                                                                                     |
|--------------------|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| <code>fatal</code> | Gorouter is unable to handle any requests due to a fatal error. | Gorouter cannot bind to its TCP port, a CF component has published invalid data to Gorouter. |
| <code>error</code> | An unexpected error has occurred.                               | Gorouter failed to fetch token from UAA service.                                             |
| <code>info</code>  | An expected event has occurred.                                 | Gorouter started or exited, Gorouter has begun to prune routes for stale droplets.           |
| <code>debug</code> | A lower-level event has occurred.                               | Route registration, route unregistration.                                                    |

### Message Contents

This section provides a sample Gorouter log message and an explanation of the contents.

```
[2017-02-01 22:54:08+0000] {"log_level":0,"timestamp":1485989648.0895808,"message":"endpoint-registered","source":"vcap.Gorouter.registry","data":{"uri":"0-*.login.bosh-lite.com","backend":"10.123.0.134:8080","modification_tag":{"guid":"","index":0}}}
```

| Property               | Description                                             |
|------------------------|---------------------------------------------------------|
| <code>log_level</code> | Logging level of the message                            |
| <code>timestamp</code> | Epoch time of the log                                   |
| <code>message</code>   | Content of the log line                                 |
| <code>source</code>    | Gorouter function that initiated the log message        |
| <code>data</code>      | Additional information that varies based on the message |


## About Access Logs

Access logs provide information for the following fields when receiving a request:

```
<Request Host> - [<Start Date>] "<Request Method> <Request URL> <Request Protocol>" <Status Code> <Bytes Received> <Bytes Sent> "<Referer>" "<User-Agent>" <Remote Address>
<Backend Address> x_forwarded_for:"<X-Forwarded-For>" x_forwarded_proto:"<X-Forwarded-Proto>" vcap_request_id:<X-Vcap-Request-ID> response_time:<Response Time> app_id:
<Application ID> app_index:<Application Index> <Extra Headers>
```

The following are optional fields: `Status Code` , `Response Time` , `Application ID` , `Application Index` , and `Extra Headers` .

If the access log lacks a `Status Code` , `Response Time` , `Application ID` , or `Application Index` , the corresponding field shows `-` .

 **Note:** Access logs are also redirected to syslog.

## User Account and Authentication (UAA) Server

Page last updated:

This topic provides an overview of the User Account and Authentication (UAA) Server, the identity management service for Cloud Foundry.

The primary role of the UAA is as an OAuth2 provider, issuing tokens for client apps to use when they act on behalf of Cloud Foundry users. In collaboration with the login server, the UAA can authenticate users with their Cloud Foundry credentials, and can act as an SSO service using those, or other, credentials.

The UAA has endpoints for managing user accounts and for registering OAuth2 clients, as well as various other management functions.

## Quick Start

You can deploy the UAA locally or to Cloud Foundry.

- [Deploy UAA Locally](#)
- [Deploy UAA to Cloud Foundry](#)

## Deploy UAA Locally

Follow the instructions below to deploy and run the UAA locally.

1. In a terminal window, clone the UAA GitHub repository.

```
$ git clone git://github.com/cloudfoundry/uaa.git
```

2. Navigate to the directory where you cloned the UAA GitHub repository, then run the `./gradlew run` command to build and run all the components that comprise the UAA and the example programs, `uaa`, `samples/api`, and `samples/app`.

```
$ cd uaa
$./gradlew run
```

3. If successful, the three apps run together on a single instance of Tomcat listening on port 8080, with endpoints `/uaa`, `/app`, and `/api`.

## Use Local UAA

Follow the steps below to access and use a locally-deployed UAA server.

1. Run the UAA server as described in the [Deploy Locally](#) section, above.
2. Open another terminal window. From the project base directory, run `curl localhost:8080/uaa/info -H "Accept: application/json"` to confirm the UAA is running. You should see basic information about the system. For example:

```
$ curl localhost:8080/uaa/info -H "Accept: application/json"
{
 "app": {
 "version": "4.19.0"
 },
 "links": {
 "uaa": "http://localhost:8080/uaa",
 "passwd": "/forgot_password",
 "login": "http://localhost:8080/uaa",
 "register": "/create_account"
 },
 "zone_name": "uaa",
 "entityID": "cloudfoundry-saml-login",
 "commit_id": "af93628",
 "idpDefinitions": {},
 "prompts": {
 "username": [
 "text",
 "Email"
],
 "password": [
 "password",
 "Password"
]
 },
 "timestamp": "2018-05-25T15:34:31-0700"
}
```

3. Run `gem install cf-uaac` to install the Cloud Foundry UAA Command Line Client (UAAC) Ruby gem.

```
$ gem install cf-uac
```

4. Run `uaac target http://localhost:8080/uaa` to target the local UAA server endpoint.

```
$ uaac target http://localhost:8080/uaa
```

- Run `uaac token client get CLIENT_NAME -s CLIENT_SECRET` to obtain an access token. Replace `CLIENT_NAME` and `CLIENT_SECRET` with actual values. For example, when starting up the UAA locally for development there should be a predefined [admin client](#) you can use:

```
$ uaac token client get admin -s adminsecret
```

If you do not specify the client secret, UAAC will show an interactive prompt where you must enter the client secret value.

The `uaac token client get` command requests an access token from the server using the OAuth2 [client credentials](#) grant type.

6. View your UAAC token context. When UAAC obtains a token, the token and other metadata is stored in the `~/uacac.yml` file on your local machine. To view the token you have obtained, use the command `uacac context`. For example:

[illegible]

Copy the access token from this output for the following step.

7. Run `uaac token decode ACCESS-TOKEN-VALUE` to view information in the token, which is encoded using the [JSON Web Token](#) format. Replace `ACCESS-TOKEN-VALUE` with your access token, copied from the `uaac context` output. The UAAC should display all the claims inside the token body. For example:

```
$ uaa token decode eyJhbGciOiJIUzI1NiIsImtpZCI6ImxhZ2FjeS10b2t1bi1rZXkiLCJ0eXAiOiJKV1QiLCJ0eXNpdGkiOiIzOWYyNWU2Y2E5Y2M0ZWlyYTdmNTAxNmU0NDZThkNG
```

Note: no key given to validate token signature

```
jti: 19f25e6ca9cc4eb2a7f5016e441ce8d4
sub: admin
authorities: clients.read clients.secret clients.write uaa.admin clients.admin scim.write scim.read
scope: clients.read clients.secret clients.write uaa.admin clients.admin scim.write scim.read
client_id: admin
cid: admin
azp: admin
grant_type: client_credentials
rev_sig: 267199d1
iat: 1528232017
exp: 1528275217
iss: http://localhost:8080/uaa/oauth/token
zid: uaa
aud: scim clients uaa admin
```

## Deploy UAA to Cloud Foundry

Follow the instructions below to build the UAA as an app and push it to Cloud Foundry using the Cloud Foundry Command Line Interface (cf CLI).

1. In a terminal window, clone the UAA GitHub repository.

```
$ git clone git://github.com/cloudfoundry/uaa.git
```

2. Navigate to the directory where you cloned the UAA GitHub repository, then run the `./gradlew :cloudfoundry-identity-uaa:war` command build the UAA as a WAR file.

```
$ cd uaa
$./gradlew :cloudfoundry-identity-uaa:war
```

3. Run the cf CLI `cf push APP-NAME -m 512M -p PATH-TO-WAR-FILE --no-start` command to push the app to Cloud Foundry. Replace `APP-NAME` with a name for your UAA app, and `PATH-TO-WAR-FILE` with the path to the WAR file you created in the previous step. For example:

```
$ cf push MYUAA -m 512M -p uaa/build/libs/cloudfoundry-identity-uaa-1.8.0.war --no-start
```

4. Run `cf set-env APP-NAME SPRING_PROFILES_ACTIVE default` to set the `SPRING_PROFILES_ACTIVE` environment variable with the value `default`. Replace `APP-NAME` with the name of your app that you used in the previous step. For example:

```
$ cf set-env MYUAA SPRING_PROFILES_ACTIVE default
```

5. Run `cf start APP-NAME` to start your app. Replace `APP-NAME` with the name of your app. For example:

```
$ cf start MYUAA
```

## Use Remote UAA

You use a UAA server that you pushed as an app to Cloud Foundry in a similar way to one you [run locally](#). You do not need app token encoding because you do not have the client secret.

Follow the steps below to access and use a UAA server that you pushed as an app to Cloud Foundry.

1. [Deploy UAA to Cloud Foundry](#) as described above.
2. From the project base directory, run `curl -H "Accept: application/json" APP-FQDN/login` to query the external login endpoint about the system. Replace `APP-FQDN` with the FQDN of your app. For example:

```
$ curl -H "Accept: application/json" uaa.example.org/login
{
 "timestamp": "2014-09-15T18:25:04+0000",
 "app": {"version": "1.8.3"},
 "commit_id": "git-metadata-not-found",
 "prompts": {"username": ["text", "Email"],
 "password": ["password", "Password"]}
}
```

- Run `gem install cf-uaac` to install the Cloud Foundry UAA Command Line Client (UAAC) Ruby gem.

```
$ gem install cf-uaac
```

- Run `uaac target APP-FQDN` to target the remote UAA Server endpoint. Replace `APP-FQDN` with the FQDN of your app.

```
$ uaac target uaa.example.org
```

- Run `uaac token get USERNAME PASSWORD` to log in. Replace `USERNAME` with your user name, and `PASSWORD` with your password. For example:

```
$ uaac token get marissa koala
```

If you do not specify a username and password, the UAAC prompts you to supply them.

The `uaac token client get` command authenticates and obtains an access token from the server using the OAuth2 implicit grant, similar to the approach intended for a standalone client like the Cloud Foundry Command Line Interface (cf CLI).

## Integration Tests

Run the integration tests with the following command:

```
$./gradlew integrationTest
```

This command starts a UAA server running in a local Apache Tomcat instance. By default, the service URL is set to `http://localhost:8080/uaa`.

You can set the environment variable `CLOUD_FOUNDRY_CONFIG_PATH` to a directory containing a `uaa.yml` file where you change the URLs used in the tests, and where you can set the UAA server context root.

## Custom YAML Configuration

Follow the steps below to modify the runtime parameters.

- Create a `uaa.yml` file in the following format:

```
uaa:
 host: UAA-HOSTNAME
 test:
 username: USERNAME
 password: PASSWORD
 email: EMAIL-ADDRESS
```

Replace the values in the above format as follows:

- UAA-HOSTNAME:** The FQDN of UAA app. Example: `uaa.example.org`
  - USERNAME:** A valid username. Example: `dev@example.org`
  - PASSWORD:** Password for the above username.
  - EMAIL-ADDRESS:** Email address for the above user. Example: `dev@example.org`
- From the `uaa/uaa` directory, run `CLOUD_FOUNDRY_CONFIG_PATH=/tmp ./gradlew test`.
  - The web app looks for a YAML file in the following locations when it starts, with later entries overriding earlier ones:



```
classpath:uaa.yml
file:${CLOUD_FOUNDRY_CONFIG_PATH}/uaa.yml
file:${UAA_CONFIG_FILE}
${UAA_CONFIG_URL}
```

## Test with PostgreSQL or MySQL

The default UAA unit tests, `./gradlew test`, use HyperSQL (hsqldb).

To use a different database management system, create a `uaa.yml` file containing `spring_profiles: default,OTHER-DBMS` in the `src/main/resources/` directory. Replace `OTHER-DBMS` with the name of the other database management system to use.

For example, run the following command to run the unit tests using PostgreSQL instead of hsqldb:

```
$ echo "spring_profiles: default,postgresql" > src/main/resources/uaa.yml
$./gradlew test integrationTest
```

Run the following command to run the unit tests using MySQL instead of hsqldb:

```
$ echo "spring_profiles: default,mysql" > src/main/resources/uaa.yml
$./gradlew test integrationTest
```

You can find the database configuration for the common and scim modules at `common/src/test/resources/(mysql|postgresql).properties` and `scim/src/test/resources/(mysql|postgresql).properties`.

## UAA Projects

The following UAA projects exist:

- `common`: A module containing a JAR with all the business logic. `common` is used in the web apps listed below.
- `uaa`: The UAA server. `uaa` provides an authentication service and authorized delegation for back-end services and apps by issuing OAuth2 access tokens.
- `api`: A sample OAuth2 resource service that returns a mock list of deployed apps. `api` provides resources that other apps might want to access on behalf of the resource owner.
- `app`: A sample user app that uses both `api` and `uaa`. `app` is a web app that requires single sign-on and access to the `api` service on behalf of users.
- `scim`: The [SCIM](#) user management module used by UAA.

## UAA Server

The authentication service, `uaa`, is a Spring MVC web app. You can deploy it in Tomcat or your container of choice, or execute `./gradlew run` to run it directly from the `uaa` directory in the source tree. When run with Gradle, `uaa` listens on port `8080` and has URL `http://localhost:8080/uaa`.

The UAA Server supports the APIs defined in the UAA-APIs document which include the following:

- The OAuth2 `/authorize` and `/token` endpoints
- A `/login_info` endpoint to allow querying for required login prompts
- A `/check_token` endpoint to allow resource servers to obtain information about an access token submitted by an OAuth2 client
- SCIM user provisioning endpoint
- OpenID connect endpoints to support authentication `/userinfo` and `/check_id`

Command line clients can perform authentication by submitting credentials directly to the `/authorize` endpoint.

An `ImplicitAccessTokenProvider` exists in Spring Security OAuth to use if your client is Java.

By default, `uaa` will launch with a context root `/uaa`.

## Configuration

A `uaa.yml` file exists in the app. This file provides defaults to the placeholders in the Spring XML.

You can override any occurrences of `${placeholder.name}` in the XML by adding it to the `uaa.yml` file, or by providing a System property, `-D` to JVM, with the same name.

All passwords and client secrets in the config files are in plain text, but are inserted into the UAA database encrypted with BCrypt.

## User Account Data

The default uses an in-memory RDBMS user store, pre-populated with a single test user `marissa` with password `koala`.

To use PostgreSQL for user data, activate the Spring profile `postgresql`.

You can configure the active profiles in `uaa.yml` using the following:

```
spring_profiles: postgresql,default
```

To use PostgreSQL instead of HyperSQL (hsqldb):

```
$ echo "spring_profiles: postgresql,default" > src/main/resources/uaa.yml
$./gradlew run
```

To bootstrap a microcloud-type environment, you need an admin client. A database initializer component that inserts an admin client exists. If the default profile is active, for example not `postgresql`, a cf CLI client exists so that the Gem login works with no additional configuration required. You can override the default settings and add additional clients in the `uaa.yml` file:

```
oauth:
 clients:
 admin:
 authorized-grant-types: client_credentials
 scope: read,write,password
 authorities: ROLE_CLIENT,ROLE_ADIN
 id: admin
 secret: adminclientsecret
 resource-ids: clients
```

You can use the admin client to create additional clients. You must have a client with read/write access to the `scim` resource to create user accounts. The integration tests handle this automatically by inserting client and user accounts as necessary for the tests.

## Sample Apps

Two sample apps are included with the UAA: `/api` and `/app`.

Run them with `./gradlew run` from the `uaa` root directory. All three apps, `/uaa`, `/api`, and `/app`, are simultaneously deployed.

### API Sample App

The `api` sample app is an example resource server. It hosts a service that returns a list of mock apps under `/apps`.

### APP Sample App

The `app` sample app is a user interface app, primarily aimed at browsers, that uses OpenID Connect for authentication and OAuth2 for access grants. `app` authenticates with the Auth service, then accesses resources in the API service. Run it with `./gradlew run` from the `uaa` root directory.

The app can operate in multiple different profiles according to the location and presence of the UAA server and the login app. By default, the app looks for a UAA on `localhost:8080/uaa`, but you can change this by setting the `UAA_PROFILE` environment variable or System Property.

The app source code, `samples/app/src/main/resources`, contains multiple properties files pre-configured with different likely locations for those servers. The names of these properties files follow the form `app-UAA_PROFILE.properties`.

The naming convention for the `UAA_PROFILE` is as follows:

- `local`: a localhost deployment
- `vcap`: a `vcap.me` deployment
- `staging`: a staging deployment

Profile names can be hyphenated to indicate multiple contexts. For example, `local-vcap` can be used when the login server is in a different location than the UAA server.

## Use Cases

1. See all apps:

```
GET /app/apps
```

Browser is redirected through a series of authentication and access grant steps, and then the photos are shown.

2. See the currently logged in user details, a selection of attributes from the OpenID provider:

```
GET /app
```

## LOGIN App

The `login` app is a user interface for authentication. The UAA can also authenticate user accounts, but only if it manages them itself, and it only provides a basic UI. You can brand and customize the login app for non-native authentication and for more complicated UI flows, like user registration and password reset.

The login app is itself an OAuth2 endpoint provider, but delegates those features to the UAA server. Therefore, configuration for the login app consists of locating the UAA through its OAuth2 endpoint URLs and registering the login app itself as a client of the UAA. A `login.yml` for the UAA locations exists, such as for a local `vcap` instance:

```
uaa:
 url: http://uaa.vcap.example.net
 token:
 url: http://uaa.vcap.example.net/oauth/token
 login:
 url: http://uaa.vcap.example.net/login.do
```

An environment variable or Java System property also exists, `LOGIN_SECRET`, for the client secret that the app uses when it authenticates itself with the UAA. The login app is registered by default in the UAA only if there are no active Spring profiles. In the UAA, the registration is located in the `oauth-clients.xml` config file:

```
id: login
secret: loginsecret
authorized-grant-types: client_credentials
authorities: ROLE_LOGIN
resource-ids: oauth
```

## Use Cases

1. Authenticate:

```
GET /login
```

The sample app presents a form login interface for the backend UAA, and an OpenID widget where a user can authenticate using Google or other credentials.

2. Approve OAuth2 token grant:

```
GET /oauth/authorize?client_id=app&response_type=code...
```

Standard OAuth2 Authorization Endpoint. The UAA handles client credentials and all other features in the back end, and the login app is used to render the UI.

### 3. Obtain access token:

```
POST /oauth/token
```

Standard OAuth2 Authorization Endpoint passed through to the UAA.

## Scopes

UAA covers multiple scopes of privilege, including access to UAA, access to [Cloud Controller](#), and access to the [router](#).

See the tables below for a description of the scopes covered by UAA:

- [UAA Scopes](#)
- [Cloud Controller Scopes](#)
- [Router Scopes](#)
- [Other Scopes](#)

### UAA Scopes

| Scope                       | Description                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>uaa.user</code>       | This scope indicates that this is a user. It is required in the token if submitting a GET request to the OAuth 2 <code>/authorize</code> endpoint.                                                                                                                                                                                     |
| <code>uaa.none</code>       | This scope indicates that this client will not be performing actions on behalf of a user.                                                                                                                                                                                                                                              |
| <code>uaa.admin</code>      | This scopes indicates that this is the superuser.                                                                                                                                                                                                                                                                                      |
| <code>scim.write</code>     | This scope gives admin write access to all SCIM endpoints, <code>/Users</code> , and <code>/Groups</code> .                                                                                                                                                                                                                            |
| <code>scim.read</code>      | This scope gives admin read access to all SCIM endpoints, <code>/Users</code> , and <code>/Groups</code> .                                                                                                                                                                                                                             |
| <code>scim.create</code>    | This scope gives the ability to create a user with a POST request to the <code>/Users</code> endpoint, but not to modify, read, or delete users.                                                                                                                                                                                       |
| <code>scim.userids</code>   | This scope is required to convert a username and origin into a user ID and vice versa.                                                                                                                                                                                                                                                 |
| <code>scim.invite</code>    | This scope is required to participate in invitations using the <code>/invite_users</code> endpoint.                                                                                                                                                                                                                                    |
| <code>groups.update</code>  | This scope gives the ability to update a group. This ability can also be provided by the broader <code>scim.write</code> scope.                                                                                                                                                                                                        |
| <code>password.write</code> | This admin scope gives the ability to change a user's password.                                                                                                                                                                                                                                                                        |
| <code>openid</code>         | This scope is required to access the <code>/userinfo</code> endpoint. It is intended for OpenID clients.                                                                                                                                                                                                                               |
| <code>idps.read</code>      | This scope gives read access to retrieve identity providers from the <code>/identity-providers</code> endpoint.                                                                                                                                                                                                                        |
| <code>idps.write</code>     | This scope gives the ability to create and update identity providers from the <code>/identity-providers</code> endpoint.                                                                                                                                                                                                               |
| <code>clients.admin</code>  | This scope gives the ability to create, modify, and delete clients.                                                                                                                                                                                                                                                                    |
| <code>clients.write</code>  | This scope is required to create and modify clients. The scopes are prefixed with the scope holder's client ID. For example, <code>id:testclient authorities:client.write</code> gives the ability to create a client that has scopes with the <code>testclient.</code> prefix. Authorities are limited to <code>uaa.resource</code> . |
| <code>clients.read</code>   | This scope gives the ability to read information about clients.                                                                                                                                                                                                                                                                        |
| <code>clients.secret</code> | This admin scope is required to change the password of a client.                                                                                                                                                                                                                                                                       |
| <code>zones.read</code>     | This scope is required to invoke the <code>/identity-zones</code> endpoint to read identity zones.                                                                                                                                                                                                                                     |
| <code>zones.write</code>    | This scope is required to invoke the <code>/identity-zones</code> endpoint to create and update identity zones.                                                                                                                                                                                                                        |
| <code>scim.zones</code>     | This is a limited scope that only allows adding a user to, or removing a user from, zone management groups under the path <code>/Groups/zones</code> .                                                                                                                                                                                 |

|                                                |                                                                                                                                                                                                                                      |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>oauth.approval</code>                    | <code>/approvals endpoint</code> . This scope is required to approve or reject clients to act on a user's behalf. This is a default scope defined in the <code>uaa.yml</code> file.                                                  |
| <code>oauth.login</code>                       | This scope is used to indicate a login app, such as external login servers, can perform trusted operations, such as creating users not authenticated in the UAA.                                                                     |
| <code>approvals.me</code>                      | This scope is not currently used.                                                                                                                                                                                                    |
| <code>uaa.resource</code>                      | This scope indicates that this is a resource server, used for the <code>/check_token</code> endpoint.                                                                                                                                |
| <code>zones.ZONE-ID.admin</code>               | This scope permits operations in a designated zone, such as creating identity providers or clients in another zone, by authenticating against the default zone. This scope is used with the <code>X-Identity-Zone-Id</code> header . |
| <code>zones.ZONE-ID.read</code>                | This scope permits reading the given identity zone. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                                                             |
| <code>zones.ZONE-ID.clients.admin</code>       | This scope translates into <code>clients.admin</code> after zone switch completes. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                              |
| <code>zones.ZONE-ID.clients.read</code>        | This scope translates into <code>clients.read</code> after zone switch completes. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                               |
| <code>zones.ZONE-ID.clients.write</code>       | This scope translates into <code>clients.write</code> after zone switch completes. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                              |
| <code>zones.ZONE-ID.clients.scim.read</code>   | This scope translates into <code>scim.read</code> after zone switch completes. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                                  |
| <code>zones.ZONE-ID.clients.scim.create</code> | This scope translates into <code>scim.create</code> after zone switch completes. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                                |
| <code>zones.ZONE-ID.clients.scim.write</code>  | This scope translates into <code>scim.write</code> after zone switch completes. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                                 |
| <code>zones.ZONE-ID.idps.read</code>           | This scope translates into <code>idps.read</code> after zone switch completes. This scope is used with the <code>X-Identity-Zone-Id</code> header .                                                                                  |

## Cloud Controller Scopes

| Scope                                         | Description                                                                                                               |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <code>cloud_controller.read</code>            | This scope gives the ability to read from any Cloud Controller route the token has access to.                             |
| <code>cloud_controller.write</code>           | This scope gives the ability to post to Cloud Controller routes the token has access to.                                  |
| <code>cloud_controller.admin</code>           | This admin scope gives full permissions to Cloud Controller.                                                              |
| <code>cloud_controller.admin_read_only</code> | This admin scope gives read permissions to Cloud Controller.                                                              |
| <code>cloud_controller.global_audit_or</code> | This scope gives read-only access to all Cloud Controller API resources except for secrets such as environment variables. |

## Routing Scopes

| Scope                                    | Description                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------|
| <code>routing.routes.read</code>         | This scope gives the ability to read the full routing table from the router.  |
| <code>routing.routes.write</code>        | This scope gives the ability to write the full routing table from the router. |
| <code>routing.router_groups.read</code>  | This scope gives the ability to read the full list of routing groups.         |
| <code>routing.router_groups.write</code> | This scopes gives the ability to write the full list of routing groups.       |

## Other Scopes

| Scope                            | Description                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------|
| <code>doppler.firehose</code>    | This scope gives the ability to read logs from the <a href="#">Loggregator Firehose</a> endpoint.     |
| <code>notifications.write</code> | This scope gives the ability to send notifications through the <a href="#">Notification Service</a> . |



## Garden

Page last updated:

This topic describes Garden, the component that Cloud Foundry uses to create and manage isolated environments called containers. Each instance of an application deployed to Cloud Foundry runs within a container. For more information about how containers work, see the [Container Mechanics](#) section of the *Container Security* topic.

## Backends


Garden has pluggable backends for different platforms and runtimes, and specifies a set of interfaces that each platform-specific backend must implement. These interfaces contain methods to perform the following actions:

- Create and delete containers
- Apply resource limits to containers
- Open and attach network ports to containers
- Copy files into and out of containers
- Run processes within containers
- Stream `STDOUT` and `STDERR` data out of containers
- Annotate containers with arbitrary metadata
- Snapshot containers for redloys without downtime

For more information, see the [Garden repository](#) on GitHub.

## Garden-runC

Cloud Foundry currently uses the [Garden-runC](#) backend, a Linux-specific implementation of the Garden interface using the [Open Container Interface](#) (OCI) standard. Previous versions of Cloud Foundry used the [Garden-Linux](#) backend.

 **Note:** PAS versions v1.8.8 and above use Garden-runC instead of Garden-Linux.

Garden-runC has the following features:

- Uses the same OCI low-level container execution code as Docker and Kubernetes, so container images run identically across all three platforms
- [AppArmor](#) is configured and enforced by default for all unprivileged containers
- Seccomp whitelisting restricts the set of system calls a container can access, reducing the risk of container breakout
- Allows pluggable networking and rootfs management

For more information, see the [Garden-runC repository](#) on GitHub.

## Garden RootFS (GrootFS)

Garden manages container filesystems through a plugin interface. Cloud Foundry uses the [GrootFS](#) plugin for this task. GrootFS is a Linux-specific implementation of the Garden volume plugin interface.

GrootFS performs the following actions:

- Creates container filesystems based on buildpacks and droplets
- Creates container filesystems based on remote docker images
- Authenticates with remote registries when using remote images
- Properly maps UID/GID for all files inside an image
- Executes garbage collection to remove unused volumes
- Applies per container disk quotas
- Provides per container disk usage stats

For more information, see [GrootFS Disk Usage](#) and the [GrootFS repository](#) [↗](#) on GitHub.



## HTTP Routing

Page last updated:

This topic describes how the Gorouter, the main component in Cloud Foundry's [routing](#) tier, routes HTTP traffic within Cloud Foundry (CF).

## HTTP Headers

HTTP traffic passed from the Gorouter to an app includes the following HTTP headers:

### X-Forwarded-Proto

The `X-Forwarded-Proto` header gives the scheme of the HTTP request from the client.

If an incoming request includes the `X-Forwarded-Proto` header, Gorouter does the following:

- Appends it to the existing header.
- Sets the scheme to HTTP if the client made an insecure request, meaning a request on port 80.
- Sets the scheme to HTTPS if the client made a secure request, meaning a request on port 443.

Developers can configure their apps to reject insecure requests by inspecting the `X-Forwarded-Proto` HTTP header on incoming traffic. The header may have multiple values represented as a comma-separated list, so developers must ensure the app rejects traffic that includes any `X-Forwarded-Proto` values that are not HTTPS.

### X-Forwarded-For

If `X-Forwarded-For` is present, the Gorouter appends the load balancer's IP address to it and forwards the list. If `X-Forwarded-For` is not present, then the Gorouter sets it to the IP address of the load balancer in the forwarded request (some load balancers masquerade the client IP). If a load balancer sends the client IP using the PROXY protocol, then the Gorouter uses the client IP address to set `X-Forwarded-For`.

If your load balancer terminates TLS on the client side of the Gorouter, it must append these headers to requests forwarded to the Gorouter. For more information, see the [Securing Traffic into Cloud Foundry](#) topic.

## HTTP Headers for Zipkin Tracing

Zipkin is a tracing system that enables app developers to troubleshoot failures or latency issues. Zipkin provides the ability to trace requests and responses across distributed systems. See [Zipkin.io](#) for more information.

When the [Zipkin feature is enabled in Cloud Foundry](#), the Gorouter examines the HTTP request headers and performs the following:

- If the `X-B3-TraceId` and `X-B3-SpanId` HTTP headers are not present in the request, the Gorouter generates values for these and inserts the headers into the request forwarded to an application. These values are also found in the Gorouter access log message for the request: `x_b3_traceid` and `x_b3_spanid`.
- If the `X-B3-TraceId` and `X-B3-SpanId` HTTP headers are present in the request, the Gorouter forwards them unmodified. In addition to these trace and span ids, the Gorouter access log message for the request includes `x_b3_parentspanid`.

Developers can then add Zipkin trace IDs to their application logging in order to trace app requests and responses in Cloud Foundry.

After adding Zipkin HTTP headers to app logs, developers can use `cf logs myapp` to correlate the trace and span ids logged by the Gorouter with the trace

ids logged by their app. To correlate trace IDs for a request through multiple apps, each app must forward appropriate values for the headers with requests to other applications.

## HTTP Headers for App Instance Routing

Developers who want to obtain debug data for a specific instance of an app can use the HTTP header `X-CF-APP-INSTANCE` to make a request to an app instance.

Perform the following steps to make an HTTP request to a specific app instance:

1. Obtain the GUID of your app:

```
$ cf app YOUR-APP --guid
```

2. List your app instances and retrieve the index number of the instance you want to debug:

```
$ cf app YOUR-APP
```

3. Make a request to the app route using the HTTP header `X-CF-APP-INSTANCE` set to the concatenated values of the app GUID and the instance index:

```
$ curl app.example.com -H "X-CF-APP-INSTANCE":"YOUR-APP-GUID:YOUR-INSTANCE-INDEX"
```

## Forward Client Certificate to Applications

Applications that require mutual TLS (mTLS) need metadata from client certificates to authorize requests. Cloud Foundry supports this use case without bypassing layer-7 load balancers and the Gorouter.

The HTTP header `X-Forwarded-Client-Cert` (XFCC) may be used to pass the originating client certificate along the data path to the application. Each component in the data path must trust that the back end component has not allowed the header to be tampered with.

If you configure the load balancer to terminate TLS and set the XFCC header from the received client certificate, then you must also configure the load balancer to strip this header if it is present in client requests. This configuration is required to prevent spoofing of the client certificate.

The following sections describe supported deployment configurations.

### Terminating TLS at Load Balancer

By default, Gorouter forwards arbitrary headers that are not otherwise mentioned in the docs; this includes the XFCC header.

For applications to receive the XFCC header, configure your load balancer to set the XFCC header with the contents of the client certificate received in the TLS handshake.

This mode is enabled when the **TLS terminated for the first time at infrastructure load balancer** option is selected in the **Networking** configuration screen of the PAS tile.

### Terminating TLS at HAProxy

This option allows you to configure support for the XFCC header while leveraging HAProxy. When selected, HAProxy sets the XFCC header to the contents of the client certificate received in the TLS handshake.

Selecting this configuration requires that the load balancer in front of HAProxy is configured to pass through the TLS handshake to HAProxy via TCP.

This mode is enabled when the **TLS terminated for the first time at HAProxy** option is selected in the **Networking** configuration screen of the PAS tile.

HAProxy trusts the Diego intermediate certificate authority. This trust is enabled automatically and permits mutual authentication between applications that are running on Pivotal Cloud Foundry.

### Terminating TLS at Gorouter

If the Gorouter is the first component to terminate TLS, such that it receives the certificate of the originating client in the mutual TLS handshake, the operator should select this option. When selected, Gorouter sets the XFCC header to the contents of the client certificate received in the TLS handshake and strips the XFCC header when present in a request.

Selecting this configuration requires that the load balancer in front of Gorouter is configured to pass through TLS handshake to Gorouter via TCP.

This mode is enabled when the **TLS terminated for the first time at the Router** option is selected in the **Networking** configuration screen of the PAS tile.

Gorouter trusts the Diego intermediate certificate authority. This trust is enabled automatically and permits mutual authentication between applications

that are running on Pivotal Cloud Foundry.

## Client-Side TLS

Depending on your needs, you can configure your deployment to terminate TLS at the Gorouter, at the Gorouter and the load balancer, or at the load balancer only. For more information, see the [Securing Traffic into Cloud Foundry](#) topic.

## TLS to Apps and Other Back End Services

The Gorouter supports one-way TLS to back end destinations, including app instances, platform services, and any other routable endpoints.

This is enabled by following the steps in [Configure Validation of App Instance Identity with TLS](#).

## Preventing Misrouting

As CF manages and balances apps, the internal IP address and ports for app instances change. To keep the Gorouter's routing tables current, a Route-Emitter on each Diego cell sends a periodic update to all Gorouters through NATS, reminding them of the location of all app instances; the default frequency of these updates is 20 seconds. The Gorouter tracks a time-to-live (TTL) for each route to back end mapping; this TTL defaults to 120 seconds and is reset when the Gorouter receives an updated registration message.

Network partitions or NATS failures can cause the Gorouter's routing table to fall out of sync, as CF continues to re-create containers across hosts to keep apps running. This can lead to routing of requests to incorrect destinations.

You can configure the Gorouter to handle this problem in two ways:

| Consistency mode                    | Security of traffic between Gorouter and Containers | Gorouter Route Pruning                                                                                  |
|-------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| <a href="#">With TLS Enabled</a>    | Encrypted via TLS                                   | Routes are pruned on failure of TLS handshake only. See <a href="#">Gorouter TLS pruning behavior</a> . |
| <a href="#">Without TLS Enabled</a> | Plain text                                          | Routes are pruned on TTL expiry                                                                         |

Both of these consistency modes are described below.

### With TLS Enabled

This consistency mode is newer and has the following benefits:

- Improved availability for applications by keeping routes in the Gorouter's routing table when TTL expires
- Increased guarantees against misrouting by validating the identity of backends before forwarding requests
- Increased security by encrypting data in flight from the Gorouter to backends

**⚠ warning:** TLS routing requires an additional 32 MB of RAM capacity on your Diego cells per app instance, as well as additional CPU capacity. Check the total amount of Diego cell memory available to allocate in your environment, and if it is less than 32 MB times the number of running app instances, scale out your Diego cells.

**⚠ warning:** You may see an increase of memory and CPU usage for your Gorouters after enabling TLS routing. Check the total amount of memory and CPU usage of the Gorouters in your environment, and if they are close to the size limit, consider scaling out your Gorouters before enabling TLS routing.

In this mode, the Diego Route-Emitters send a modified route registration message to NATS that includes a unique identifier for the app instance, as well instructions to use TLS when communicating with the instance. See [TLS to Apps and Other Back End Services](#) for details.

Before forwarding traffic to an app instance, the Gorouter initiates a TLS handshake with an [Envoy proxy](#) running in each app container. In the TLS handshake, the Envoy proxy presents a certificate generated by Diego for each container which uniquely identifies the container using the same app instance identifier sent by the Route-Emitter, configured in the certificate as a domain Subject Alternative Name (SAN).

If the Gorouter confirms that the app instance identifier in the certificate matches the one received in the route registration message, the Gorouter forwards the HTTP request over the TLS session, and the Envoy proxy then forwards it to the app process. If the instance identifiers do not match, the Gorouter removes the app instance from its routing table and transparently retries another instance of the app.

## Configure Validation of App Instance Identity with TLS

By default, Gorouter does not use TLS to verify app identity. To enable Gorouter to communicate with and validate app containers over TLS in Linux cells, perform the following steps:

1. In Ops Manager, click the Pivotal Application Service, Isolation Segment, or Small Footprint Runtime tile.
2. Navigate to the **Application Containers** pane.
3. Enable the **Router uses TLS to verify application identity** checkbox. With this configuration, Diego cells run an Envoy proxy for each app instance.

## Without TLS Enabled

In this consistency mode, the Diego Route-Emitters on each cell send route registration messages that include instructions for the Gorouter to send unencrypted requests to the app instance. If the Gorouter does not receive an update for the route within the time-to-live (TTL) interval, the route is pruned from the Gorouter's routing table. See [TLS to Apps and Other Back End Services](#) for details.

This pruning method was developed before the alternative was available.

## Consistency Mode Can Differ by Instance Group

The Gorouter can [validate app instance identity using TLS](#) only when Diego cells are configured appropriately. Because cells are configured for TLS through the instance group that they belong to, the Gorouter can run in different consistency modes with cells in different instance groups. For example, the Gorouter can communicate over TLS and validate the cells in one Isolation Segment, while communicating with cells in another Isolation Segment via plain text and [without validating instance identity](#).

Currently, only Linux cells support the Gorouter validating app instance identities [using TLS](#). With Windows cells, the Gorouter runs [without TLS enabled](#), forwarding requests to Windows apps over plain text and pruning based on route TTL.

## Transparent Retries

If the Gorouter cannot establish a TCP connection with a selected application instance, the Gorouter considers the instance ineligible for requests for 30 seconds and transparently attempts to connect to another application instance. Once the Gorouter has established a TCP connection with an application instance, the Gorouter forwards the HTTP request.

See the [Round-Robin Load Balancing](#) section below for more information about how the Gorouter forwards requests to application instances.

## Round-Robin Load Balancing

The Gorouter uses the round-robin algorithm for load balancing incoming requests to application instances. The Gorouter maintains a dynamically updated list of application instances for each route, and forwards each request for a given route to the next application instance in the list.

## WebSockets

WebSockets is a protocol providing bi-directional communication over a single, long-lived TCP connection, commonly implemented by web clients and servers. WebSockets are initiated through HTTP as an upgrade request. The Gorouter supports this upgrade handshake, and holds the TCP connection open with the selected application instance. To support WebSockets, the operator must configure the load balancer correctly. Depending on the configuration, clients may have to use a different port for WebSocket connections, such as port 4443, or a different domain name. For more information, see the [Supporting WebSockets](#) topic.

## Session Affinity

The Gorouter supports session affinity, or *sticky sessions*, for incoming HTTP requests to compatible apps.

With sticky sessions, when multiple instances of an app are running on CF, requests from a particular client always reach the same app instance. This allows apps to store session data specific to a user session.

- To support sticky sessions, configure your app to return a `JSESSIONID` cookie in responses. The app generates a `JSESSIONID` as a long hash in the following format:


```
1A530637289A03B07199A44E8D531427
```

- If an app returns a `JSESSIONID` cookie to a client request, the CF routing tier generates a unique `VCAP_ID` for the app instance based on its GUID in the following format:

```
323f211e-fea3-4161-9bd1-615392327913
```

- On subsequent requests, the client must provide both the `JSESSIONID` and `VCAP_ID` cookies.

The CF routing tier uses the `VCAP_ID` cookie to forward client requests to the same app instance every time. The `JSESSIONID` cookie is forwarded to the app instance to enable session continuity. If the app instance identified by the `VCAP_ID` crashes, the Gorouter attempts to route the request to a different instance of the app. If the Gorouter finds a healthy instance of the app, it initiates a new sticky session.

 **Note:** CF does not persist or replicate HTTP session data across app instances. If an app instance crashes or is stopped, session data for that instance is lost. If you require session data to persist across crashed or stopped instances, or to be shared by all instances of an app, store session data in a CF marketplace service that offers data persistence.

## Keepalive Connections

### From Front End Clients

The Gorouter supports keepalive connections from clients and does not close the TCP connection with clients immediately after returning an HTTP response. Clients are responsible for closing these connections.

### To Back End Servers

If keepalive connections are disabled, the Gorouter closes the TCP connection with an app instance or system component after receiving an HTTP response.

If keepalive connections are enabled, the Gorouter maintains established TCP connections to back ends. the Gorouter supports up to 100 idle connections to each back end:

- If an idle connection exists for a given back end, the Gorouter reuses it to route subsequent requests.
- If no idle connection exists for this back end, the Gorouter creates a new connection.

## Gorouter Retry Behavior

When you deploy an app that requires Diego cells to restart or recreate, the app may not respond to a Gorouter request before the keepalive connection breaks. The following table describes how the Gorouter behaves if it cannot establish a TCP connection to an app:

| If the Gorouter ...                                                                | then the Gorouter ...            |
|------------------------------------------------------------------------------------|----------------------------------|
| cannot establish a TCP connection to the routing back end for the app              | retries the request three times. |
| establishes a TCP connection to the routing back end, but the app does not respond | waits 15 minutes for a response. |

In both cases, if the app still does not respond to the request, the Gorouter returns a `502` error.



## Diego Components and Architecture

Page last updated:

This topic provides an overview of the structure and components of Diego, the container management system for Pivotal Cloud Foundry versions 1.6 and newer.

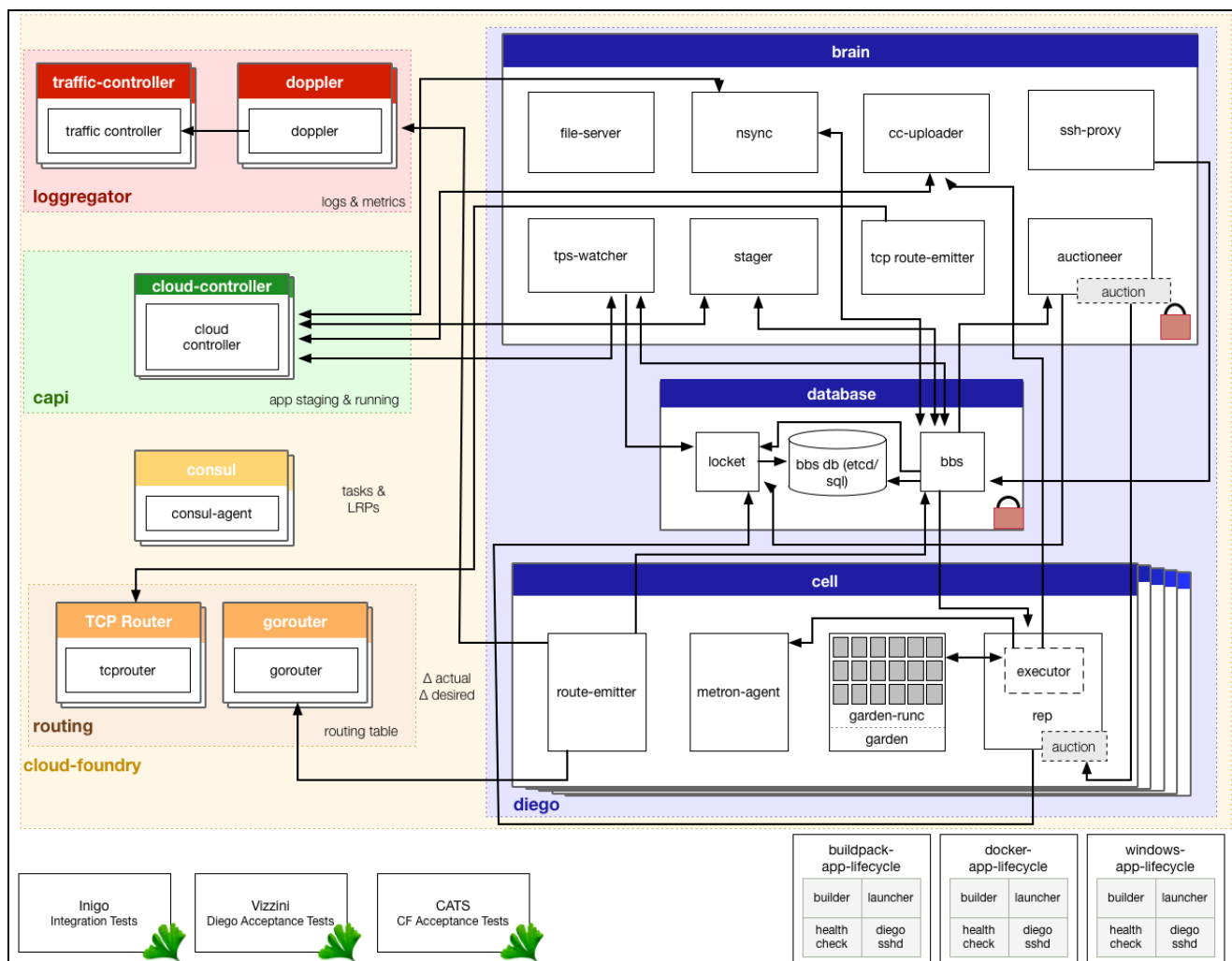
This topic includes the following sections:

- [Architecture Diagram](#)
- [Diego Components](#)
  - [Diego Brain](#)
  - [Diego Cell](#)
  - [Database VMs](#)
  - [BOSH DNS](#)
- [Platform-Specific Components](#)
  - [Garden Back Ends](#)
  - [App Lifecycle Binaries](#)

## Architecture Diagram

Cloud Foundry uses the Diego architecture to manage app containers. Diego components assume app scheduling and management responsibility from the Cloud Controller.

See the following diagram and descriptions for information about the way Diego handles app requests.



[View a larger version of this image.](#)

1. The Cloud Controller passes requests to stage and run apps to several components on the [Diego Brain](#).
2. The Diego Brain components translate staging and running requests into [Tasks and Long Running Processes](#) (LRPs), then submit these to the [Bulletin Board System](#) (BBS) through an API over HTTP.
3. The BBS submits the Tasks and LRPs to the [Auctioneer](#), part of the [Diego Brain](#).
4. The Auctioneer distributes these Tasks and LRPs to [Cells](#) through an [Auction](#). The Diego Brain communicates with Diego Cells using SSL/TLS protocol.
5. Once the Auctioneer assigns a Task or LRP to a Cell, an in-process [Executor](#) creates a [Garden](#) container in the Cell. The Task or LRP runs in the container.
6. The [BBS](#) tracks desired LRPs, running LRP instances, and in-flight Tasks. It also periodically analyzes this information and corrects discrepancies to ensure consistency between `ActualLRP` and `DesiredLRP` counts.
7. The [Metron Agent](#), part of the Cell, forwards app logs, errors, and metrics to the Cloud Foundry Loggregator. For more information, see the [Application Logging in Cloud Foundry](#) topic.

## Diego Components

Diego components run and monitor Tasks and LRPs.

### Diego Brain

Diego Brain components distribute Tasks and LRPs to Diego Cells, and correct discrepancies between `ActualLRP` and `DesiredLRP` counts to ensure fault-tolerance and long-term consistency.

The Diego Brain consists of the following:

- [Auctioneer](#)
- [CC-Uploader](#)
- [File Server](#)
- [SSH Proxy](#)
- [TPS Watcher](#)
- [TCP Route-emitter](#)
- [Nsync](#)
- [Stager](#)

#### Auctioneer

- Uses the [auction package](#) [↗](#) to run Diego Auctions for Tasks and LRPs
- Communicates with Cell [Reps](#) over SSL/TLS
- Maintains a lock in the BBS that restricts auctions to one Auctioneer at a time

See the [Auctioneer repository](#) [↗](#) on GitHub for more information.

#### CC-Uploader

- Mediates uploads from the Executor to the Cloud Controller
- Translates simple HTTP POST requests from the Executor into complex multipart-form uploads for the Cloud Controller

See the [CC-Uploader repository](#) [↗](#) on GitHub for more information.

#### File Server



- This “blobstore” serves static assets that can include general-purpose [App Lifecycle binaries](#) and app-specific droplets and build artifacts.

See the [File Server repository](#) on GitHub for more information.

## SSH Proxy

- Brokers connections between SSH clients and SSH servers running inside instance containers

See to [Application SSH](#), [Application SSH Overview](#), or the [Diego SSH repository](#) on GitHub for more information.

## TPS Watcher

- Provides the Cloud Controller with information about currently running LRPs to respond to `cf apps` and `cf app APP_NAME` requests
- Monitors `ActualLRP` activity for crashes and reports them the Cloud Controller

See the [TPS repository](#) on GitHub for more information.

## TCP Route-Emitter

- Monitors `DesiredLRP` and `ActualLRP` states, emitting TCP route registration and unregistration messages to the Cloud Foundry [routing API](#) when it detects changes
- Periodically emits TCP routes to the Cloud Foundry routing API

## Nsync

- Listens for app requests to update the `DesiredLRPs` count and updates `DesiredLRPs` through the BBS
- Periodically polls the Cloud Controller for each app to ensure that Diego maintains accurate `DesiredLRPs` counts

See the [Nsync repository](#) on GitHub for more information.

## Stager

- Translates staging requests from the Cloud Controller into generic Tasks and LRPs
- Sends a response to the Cloud Controller when a Task completes

See the [Stager repository](#) on GitHub for more information.

## Diego Cell

Diego Cell components manage and maintain Tasks and LRPs.

The Diego Cell consists of the following:

- [Rep](#)
- [Executor](#)
- [Garden](#)
- [Metron Agent](#)
- [Route-emitter](#)

## Rep

- Represents a Cell in Diego Auctions for Tasks and LRPs
- Mediates all communication between the Cell and the BBS
- Ensures synchronization between the set of Tasks and LRPs in the BBS with the containers present on the Cell
- Maintains the presence of the Cell in the BBS

- Runs Tasks and LRPs by asking the in-process Executor to create a container and `RunAction` recipes

See the [Rep repository](#) on GitHub for more information.

## Executor

- Runs as a logical process inside the Rep
- Implements the generic Executor actions detailed in the [API documentation](#)
- Streams `STDOUT` and `STDERR` to the Metron agent running on the Cell

See the [Executor repository](#) on GitHub for more information.

## Garden

- Provides a platform-independent server and clients to manage Garden containers
- Defines the [Garden-runC](#) interface for container implementation

See the [Garden](#) topic or the [Garden repository](#) on GitHub for more information.

## Metron Agent

Forwards app logs, errors, and app and Diego metrics to the [Loggregator](#) Doppler component

See the [Metron repository](#) on GitHub for more information.

## Route-Emitter

- Monitors `DesiredLRP` and `ActualLRP` states, emitting route registration and unregistration messages to the Cloud Foundry [Gorouter](#) when it detects changes
- Periodically emits the entire routing table to the Cloud Foundry Gorouter

See the [Route-Emitter repository](#) on GitHub for more information.

## Database VMs

The Diego database VM consists of the following components.

### Diego Bulletin Board System

- Maintains a real-time representation of the state of the Diego cluster, including all desired LRPs, running LRP instances, and in-flight Tasks
- Provides an RPC-style API over HTTP to [Diego Core](#) components and external clients, including the [SSH Proxy](#) and [Route-Emitter](#).
- Ensure consistency and fault tolerance for Tasks and LRPs by comparing desired state (stored in the database) with actual state (from running instances)
- Acts to keep `DesiredLRP` count and `ActualLRP` count synchronized in the following ways:
  - If the `DesiredLRP` count exceeds the `ActualLRP` count, requests a start auction from the Auctioneer
  - If the `ActualLRP` count exceeds the `DesiredLRP` count, sends a stop message to the Rep on the Cell hosting an instance
- Monitors for potentially missed messages, resending them if necessary

See the [Bulletin Board System repository](#) on GitHub for more information.

## MySQL

- Provides a consistent key-value data store to Diego

## Locket

- Provides a consistent key-value store for maintenance of distributed locks and component presence

## Go MySQL Driver

The Diego BBS stores data in MySQL. Diego uses the Go MySQL Driver to communicate with MySQL.

See the [Go MySQL Driver repository](#) on GitHub for more information.

## BOSH DNS

- Provides service discovery through colocated DNS servers on all BOSH-deployed VMs
- Provides client-side load-balancing by randomly selecting a healthy VM when multiple VMs are available

See the [BOSH DNS documentation](#) for more information.

# Platform-Specific Components

## Garden Back Ends

Garden contains a set of interfaces that each platform-specific backend must implement. See the [Garden](#) topic or the [Garden repository](#) on GitHub for more information.

## App Lifecycle Binaries

The following three platform-specific binaries deploy apps and govern their lifecycle:

- The **Builder**, which stages a CF app. The Builder runs as a Task on every staging request. It performs static analysis on the app code and does any necessary pre-processing before the app is first run.
- The **Launcher**, which runs a CF app. The Launcher is set as the Action on the `DesiredLRP` for the app. It executes the start command with the correct system context, including working directory and environment variables.
- The **Healthcheck**, which performs a status check on running CF app from inside the container. The Healthcheck is set as the Monitor action on the `DesiredLRP` for the app.

## Current Implementations

- [Buildpack App Lifecycle](#) implements the Cloud Foundry buildpack-based deployment strategy.
- [Docker App Lifecycle](#) implements a Docker deployment strategy.

## Application SSH Components and Processes

Page last updated:

This document describes details about the Pivotal Application Service SSH components for access to deployed application instances. Pivotal Application Service supports native SSH access to applications and load balancing of SSH sessions with the load balancer for your PAS deployment.

The [SSH Overview](#) document describes procedural and configuration information about application SSH access.

### SSH Components

The PAS SSH includes the following central components, which are described in more detail below:

- An implementation of an SSH [proxy server](#).
- A lightweight SSH [daemon](#).

If these components are deployed and configured correctly, they provide a simple and scalable way to access containers apps and other long running processes (LRPs).

### SSH Daemon

The SSH daemon is a lightweight implementation that is built around the Go SSH library. It supports command execution, interactive shells, local port forwarding, and secure copy. The daemon is self-contained and has no dependencies on the container root file system.

The daemon is focused on delivering basic access to application instances in PAS. It is intended to run as an unprivileged process, and interactive shells and commands will run as the daemon user. The daemon only supports one authorized key, and it is not intended to support multiple users.

The daemon can be made available on a file server and Diego LRPs that want to use it can include a download action to acquire the binary and a run action to start it. PAS applications will download the daemon as part of the lifecycle bundle.

### SSH Proxy Authentication

The SSH proxy hosts the user-accessible SSH endpoint and is responsible for authentication, policy enforcement, and access controls in the context of PAS. After a user has successfully authenticated with the proxy, the proxy will attempt to locate the target container and create an SSH session to a daemon running inside the container. After both sessions have been established, the proxy will manage the communication between the user's SSH client and the container's SSH Daemon.

## How Diego Balances App Processes

Page last updated:

[Diego](#) balances app processes over the virtual machines (VMs) in a Cloud Foundry (CF) installation using the Diego Auction. When new processes need to be allocated to VMs, the Diego Auction determines which ones should run on which machines. The auction algorithm balances the load on VMs and optimizes app availability and resilience. This topic explains how the Diego Auction works.

Refer to the [Auction repository](#) on GitHub for source code and more information.

## Tasks and Long-Running Processes

The Diego Auction distinguishes between two types of jobs: **Tasks** and **Long-Running Processes (LRPs)**.

- **Tasks** run once, for a finite amount of time. A common example is a staging task that compiles an app's dependencies, to form a self-contained droplet that makes the app portable and runnable on multiple VMs. Other examples of tasks include making a database schema change, bulk importing data to initialize a database, and setting up a connected service.
- **Long-Running Processes** run continuously, for an indefinite amount of time. LRP terminate only if stopped or killed, or if they crash. Examples include web servers, asynchronous background workers, and other applications and services that continuously accept and process input. To make high-demand LRPs more available, Diego may allocate multiple instances of the same application to run simultaneously on different VMs, often spread across Availability Zones that serve users in different geographic regions.

The Diego Auction process repeats whenever new jobs need to be allocated to VMs. Each auction distributes a current **batch** of work, Tasks and LRPs, that can include newly-created jobs, jobs left unallocated in the previous auction, and jobs left orphaned by failed VMs. Diego does not redistribute jobs that are already running on VMs. Only one auction can take place at a time, which prevents placement collisions.


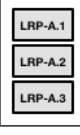

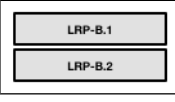
## Ordering the Auction Batch

The Diego Auction algorithm allocates jobs to VMs to fulfill the following outcomes, in decreasing **priority** order:

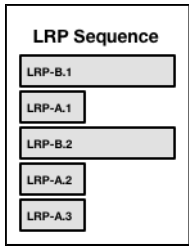
1. Keep at least one instance of each LRP running.
2. Run all of the Tasks in the current batch.
3. Distribute as much of the total desired LRP load as possible over the remaining available VMs, by spreading multiple LRP instances broadly across VMs and their Availability Zones.

To achieve these outcomes, each auction begins with the [Diego Auctioneer](#) component arranging the batch's jobs into a priority order. Some of these jobs may be duplicate instances of the same process that Diego needs to allocate for high-traffic LRPs, to meet demand. So the Auctioneer creates a list of multiple LRP instances based on the desired instance count configured for each process.

For example, if the process LRP-A has a desired instance count of 3 and a memory load of 2, and process LRP-B has 2 desired instances and a load of 5, the Auctioneer creates a list of jobs for each process as follows:

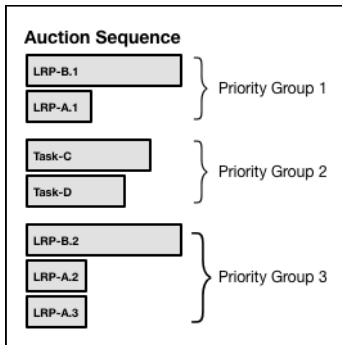
| Process | Desired Instances | Load                                                                                  | Jobs                                                                                  |
|---------|-------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| LRP-A   | 3                 | 2  |  |
| LRP-B   | 2                 | 5  |  |

The Auctioneer then builds an ordered sequence of LRP instances by cycling through the list of LRPs in decreasing order of load. With each cycle, it adds another instance of each LRP to the sequence, until all desired instances of the LRP have been added. With the example above, the Auctioneer would order the LRPs like this:



The Auctioneer then builds an ordered sequence for all jobs, both LRPs and Tasks. Reflecting the auction batch [priority order](#), the first instances of LRPs are first priority. Tasks are next, in decreasing order of load. Duplicate LRP jobs come last.

Adding one-time Task-C (load = 4) and Task-D (load = 3) to the above example, the priority order becomes:



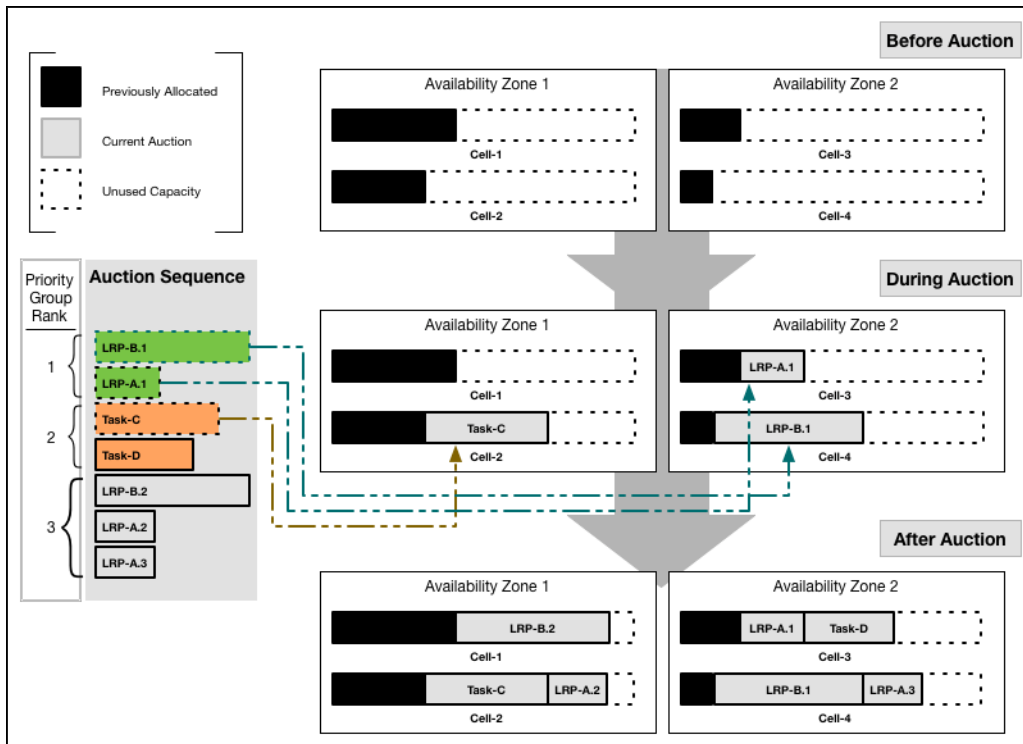
## Auctioning the Batch to the Cells

With all jobs sorted in priority order, the Auctioneer allocates each in turn to one of the VMs. The process resembles an auction, where VMs “bid” with their suitability to run each job. Facilitating this process, each app VM has a resident [Cell](#) that monitors and allocates the machine’s operation. The Cell participates in the auction on behalf of the virtual machine that it runs on.

Starting with the highest-priority job in the ordered sequence, the Auctioneer polls all the Cells on their fitness to run the currently-auctioned job. Cells “bid” to host each job according to the following priorities, in decreasing order:

1. Allocate all jobs only to Cells that have the correct software stack to host them, and sufficient resources given their allocation so far during this auction.
2. Allocate LRP instances into Availability Zones that are not already hosting other instances of the same LRP.
3. Within each Availability Zone, allocate LRP instances to run on Cells that are not already hosting other instances of the same LRP.
4. Allocate any job to the Cell that has lightest load, from both the current auction and jobs it has been running already. In other words, distribute the total load evenly across all Cells.

Our example auction sequence has seven jobs: five LRP instances and two Tasks. The following diagram shows how the Auctioneer might distribute this work across four Cells running in two Availability Zones:



If the Auctioneer reaches the end of its sequence of jobs, having distributed all jobs to the Cells, it submits requests to the Cells to execute their allotted work. If the Cells ran out of capacity to handle all jobs in the sequence, the Auctioneer carries the unallocated jobs over and merges them into the next auction batch, to be allocated in the next auction.

## Triggering Another Auction

The Diego Auction process repeats to adapt a Cloud Foundry deployment to its changing workload. For example, the BBS initiates a new auction when it detects that the actual number of running instances of LRPs does not match the number desired. Diego's BBS component monitors the number of instances of each LRP that are currently running. The [BBS](#) component periodically compares this number with the desired number of LRP instances, as configured by the user. If the actual number falls short of what is desired, the BBS triggers a new auction. In the case of a surplus of application instances, the BBS kills the extra instances and initiates another auction.

The Cloud Controller also triggers an auction whenever a Cell fails. After any auction, if a Cell responds to its work request with a message that it cannot perform the work after all, the Auctioneer carries the unallocated work over into the next batch. But if the Cell fails to respond entirely, for example if its connection times out, the unresponsive Cell may still be running its work. In this case, the Auctioneer does not automatically carry the Cell's work over to the next batch. Instead, the Auctioneer defers to the BBS to continue monitoring the states of the Cells, and to re-assign unassigned work later if needed.

## PCF Operator Guide

### For PCF Operators

This guide shows you how to run a PCF platform. This ongoing responsibility may include but is not limited to:

- Configuring PCF capabilities
- Integrating PCF with external systems
- Updating PCF and installed products
- Monitoring PCF health and performance
- Adjusting PCF resources and options to fix health or performance issues
- Diagnosing and troubleshooting PCF problems
- Managing Pivotal Application Service (PAS) users, resources, and infrastructure
- Installing software services and otherwise enabling PCF developers
- Maintaining PCF
- Keeping PCF secure

If you do these things, you are a PCF **operator**, and the contents of this guide are for you.

### Guide Contents

- [Day 2 Configurations](#) - Setting up internal operations and external integrations for PCF.
- [Ongoing Operations](#) - Routine procedures for running and growing the platform, including:
  - PCF Upgrades
  - IaaS Changes
  - Monitoring, Logging, and Reporting
  - Platform Tuning
  - Enabling Developers
  - Backing Up
  - Security
- [Managing PAS Runtimes](#) - Procedures performed by people with administrator or manager roles in Pivotal Application Service (PAS), such as managing users, orgs, spaces, and service instances. Operators can perform these actions by [logging in with Admin credentials](#), which grants them the role of Org Manager across all PAS orgs.
- [Using Ops Manager](#) - Ops Manager's dashboard interface streamlines the installation, configuration, and upgrading of PCF platform services and add-ons.
- [Using the Cloud Foundry Command Line Interface \(cf CLI\)](#) - Using the cf CLI to send commands to the Cloud Controller, the executive component of PAS.
- [Troubleshooting and Diagnostics](#) - Tools and procedures for troubleshooting PCF.



## Identifying the API Endpoint for Your PAS Instance

Page last updated:

The API endpoint for your Pivotal Application Service (PAS) deployment, its target URL, is the API endpoint of the deployment's Cloud Controller. Find your Cloud Controller API endpoint by consulting your cloud operator, from the Apps Manager, or from the command line.

### From the Apps Manager

Log in to the Apps Manager for your PAS instance, then click **Tools** in the left navigation panel. The **Getting Started** section of the Tools page shows your API endpoint.

```
GETTING STARTED

$ cf help
$ cf login -a https://api.your_endpoint.com
API endpoint: https://api.your_endpoint.com
Username> your_username
Password> your_password
Org> your_org
Space> your_space
$ cf push your_app
```

### From the Command Line

From a command line, use the `cf api` command to view your API endpoint.

Example:

```
$ cf api
API endpoint: https://api.example.com (API version: 2.2.0)
```

## Creating New PAS User Accounts

Page last updated:

When you first deploy your [Pivotal Application Service \(PAS\)](#), there is only one user: an administrator. At this point, you can add accounts for new users who can then push applications using the Cloud Foundry Command Line Interface (cf CLI).

How to add users depends on whether or not you have SMTP enabled, as described in the options below.

### Option 1: Adding New Users when SMTP is Enabled

If you have enabled SMTP, your users can sign up for accounts and create their own orgs. They do this using the [Pivotal Cloud Foundry](#) (PCF) Apps Manager, a self-service tool for managing organizations, users, applications, and application spaces.

Instruct users to complete the following steps to log in and get started using the Apps Manager.

1. Browse to `apps.YOUR-SYSTEM-DOMAIN`. Refer to PAS **Domains** to locate your system domain.
2. Select **Create an Account**.
3. Enter your email address and click **Create an Account**. You will receive an email from the Apps Manager when your account is ready.
4. When you receive the new account email, follow the link in the email to complete your registration.
5. You will be asked to choose your organization name.

You now have access to the Apps Manager. Refer to the Apps Manager documentation at [docs.pivotal.io](#) for more information about using the Apps Manager.

### Option 2: Adding New Users when SMTP is Not Enabled

If you have not enabled SMTP, only an administrator can create new users, and there is no self-service facility for users to sign up for accounts or create orgs.

The administrator creates users with the cf CLI. See [Creating and Managing Users with the cf CLI](#).

[Return to the Installing Pivotal Cloud Foundry Guide](#)

## Configuring SSL/TLS Termination at HAProxy

Page last updated:

Both Pivotal Application Service (PAS) and Isolation Segments for Pivotal Cloud Foundry include an HAProxy instance.

HAProxy is appropriate to use in a deployment when features are needed that are offered by HAProxy but are not offered by the CF Routers or IaaS-provided load balancers such as with Azure load balancers. These include filtering of protected domains from trusted networks.

While HAProxy instances provide load balancing for the Gorouters, HAProxy is not itself highly available. For production environments, use a highly-available load balancer to scale HAProxy horizontally. The load balancer does not need to terminate TLS or even operate at layer 7 (HTTP); it can simply provide layer 4 load balancing of TCP connections. Use of HAProxy does not remove the need for CF Routers; the Gorouter must always be deployed for HTTP applications, and TCP Router for non-HTTP applications.

You can generate a self-signed certificate for HAProxy if you do not want to obtain a signed certificate from a well-known certificate authority.


## Procedure: Terminate SSL/TLS at HAProxy

In PCF, perform the following steps to configure SSL termination on HAProxy:

1. Navigate to the Ops Manager Installation Dashboard.
2. Click the **Pivotal Application Service** tile in the Installation Dashboard.
3. Click **Networking**.
4. Configure the following based on the IaaS of your PCF deployment.

| If your PCF deployment is on: | Then configure the following:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | See also:                                                                                                                                                 |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| OpenStack or vSphere          | <p>Decide whether you want your HAProxy to be highly available.</p> <ul style="list-style-type: none"> <li>◦ If you need highly available HAProxy, then perform the following steps: <ol style="list-style-type: none"> <li>1. Choose an IP address for each HAProxy instance on the subnet where you deployed PCF.</li> <li>2. In the <b>HAProxy IPs</b> field of the <b>Networking</b> page, enter the IP addresses you have selected for your HAProxy instances.</li> <li>3. Configure your load balancer (for example, F5 or NSX) to forward domain names to the HAProxy IP addresses.</li> </ol> </li> <li>◦ If you do not require high availability (for example, you are setting up a development environment), then perform the following steps: <ol style="list-style-type: none"> <li>1. Skip setting up the load balancer.</li> <li>2. Choose one IP address for the single HAProxy instance.</li> <li>3. Configure DNS to point at the IP address. See <a href="#">How to Set Up DNS for HAProxy</a>.</li> </ol> </li> </ul> | For more information, see the Pivotal Application Service (PAS) networking configuration topic for <a href="#">OpenStack</a> or <a href="#">vSphere</a> . |
| AWS, GCP or Azure             | <ol style="list-style-type: none"> <li>1. Leave the HAProxy IP address blank.</li> <li>2. In the <b>Resource Config</b> page of PAS tile, locate the HAProxy job.</li> <li>3. In the <b>Load Balancer</b> column for the HAProxy job, specify the appropriate IaaS load balancer resource.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | For more information, see the PAS installation instructions for <a href="#">AWS</a> , <a href="#">Azure</a> , or <a href="#">GCP</a> .                    |

5. In the **Certificates and Private Keys for HAProxy and Routerfield**, click the **Add** button to define at least one certificate keypair for HAProxy and Router. For each certificate keypair that you add, assign a name, enter the PEM-encoded certificate chain and PEM-encoded private key. You can either upload your own certificate or generate an RSA certificate in PAS. For options and instructions on creating a certificate for your wildcard domains, see [Creating a Wildcard Certificate for PCF Deployments](#).

6. In the **Minimum version of TLS supported by HAProxy and Router**, select the minimum version of TLS to use in HAProxy communications. HAProxy use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the HAProxy, see [TLS Cipher Suites](#).
  7. Under **HAProxy forwards requests to Router over TLS**, leave **Enabled** selected and provide the backend certificate authority.
  8. If you want to use a specific set of TLS ciphers for HAProxy, configure **TLS Cipher Suites for HAProxy**. Enter an ordered, colon-separated list of TLS cipher suites in the OpenSSL format. For example, if you have selected support for an earlier version of TLS, you can enter cipher suites supported by this version. For a list of TLS ciphers supported by the HAProxy, see [TLS Cipher Suites](#).
  9. If you expect requests larger than the default maximum of 16 Kbytes, enter a new value (in bytes) for **HAProxy Request Max Buffer Size**. You may need to do this, for example, to support apps that embed a large cookie or query string values in headers.
  10. If you want to force browsers to use HTTPS when making requests to HAProxy, select **Enable** in the **HAProxy support for HSTS** field and complete the following optional configuration steps:
    - a. (Optional) Enter a **Max Age in Seconds** for the HSTS request. By default, the age is set to one year. HAProxy will force HTTPS requests from browsers for the duration of this setting.
    - b. (Optional) Select the **Include Subdomains** checkbox to force browsers to use HTTPS requests for all component subdomains.
    - c. (Optional) Select the **Enable Preload** checkbox to force instances of Google Chrome, Firefox, and Safari that access your HAProxy to refer to their built-in lists of known hosts that require HTTPS, of which HAProxy is one. This ensures that the first contact a browser has with your HAProxy is an HTTPS request, even if the browser has not yet received an HSTS header from your HAProxy.
  11. (Optional) If you are not using SSL encryption or if you are using self-signed certificates, you can select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.
-  Use this checkbox only for development and testing environments. Do not select it for production environments.
12. (Optional) If you do not want HAProxy or the Gorouter to accept any non-encrypted HTTP traffic, select the **Disable HTTP on HAProxy and Router** checkbox.
  13. In the **Configure the CF Router support for the X-Forwarded-Cert header** field, select **Always forward the XFCC header in the request, regardless of the whether the client connection is mTLS**.
  14. (Optional) If your PCF deployment uses HAProxy and you want it to receive traffic only from specific sources, use the following fields:
    - o **Protected Domains**: Enter a comma-separated list of domains from which PCF can receive traffic.
    - o **Trusted CIDRs**: Optionally, enter a space-separated list of CIDRs to limit which IP addresses from the Protected Domains can send traffic to PCF.
  15. Click **Save**.

## How to Set Up DNS for HAProxy

You only need to perform this procedure if you are using one instance of HAProxy such as in a development environment. If you would like HAProxy to be highly available, you must have a load balancer in front of it. In this case, you would point DNS at the load balancer.

To use a single instance HAProxy load balancer in a vSphere or OpenStack deployment, create a wildcard A record in your DNS and configure some fields in the PAS product tile.

1. Create an A record in your DNS that points to the HAProxy IP address. The A record associates the **System Domain** and **Apps Domain** that you configure in the **Domains** section of the PAS tile with the HAProxy IP address.

For example, with `cf.example.com` as the main subdomain for your Cloud Foundry (CF) deployment and an HAProxy IP address `203.0.113.1`, you must create an A record in your DNS that serves `example.com` and points `*.cf` to `203.0.113.1`.

| Name | Type | Data        | Domain      |
|------|------|-------------|-------------|
| *.cf | A    | 203.0.113.1 | example.com |

2. Use the Linux `host` command to test your DNS entry. The `host` command should return your HAProxy IP address.

Example:

```
$ host cf.example.com
cf.example.com has address 203.0.113.1
$ host anything.example.com
anything.cf.example.com has address 203.0.113.1
```

## Configuring Frontend Idle Timeout for Gorouter and HAProxy

This topic describes how to configure the **Frontend Idle Timeout for Gorouter and HAProxy** field in the Pivotal Application Service (PAS) **Networking** pane.

You can optionally use the **Frontend Idle Timeout for Gorouter and HAProxy** field to help prevent connections from your load balancer to Gorouter or HAProxy from being closed prematurely. The value you enter sets the duration, in seconds, that Gorouter or HAProxy maintains an idle open connection from a load balancer that supports keep-alive.

In general, set the value higher than your load balancer's backend idle timeout to avoid the race condition where the load balancer sends a request before it discovers that Gorouter or HAProxy has closed the connection.

See the following table for specific guidance and exceptions to this rule:

| aaS   | Guidance                                                                                                                                                                                                                                                          |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS   | AWS ELB has a default timeout of 60 seconds, so Pivotal recommends a value greater than <code>60</code> .                                                                                                                                                         |
| Azure | By default, Azure load balancer times out at 240 seconds without sending a TCP RST to clients, so as an exception, Pivotal recommends a value lower than <code>240</code> to force the load balancer to send the TCP RST.                                         |
| GCP   | GCP has a default timeout of 600 seconds. For GCP HTTP load balancers, Pivotal recommends a value greater than <code>600</code> . For GCP TCP load balancers, Pivotal recommends a value less than <code>600</code> to force the load balancer to send a TCP RST. |
| Other | Set the timeout value to be greater than that of the load balancer's backend idle timeout.                                                                                                                                                                        |

## Configuring Route Service Lookup

This topic describes configuring route service lookup in Pivotal Application Service (PAS).

### Overview

Developers can bind their app to a route service to preprocess requests before they reach an app. Example use cases include authentication, rate limiting, and caching services. For more information, see [Route Services](#).

The **Bypass security checks for route service lookup** field in the PAS tile allows you to configure how the router handles traffic for apps that are bound to route services. The configuration options are as follows:

- **Default Lookup:**
  - Default lookup is configured when you do not select **Bypass security checks for route service lookup**. In this case, the router does not check for an existing route. It sends traffic back through the load balancer when the traffic is for an internal route service.
- **Bypass Mode:**
  - Bypass mode is configured when you select **Bypass security checks for route service lookup**. The router checks for an existing route. If the router finds the route and the route service is internal, it sends the traffic directly to the route service and skips the load balancer. This improves performance, but introduces the security risk described in [Bypass Mode and External Route Service \(Security Risk\)](#).

For more details, see [Summary of Behavior in Different Configurations](#) below.

For configuration guidance and procedures, see [Configure Route Service Lookup](#) below.

## Configure Route Service Lookup

The following sections provide guidance and configuration steps for route service lookup.

### Guidance

Pivotal recommends that you do not configure PAS for bypass mode because of the security risk described in [Bypass Mode and External Route Service \(Security Risk\)](#). However, you may need to do so if your load balancer requires mutual TLS from clients.

If your load balancer requires mutual TLS from clients and PAS is configured for default lookup, the router cannot handle traffic successfully for internal route services. This is because the router does not have the necessary certificates from the client to communicate back with the load balancer for DNS lookup. Therefore you must configure bypass mode so the router can send the traffic directly to the route service.

### Configuring PAS for Bypass Mode


To configure bypass mode, do the following:

1. Select **Bypass security checks for route service lookup** in the **Networking** pane of the PAS tile.
2. Follow the steps in [Mitigate Security Risk](#).

### Mitigate Security Risk

To prevent users from intercepting traffic for externally hosted route services, do the following.

1. Create an org for use by the PAS administrator.
2. Register all external route service domains as private domains in the org you created.
3. Monitor PAS for the addition of new external route services and ensure you follow the same process for those. One way to do this is by using `cf curl` to regularly view a list of user-provided service instances. You can do this by running `cf curl /v2/user_provided_service_instances`.

 **Note:** Since route services can be added by any space developer, this may be difficult to manage.

## Configuring PAS for Default Lookup

To configure PAS for default lookup behavior, with bypass mode disabled, do the following:

1. Ensure that **Bypass security checks for route service lookup** in the **Networking** pane of the PAS tile is not selected.
2. Communicate to developers of route services that the domain name for their internally hosted route services must resolve to the load balancer.
3. If your load balancer or router terminates TLS, do the following:
  - a. Work with developers of route services to ensure the load balancer or router have TLS certificates that are valid for the route service URL.
  - b. Ensure that the TLS certificate from your load balancer is either signed by a well known CA, or the CA has been added to the **Certificate Authorities Trusted by Router and HAProxy** field in the **Networking** pane of the PAS and Isolation Segment tiles. The CA for the TLS certificate provided by the load balancer must be trusted by the Router.
4. Work with route service developers to verify that their internal route service apps are reachable. You can do this by visiting the HTTPS URL of the route service directly and confirming that the app received the request with the `cf logs` output for the route service app.

## Summary of Behavior in Different Configurations

The following sections describe how the router behaves when bypass mode is enabled or disabled and when a route service is internal or external.

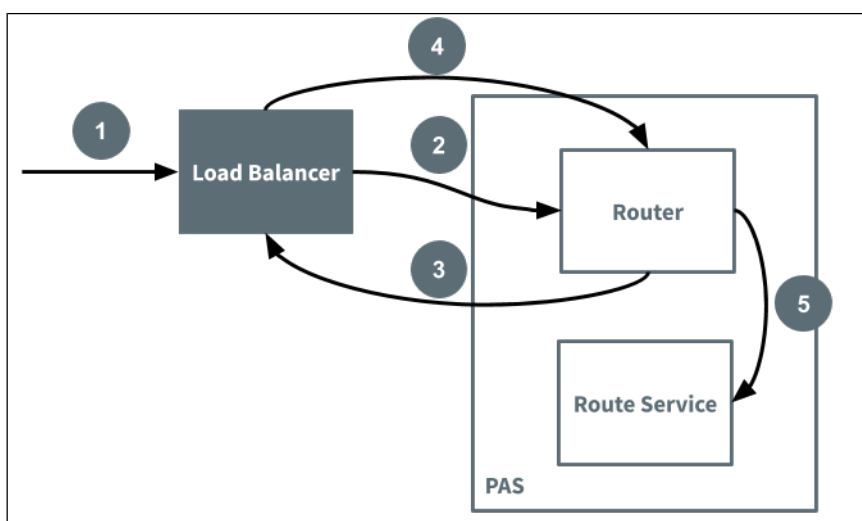
### Default Lookup and Internal Route Service

This section describes how the router handles app requests when the following is true:

- The **Bypass security checks for route service lookup** field in PAS is not selected.
- The app is bound to a route service that is hosted on PAS.

In this case, when the router receives the request, it sends the traffic back to the load balancer to resolve DNS. The load balancer then sends the traffic back to the router.

The following diagram illustrates the flow of the request and numbers the steps to indicate order of occurrence.



### Bypass Mode and Internal Route Service

This section describes how the router handles app requests when the following is true:

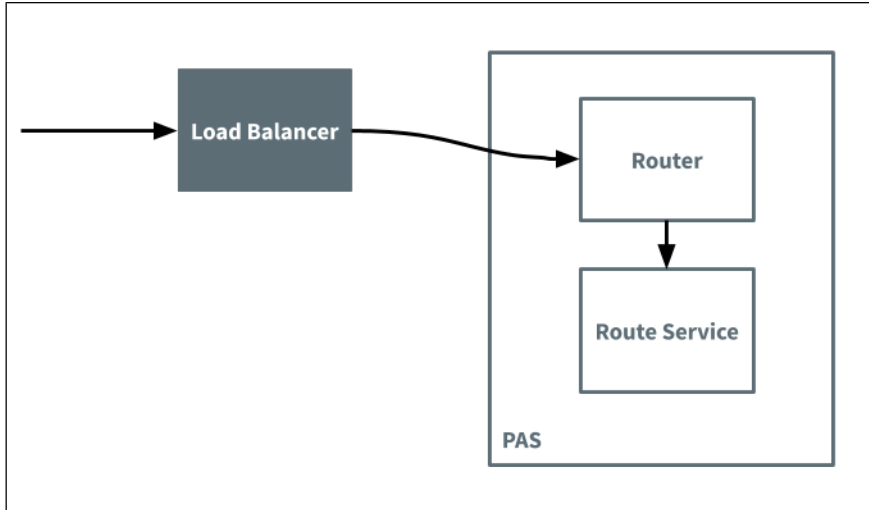
- The **Bypass security checks for route service lookup** field in PAS is selected.



- The app is bound to a route service that is hosted on PAS

In this case, when the router receives the request, it sends it directly to the route service. This assumes the router finds an existing route for the route service.

The following diagram illustrates the flow of the request.



## Bypass Mode and External Route Service (Security Risk)

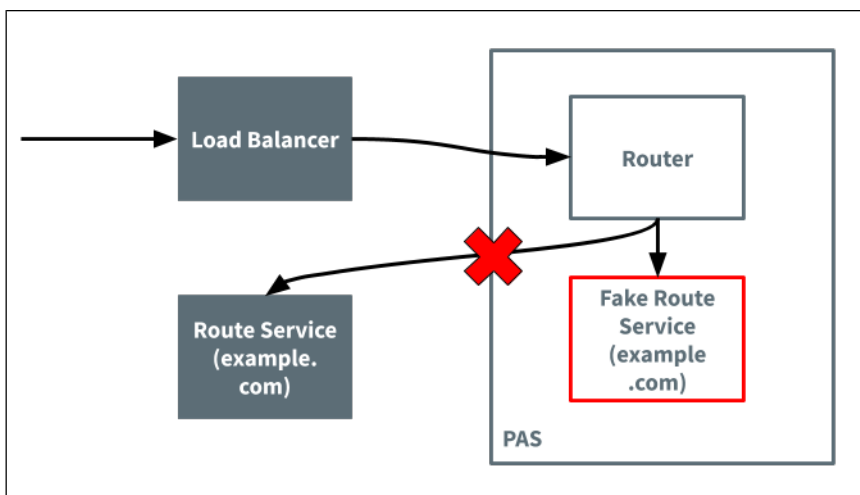
This section describes how the router handles app requests when the following is true:

- The **Bypass security checks for route service lookup** field in PAS is selected.
- The app is bound to a route service that is hosted outside of PAS.

In this case, when the router receives the request, it checks for an existing route and then sends the request directly to the route service. This introduces the ability for route service traffic to be intercepted. A developer can register the external route service domain as a private domain in PAS and map it to their own, malicious app. When the router receives a request for the original app bound to the external route service, it will find the domain internally and send the request to the malicious app.

**Note:** This vulnerability exists for both externally hosted route services and route services hosted on a separate foundation. If all of your route services are hosted internally on the same foundation, you are not at risk for this vulnerability. However, you would be at risk if externally hosted route services are later configured.

The following diagram illustrates the flow of the request in the case that it is intercepted:



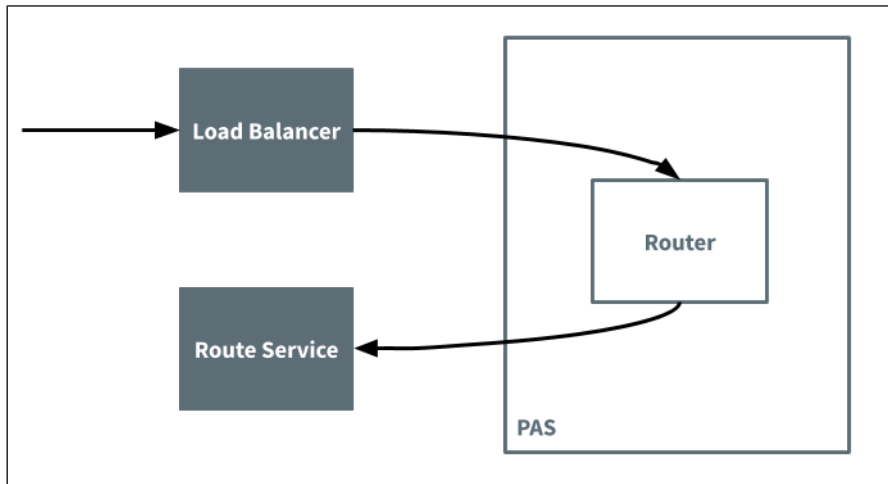
## Default Lookup and External Route Service

This section describes how the router handles app requests when the following is true:

- The **Bypass security checks for route service lookup** field in PAS is not selected.
- The app is bound to a route service that is hosted outside of PAS.

In this case, the router sends traffic directly to the external route service without checking for an existing route.

The following diagram illustrates the flow of the request.



## Configuring Proxy Settings for All Applications

This topic describes how to globally configure proxy settings for all applications in your Pivotal Cloud Foundry (PCF) deployment. Some environments restrict access to the Internet by requiring traffic to pass through an HTTP or HTTPS proxy. PCF operators can use the Cloud Foundry Command Line Interface (cf CLI) to provide the proxy settings to all applications, including system applications and service brokers.

**Note:** Incorrectly configuring proxy settings can prevent applications from connecting to the Internet or accessing required resources. They can also cause errands to fail and break system applications and service brokers. Although errands, system applications, and service brokers do not need to connect to the Internet, they often need to access other resources on PCF. Incorrect proxy settings can break these connections.

## Set Environment Variables

To globally configure proxy settings for PCF applications, perform the following steps to set three environment variables for both the staging environment variable group and the running environment variable group.

For more information about variable groups, see the [Environment Variable Groups](#) section in the *Cloud Foundry Environment Variables* topic.

This procedure explains how to set proxy information for both staging and running applications. However, you can set proxy settings for only staging or only running applications.

1. Target your Cloud Controller with the cf CLI. If you have not installed the cf CLI, see the [Installing the cf CLI](#) topic.

```
$ cf api api.YOUR-SYSTEM-DOMAIN
Setting api endpoint to api.YOUR-SYSTEM-DOMAIN...
OK
API endpoint: https://api.YOUR-SYSTEM-DOMAIN (API version: 2.54.0)
Not logged in. Use 'cf login' to log in.
```

2. Log in with your UAA administrator credentials. To retrieve these credentials, navigate to the Pivotal Application Service (PAS) tile in the Ops Manager Installation Dashboard and click **Credentials**. Under **UAA**, click **Link to Credential** next to **Admin Credentials** and record the password.

```
$ cf login
API endpoint: https://api.YOUR-SYSTEM-DOMAIN

Email> admin
Password>
Authenticating...
OK
```

3. To configure proxy access for applications that are staging, run the following command, replacing the placeholder values:

```
$ cf set-staging-environment-variable-group '{"http_proxy": "http://YOUR-PROXY:8080/", "https_proxy": "http://YOUR-PROXY:8080/", "no_proxy": "NO-PROXY.EXAMPLE.COM"}
```

- `http_proxy`: Set this value to the proxy to use for HTTP requests.
- `https_proxy`: Set this value to the proxy to use for HTTPS requests. In most cases, this will be the same as `http_proxy`.
- `no_proxy`: Set this value to a comma-separated list of DNS names or IP addresses that can be accessed without passing through the proxy. This value may not be needed, because it depends on your proxy configuration. From now on, the proxy settings are applied to staging applications.

4. To configure proxy access for applications that are running, run the following command, replacing the placeholder values as above:

```
$ cf set-running-environment-variable-group '{"http_proxy": "http://YOUR-PROXY:8080/", "https_proxy": "http://YOUR-PROXY:8080/", "no_proxy": "NO-PROXY.EXAMPLE.COM"}
```

To configure proxy settings for Java-based applications, use the following command instead, replacing the placeholder values. For `http.nonProxyHosts`, use a pipe-delimited list rather than a comma-separated list.

```
$ cf set-running-environment-variable-group '{"JAVA_OPTS": "-Dhttp.proxyHost=YOUR-PROXY -Dhttp.proxyPort=8080 -Dhttp.nonProxyHosts=NO-PROXY.EXAMPLE.COM"}'
```

For more information about these Java proxy settings, see [Java Networking and Proxies](#).

5. To apply the proxy configuration for the running environment variable group, you must restart each application that you want to use the new configuration.

## Troubleshooting

If an application fails after you apply the global proxy settings, try the following solutions.

### Exclude an App From Global Proxy Settings

If your application fails, try instructing the application to ignore the global proxy settings. Perform the following commands to manually unset the proxy environment variables for the failing application:

1. Set the proxy environment variables for `http_proxy` to an empty value:

```
$ cf set-env YOUR-APP http_proxy "
```

2. Set the proxy environment variables for `https_proxy` to an empty value:

```
$ cf set-env YOUR-APP https_proxy "
```

3. Set the proxy environment variables for `no_proxy` to an empty value:

```
$ cf set-env YOUR-APP no_proxy "
```

### Change Case of HTTP

Your application and language runtime may be case-sensitive. Try performing the steps in the [Set Environment Variables](#) section using uppercase for `HTTP_PROXY`, `HTTPS_PROXY`, and `NO_PROXY` instead of lowercase. Refer to the following example.

```
$ cf set-staging-environment-variable-group '{"HTTP_PROXY": "http://YOUR-PROXY:8080/", "HTTPS_PROXY": "http://YOUR-PROXY:8080/"}'
```

### Check Proxy Settings

If you have set up your proxy so that it can only send traffic to the Internet, then a request to an internal resource like PCF fails. You must set `no_proxy` so that traffic destined for PCF and other internal resources is sent directly and does not go through the proxy. For instance, setting `no_proxy` to include your system and application domains will ensure that requests destined for those domains are sent directly.

### Verify Interpretation

The interpretation of `no_proxy` depends on the application and the language runtime. Most support `no_proxy`, but the specific implementation may vary. For example, some match DNS names that end with the value set in `no_proxy`: `example.com` would match `test.example.com`. Others support the use of the asterisk as a wildcard to provide basic pattern matching in DNS names: `*.example.com` would match `test.example.com`. Most applications and language runtimes do not support pattern matching and wildcards for IP addresses.

## Restricting App Access to Internal PCF Components

This topic describes how to secure the component virtual machines (VMs) of your Pivotal Cloud Foundry (PCF) deployment from being accessed by apps.

### Introduction


See the following list to understand the concepts for this topic:

- **How PCF determines where apps can send traffic:**
  - PCF uses *Application Security Groups (ASGs)*, which are network policy rules specifying protocols, ports, and IP ranges that apply to outbound network connections initiated from apps. See [ASGs](#).
- **Why you must create new rules for outbound app traffic:**
  - PCF installs with a [default ASG](#) that allows apps running on your deployment to send traffic to almost any IP address. This means apps are not blocked from initiating connections to most network destinations unless an administrator takes action to update the ASGs with a more restrictive policy.
- **How you can set up new rules:**
  - To help secure your component VMs against apps while ensuring your apps can access the services they need, follow the [procedure](#) below, which includes these steps:

| Step | Description                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <a href="#">Determine Your Network Layout:</a><br>The procedure for securing your deployment with ASGs varies depending on your network layout, which you can determine using Ops Manager.                                                           |
| 2    | <a href="#">Ensure Access for PCF System Apps:</a><br>Bind the default ASG to the <code>system</code> org so that PCF system apps can continue accessing the system components they need after you remove the deployment-wide default ASG in Step 4. |
| 3    | <a href="#">Create New ASGs:</a><br>Block apps from sending traffic to system components, but allow them to send traffic to the services they need.                                                                                                  |
| 4    | <a href="#">Remove the Default ASG:</a><br>After you create and bind new ASGs, you no longer need the deployment-wide default ASG bindings that allow apps to send traffic to any IP.                                                                |
| 5    | <a href="#">Restart your Apps:</a><br>To apply the ASG changes, you must restart all of the apps in your deployment.                                                                                                                                 |

- **When to set up new rules:**
  - Pivotal recommends that you complete this procedure directly after installing PCF, prior to developers pushing apps to the platform. If you complete the procedure after apps have been pushed to the platform, you must restart all the apps in your deployment.

### Prerequisites

The procedure below requires that you have the latest release of [ASG Creator](#)  from the Cloud Foundry incubator repository on Github. See [About the ASG Creator Tool](#).

### Procedure


Follow these steps to apply ASGs that prevent apps running on your deployment from accessing internal PCF components.

#### Step 1: Determine Your Network Layout

The procedure for securing your deployment with ASGs varies depending on your network layout, which you can determine by following these steps:

1. Log in to Ops Manager.

- For each tile, click **Assign AZs and Networks** and record the selected **Network** that the tile is installed on.
- Based on the information you gathered, determine which of the following network layouts you have:

| Layout Name            | Layout Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| One Network            | <ul style="list-style-type: none"> <li>One network for Ops Manager and the BOSH Director, Pivotal Application Service (PAS), and services.</li> </ul> <div>  <b>Note:</b> You cannot secure your deployment with ASGs if you have this network layout. Because PCF dynamically allocates IPs, they cannot be easily excluded in the case of a single network.         </div> |
| Two Networks           | <ul style="list-style-type: none"> <li>One network for Ops Manager and the BOSH Director.</li> <li>One network for PAS and Services.</li> </ul>                                                                                                                                                                                                                                                                                                               |
| Three Networks         | <ul style="list-style-type: none"> <li>One network for Ops Manager and the BOSH Director.</li> <li>One network for PAS.</li> <li>One network for all services.</li> </ul>                                                                                                                                                                                                                                                                                     |
| Three or More Networks | <ul style="list-style-type: none"> <li>One network for Ops Manager and the BOSH Director.</li> <li>One network for PAS.</li> <li>One network for each service.</li> </ul>                                                                                                                                                                                                                                                                                     |

- If your network layout includes two or more networks, continue [Step 2: Ensure Access for PCF System Apps](#).

## Step 2: Ensure Access for PCF System Apps

Follow these steps to apply the default ASG to the `system` org. This provides network access to PCF system apps without restrictions, which enables them to continue functioning properly after you perform [Step 4: Remove the Deployment-wide Default ASG Binding](#).

- Bind the default ASG to the [staging set](#) in the `system` org:

```
$ cf bind-staging-security-group default_security_group
```

- Bind the default ASG to the [running set](#) in the `system` org:

```
$ cf bind-running-security-group default_security_group
```

## Step 3: Create New ASGs

Follow these steps to create ASGs that block apps from accessing PCF components and create any additional ASGs that allow apps to access the services they require.

### Part A: Record CIDRs

Gather the CIDRs for each network in your deployment:

- From the BOSH Director tile, click **Create Networks** within the **Settings** tab.
- In the **Networks** section, expand each network in your deployment by clicking its name.
- Record the **CIDR** for each network.

### Part B: Create and Bind ASGs that Block Network Access


Create ASGs that block apps from sending traffic to the networks that host Ops Manager, PAS, and, optionally, any installed services.

1. Create a `config.yml` containing the appropriate content for your network layout and replace the indicated values with the CIDRs you gathered:

- **Two Network Layout:**


```
exclude:
- YOUR-OPS-MANAGER-CIDR
- YOUR-PAS-AND-SERVICES-CIDR
```

- **Three Network Layout:**

 **Note:** If you want to secure only the Ops Manager and PAS components, you can remove the services CIDR from the `exclude` section.

```
exclude:
- YOUR-OPS-MANAGER-CIDR
- YOUR-PAS-CIDR
- YOUR-SERVICES-CIDR
```

- **Three or More Network Layout:**

 **Note:** If you want to secure only the Ops Manager and PAS components, you can remove the services CIDRs from the `exclude` section.

```
exclude:
- YOUR-OPS-MANAGER-CIDR
- YOUR-PAS-CIDR
- YOUR-SERVICE-CIDR-1
- YOUR-SERVICE-CIDR-2
etc...
```

2. Run the following command to generate the default `public-networks.json` and `private-networks.json` files that contain your ASG rules, specifying the location of the `config.yml` file as input:

```
$ asg-creator create --config config.yml
```

3. Create the `public-networks` ASG by running the following command:

```
$ cf create-security-group public-networks public-networks.json
```

4. Bind the ASG to the default staging set:

```
$ cf bind-staging-security-group public-networks
```

5. Bind the ASG to the default running set:

```
$ cf bind-running-security-group public-networks
```

6. Create the `private-networks` ASG by running the following command:


```
$ cf create-security-group private-networks private-networks.json
```


7. Bind the ASG to the default staging set:



```
$ cf bind-staging-security-group private-networks
```

8. Bind the ASG to the default running set:

```
$ cf bind-running-security-group private-networks
```

 **Note:** You can create and bind additional ASGs by following the procedures in [Create ASGs](#) and [Bind ASGs](#).

 **Note:** This part is only necessary if you blocked apps from a network that hosts services in the previous part. If you did not block apps from a network that hosts services, proceed to [Step 4: Remove the Default ASG](#).

 **warning:** In the two network layout, PAS and services share the same network. This means that each time you create an ASG that allows apps to access a new port and protocol within the network, you further expose the PAS component VMs. This is a limitation of a two network layout. For guidance on network topology, see [Reference Architectures](#) .

Now that you have created ASGs to secure the Ops Man, PAS, and service components, work with developers to create additional ASGs that give apps access to the services they need.

For more information about creating and binding ASGs, see the following:

- [Managing ASGs with the cf CLI](#)
- [Typical ASGs](#)

## Step 4: Remove the Default ASG

Now that you have bound new ASGs to determine outbound traffic rules, you no longer need the default ASG bindings that allow apps to send traffic to any IP address.

1. Unbind the default ASG from the staging set:

```
$ cf unbind-staging-security-group default_security_group
```

2. Unbind the default ASG from the running set:


```
$ cf unbind-running-security-group default_security_group
```


## Step 5: Restart your Apps

To apply the ASG changes, you must restart all of the apps in your deployment. To mitigate app downtime during the restart, Pivotal recommends a [blue-green](#) deployment strategy.

 **Notes:** You do not need to restart the apps in the `system` org.

1. Work with developers to restart a few of their apps individually and test that they still work correctly with the new ASGs in place. If an app does not work as expected, you likely must create another ASG that allows the app to send traffic to a service it requires.

 **Note:** To quickly roll back to the original overly-permissive state, you can re-bind the `default_security_group` ASG to the `default-staging` and `default-running` sets. You must then restart your apps to re-apply the original ASGs.


2. Restart the rest of the apps running on your deployment. Optionally, you can use the [app-restarter cf CLI plugin](#)  to restart all apps in a particular space, org, or deployment.



## Configuring Application Security Groups for Email Notifications

Page last updated:

To allow the Notifications Service to have network access you need to create [Application Security Groups](#) (ASGs).

 **Note:** Without Application Security Groups the service is not usable.


### Prerequisite

Review the [Getting Started with the Notifications Service](#) topic to ensure you have setup the service.

### Configure Network Connections

The Notifications Service is deployed as a suite of applications to the `notifications-with-ui` space in the `system` org, and requires the following outbound network connections:

| Destination                   | Ports            | Protocol         | Reason                                                                                                                                |
|-------------------------------|------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <code>SMTP_SERVER</code>      | 587<br>(default) | tcp<br>(default) | This service is used to send out email notifications                                                                                  |
| <code>LOAD_BALANCER_IP</code> | 80, 443          | tcp              | This service will access the load balancer                                                                                            |
| <code>ASSIGNED_NETWORK</code> | 3306             | tcp              | This service requires access to internal services. <code>ASSIGNED_NETWORK</code> is the CIDR of the network assigned to this service. |

 **Note:** The SMTP Server port and protocol are dependent on how you configure your server.

### Create a SMTP Server ASG


1. Navigate to the Ops Manager **Installation Dashboard** and click the **Pivotal Application Service** tile > **Settings** tab.
2. Record the information in the **Address of SMTP Server** and **Port of SMTP Server** fields.
3. Using the **Address of SMTP Server** information you obtained in the previous step, find the IP addresses and protocol of your SMTP Server from the service you are using. You might need to contact your service provider for this information.
4. Create a `smtp-server.json` file. For `destination`, you must enter the IP address of your SMTP Server.

```
[
 {
 "protocol": "tcp",
 "destination": SMTP_SERVER_IPS,
 "ports": "587"
 }
]
```

5. Create a security group called `smtp-server`:

```
cf create-security-group smtp-server smtp-server.json
```

### Create a Load Balancer ASG

 **Note:** If you already have a ASG setup for a Load Balancer, you do not need to perform this step. Review your [ASGs](#) to check which groups you have setup.

If you are using the built-in HAProxy as your load balancer, follow this procedure. If you are using an external load balancer, you must obtain your HAProxy IPs from the service you are using.

1. Record the **HAProxy** IPs in the **Pivotal Application Service** tile > **Settings** > **Networking** tab.
2. Create a `load-balancer-https.json` file. For `destination`, use the **HAProxy** IPs you recorded above.

```
[
 {
 "protocol": "tcp",
 "destination": "10.68.196.250",
 "ports": "80,443"
 }
]
```

3. Create a security group called `load-balancer-https`:

```
$ cf create-security-group load-balancer-https load-balancer-https.json
```

## Create an Assigned Network ASG

 **Note:** If you use external services, the IP addresses, ports, and protocols depend on the service.

1. Navigate to the Ops Manager **Installation Dashboard** > **Pivotal Application Service** tile > **Settings** > **Assign AZs and Networks** section.
2. Navigate to the network selected in the dropdown.
3. Record the **BOSH Director** tile > **Settings** tab > **Create Networks** > **CIDR** for the network identified in the previous step. Ensure the subnet mask allows the space to access `p-mysql`, `p-rabbitmq`, and `p-redis`.
4. Create a file `assigned-network.json`. For the `destination`, enter the **CIDR** you recorded above.

```
[
 {
 "protocol": "tcp",
 "destination": "10.68.0.0/20",
 "ports": "3306,5672,6379"
 }
]
```

5. Create a security group called `assigned-network`:

```
$ cf create-security-group assigned-network assigned-network.json
```

## Bind the ASGs

1. Target the `system` org:

```
$ cf target -o system
```

2. Create a `notifications-with-ui` space:

```
$ cf create-space notifications-with-ui
```

3. Bind the ASGs you created in this topic to the `notifications-with-ui` space:

```
$ cf bind-security-group smtp-server system notifications-with-ui
$ cf bind-security-group load-balancer-https system notifications-with-ui
$ cf bind-security-group assigned-network system notifications-with-ui
```



## Configuring SSH Access for PCF

Page last updated:

To help troubleshoot applications hosted by a deployment, [Pivotal Cloud Foundry \(PCF\)](#) [↗](#) supports SSH access into running applications. This document describes how to configure a PCF deployment to allow SSH access to application instances, and how to configure load balancing for those application SSH sessions.

### Pivotal Application Service Configuration

This section describes how to configure Pivotal Application Service (PAS) to enable or disable deployment-wide SSH access to application instances. In addition to this deployment-wide configuration, Space Managers have SSH access control over their Space, and Space Developers have SSH access control over their to their Applications. For details about SSH access permissions, see the [Application SSH Overview](#) topic.

To configure PAS SSH access for application instances:

1. Open the PAS tile in Ops Manager.
2. Under the **Settings** tab, select the **Application Containers** section.
3. Enable or disable the **Allow SSH access to app containers** checkbox.
4. Optionally, select **Enable SSH when an app is created** to enable SSH access for new apps by default in spaces that allow SSH. If you deselect this checkbox, developers can still enable SSH after pushing their apps by running `cf enable-ssh APP-NAME`.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

☒ Enable Custom Buildpacks

☒ Allow SSH access to app containers

☒ Enable SSH when an app is created

☒ Enable the GrootFS container image plugin for Garden RunC

☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888

Docker Images Disk-Cleanup Scheduling on Cell VMs\*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) ( min: 1 ) \*

10240

### SSH Load Balancer Configuration

For IaaSes where load-balancing is available as a service, you should provision a load balancer to balance load across SSH proxy instances. Configure this load balancer to forward incoming TCP traffic on port `2222` to a target pool where you deploy `diego_brain` instances.

For AWS, Azure, and GCP IaaSes, you configure SSH load balancers in the **Resource Config** pane. To register SSH proxies with a load balancer, enter your load balancer name in the **Load Balancers** field in the **Diego Brain** row.

Ops Manager supports an API-only `nsx_lbs` field. You can configure load balancers in vSphere using this field.

## Securing Services Instance Credentials with Runtime CredHub

This topic describes how Pivotal Cloud Foundry (PCF) operators can ensure service instance credentials are securely stored in CredHub.


- **What is runtime CredHub?**
  - The Pivotal Application Service (PAS) tile includes its own CredHub component, separate from the CredHub component included with the BOSH Director tile. For more information about this centralized credential management component, see the [CredHub](#) documentation.
- **What is runtime CredHub used for?**
  - Runtime CredHub exists to securely store service instance credentials. Previously, PCF could only use the Cloud Controller database for storing these credentials.
- **What are service instance credentials?**
  - When developers want their app to use a service, such as those provided by the Spring Cloud Services tile for PCF, they must bind their app to an instance of that service. Service bindings include credentials that developers can use to access the service from their app. For more information, see [Binding Credentials](#).
- **How can I ensure that service instance credentials are stored in runtime CredHub?**
  - You must configure PAS to enable this functionality by following the procedure below. Not all services support the use of runtime CredHub.
- **Can I use runtime CredHub to store service instance credentials if some of my services do not support the use of runtime CredHub?**
  - PAS supports both services that do and do not use runtime CredHub. Services that do not use runtime CredHub continue to pass their credentials to the Cloud Controller database.
- **Can I rotate service instance credentials in runtime CredHub?**
  - Runtime CredHub supports credential rotation. For more information, see [Rotating Runtime CredHub Encryption Keys](#).

## PCF Services that Use Secure Binding Credentials

The procedures in this document are only effective for services that support storing their instance credentials in runtime CredHub. To learn whether a service supports this feature, see the table below or the documentation for that service.

| Service                        | Versions with Secure Binding Credentials       | Pivotal Network Listing                        |
|--------------------------------|------------------------------------------------|------------------------------------------------|
| CredHub Service Broker for PCF | All                                            | <a href="#">CredHub Service Broker for PCF</a> |
| MySQL for PCF v2               | v2.3 and later (available to user groups only) | <a href="#">MySQL for PCF v2</a>               |
| Spring Cloud Services for PCF  | v1.5 and later                                 | <a href="#">Spring Cloud Services for PCF</a>  |
| RabbitMQ for PCF               | v1.12 and later                                | <a href="#">RabbitMQ for PCF</a>               |
| Redis for PCF                  | v1.13 and later                                | <a href="#">Redis for PCF</a>                  |

## Prerequisites

 **Breaking Change:** If you opt out of the [BOSH DNS feature](#), your PCF deployment cannot support Secure Service Instance Credentials.

Runtime CredHub allows you to use one or more Hardware Security Modules (HSMs) to store encryption keys. If you wish to use an HSM with CredHub, you must configure the HSM before completing the procedures below. For more information, see [Preparing CredHub HSMs for Configuration](#).

## Step 1: Configure the PAS Tile

To configure the PAS tile to support securing service instance credentials in CredHub, you need to:

- In the **CredHub** pane, provide at least one encryption key. CredHub supports multiple encryption key providers.
- In the **Resource Config** pane, set the number of **CredHub** instances to at least one.

CredHub configuration options include:


- Internal or external databases
- Encryption keys stored internally, externally in a Hardware Security Module (HSM), or both

To configure the PAS tile, follow the instructions in the PAS installation topic for your IaaS:

- [Deploying PAS on AWS](#)
- [Deploying PAS on AWS using Terraform](#)
- [Deploying PAS on Azure](#)
- [Deploying PAS on Azure using Terraform](#)
- [Deploying PAS on GCP](#)
- [Deploying PAS on GCP using Terraform](#)
- [Installing PAS after Deploying PCF on OpenStack](#)
- [Configuring PAS for vSphere](#)

## Step 2: Create Application Security Groups

Application Security Groups (ASGs) are network policy rules specifying protocols, ports, and IP ranges that apply to outbound network connections initiated from apps. You must follow the steps below to ensure the ASGs for your deployment allow apps to communicate with the runtime CredHub API.

 **Note:** The default ASGs in PCF allow apps running on your deployment to send traffic to almost any IP address. This step is only required if your ASGs restrict network access from apps to the network that PAS runs on, as documented in [Restricting App Access to Internal PCF Components](#).

1. From the PAS tile, click **Assign AZs and Networks** and record the selected Network where the tile is installed.
2. From the BOSH Director tile, within the **Settings** tab, click **Create Networks**.
3. In the **Networks** section, click the name of the PAS network to expand it.
4. Record the CIDR for the PAS network.
5. Create a file named `runtime-credhub.json` for specifying your ASG rules. Copy the content below into the file. Replace `YOUR-PAS-CIDR` with the CIDR you recorded in the previous step.

```
[
 {
 "protocol": "tcp",
 "destination": "YOUR-PAS-CIDR",
 "ports": "8844"
 }
]
```

6. Run the following command to create an ASG that allows apps to access the CredHub API:

```
$ cf create-security-group runtime-credhub ~/workspace/runtime-credhub runtime-credhub.json
```

7. Bind this ASG to your deployment or the specific space in which you want apps to access CredHub. For more information about binding ASGs, see [Bind ASGs](#). Ensure that apps deployed as part of the service tile installation process have access to CredHub in addition to the apps pushed to the platform by developers. For example, the Spring Cloud Services tile deploys the `spring-cloud-broker` app to the `p-spring-cloud-services` space of the `system` org.
8. Restart apps for the ASGs to take effect. Optionally, you can use the [app-restarter cf CLI plugin](#) to restart all apps in a particular space, org, or deployment.

## Step 3: Unbind and Rebind Service Instances

For any service instance bindings that existed before runtime CredHub was supported for that service, you must work with your developers to unbind and rebind the service instances to their apps. If you do not unbind and rebind the service, apps continue functioning as normal and fetching credentials from the Cloud Controller database.

 **Note:** This step is not required for bindings created after you installed the new version of the service tile that supports CredHub and you

completed the procedures in steps 1 and 2 of this topic.

1. Unbind the service instance from the app:

```
$ cf unbind-service YOUR-APP YOUR-SERVICE-INSTANCE
```

2. Rebind the service instance to the app:

```
$ cf bind-service YOUR-APP YOUR-SERVICE-INSTANCE
```

3. Review the `VCAP_SERVICES` environment variable to verify that the new service instance binding includes CredHub pointers:

```
$ cf env YOUR-APP
```

See the [VCAP\\_SERVICES](#) section of *Cloud Foundry Environment Variables* for help parsing the output of the `cf-env` command.

4. Restart the app to apply the service instance binding:

```
$ cf restart YOUR-APP
```

If you run `cf-env` again, you can see the `VCAP-SERVICES` environment variable now contains the credentials for the service instance binding.



## Identifying PAS Jobs Using vCenter

Page last updated:

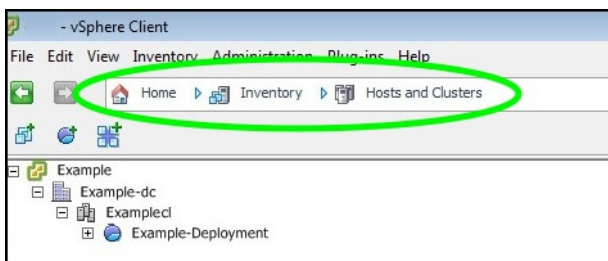
To effectively monitor, control, and manage the virtual machines making up your Pivotal Application Service (PAS) deployment, you may need to identify which VM corresponds to a particular job in PAS. You can find the CID of a particular VM from [Pivotal Cloud Foundry](#) (PCF) Operations Manager by navigating to PAS **Status**.

If you have deployed PAS to VMware vSphere, you can also identify which PAS job corresponds to which VM using the vCenter vSphere client.

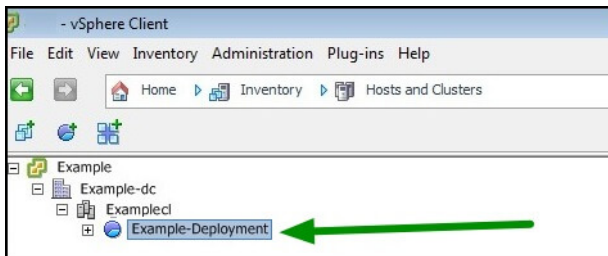
**Note:** The CID shown in Ops Manager is the name of the machine in vCenter.

## Identifying PAS Jobs Using vCenter

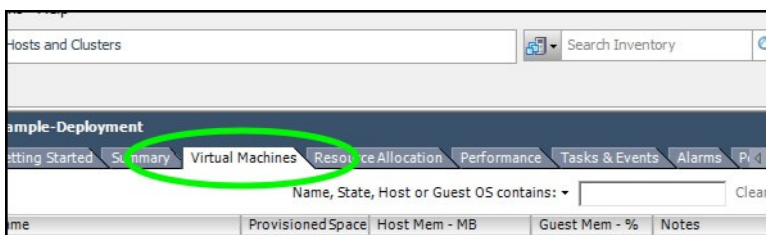
1. Launch the vSphere client and log in to the vCenter Server system.
2. Select the **Inventory > Hosts and Clusters** view.



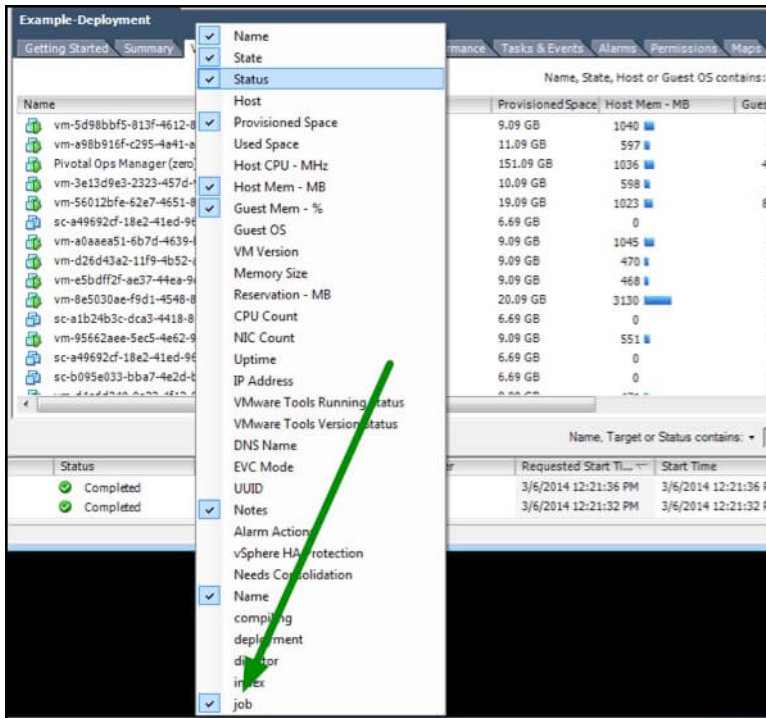
3. Select the Resource Pool containing your PAS deployment.



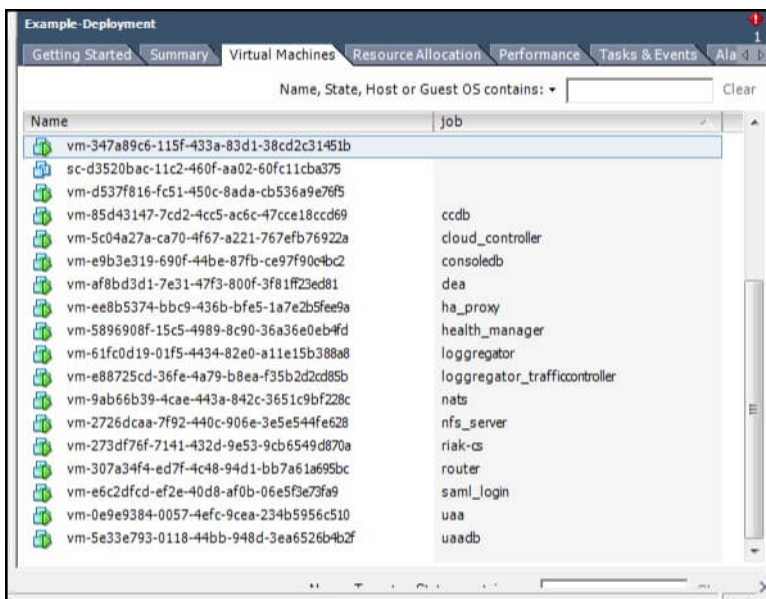
4. Select the **Virtual Machines** tab.



5. Right-click the column label heading and check **job**.



6. The job column displays the PAS job associated with each virtual machine.



## Configuring Logging in PAS

Page last updated:

This topic describes the types of logs that Pivotal Cloud Foundry (PCF) generates. It also explains how to forward system logs to an external aggregator service, how to scale [Loggregator](#) component VMs to keep up with app log volume, and how to manage app traffic logging.

### System Logs, App Logs, App Traffic Logs

Pivotal Cloud Foundry (PCF) generates two types of logs, *system logs* from PCF components and *app logs* from hosted apps, as differentiated in the table below:

| Log Type    | Originate from      | Follow format                                  | Stream from           | Can to stream out to (configurable)            | Visible to               |
|-------------|---------------------|------------------------------------------------|-----------------------|------------------------------------------------|--------------------------|
| System Logs | Platform components | Syslog standard                                | rsyslog agent         | Component syslog drain                         | Operators                |
| App Logs    | Hosted apps         | Format is up to the developer                  | Firehose <sup>1</sup> | External data platform, optionally via nozzles | Developers and Operators |
|             |                     | (Optional) With <a href="#">Syslog Adapter</a> |                       |                                                |                          |
|             |                     | Converted to syslog standard                   | Syslog Adapter        | External syslog drain                          |                          |

<sup>1</sup>The Loggregator Firehose also streams component metrics.

**App traffic logs are system logs.** When app containers communicate, or attempt to communicate, their host cells generate *app traffic logs*. App traffic logs are system logs, not app logs. These logs come from host cells, not apps, and they carry no information from within the app. App traffic logs only show app communication behavior, as detected from outside by the host cell.

### Enable Log Cache

Log Cache is a Loggregator feature that lets you filter and query app logs through a CLI plugin or API endpoints. Cached app logs are available on demand; you do not need to stream them continuously.

 **Breaking Change:** App Autoscaler is dependent on Log Cache. When you disable Log Cache, App Autoscaler fails.

### Log Cache in PAS

To begin generating queryable app logs, you must enable Log Cache in the PAS tile.

Cell Memory Capacity (MB) ( min: 1 )

Cell Disk Capacity (MB) ( min: 1 )

Whitelist for non-RFC-1918 Private Networks \*

CF CLI Connection Timeout

☒ Enable log-cache

Save

To enable Log Cache, do the following:

1. From the Pivotal Application Service (PAS) tile, select **Advanced Features**.
2. Select the **Enable Log Cache** checkbox.
3. Click **Save**.

After you have enabled Log Cache, use the CLI plugin or API to query and filter app logs.

## Example uses of the Log Cache CLI Plugin

To access cached logs with the Log Cache CLI plugin, you must first download and install the plugin.

[Download the Log Cache CLI plugin](#).

Once you have installed the plugin, the basic command to access cached app logs is:

```
$ cf tail [OPTIONS] [SOURCE ID/APP]
```

Here are some ways you can use Log Cache to filter app logs:

- `--start-time` : Displays the start of the cache or the start of a time period you specify. Results display as a UNIX timestamp, in nanoseconds. Pair with `--end-time` to view logs within a time period.
- `--end-time` : Displays the end of the cache or the end of a time period you specify. Results display as a UNIX timestamp, in nanoseconds. Pair with `--start-time` to view logs within a time period.
- `--json` : Output logs in JSON.
- `--follow` : Append exported logs to `stdout`.

For more information on using the Log Cache CLI, see [Log Cache CLI: Usage](#).

## Example uses of the Log Cache API

The Log Cache API is hosted on PCF, and references your system domain to return responses. The root URL for API calls is

```
https://log-cache.[YOUR-SYSTEM-DOMAIN]
```

The basic call to access and filter cached app logs is:

```
GET https://log-cache.[YOUR-SYSTEM-DOMAIN]/v1/read/[SOURCE-ID]
```


Append the following parameters to the `GET` to customize app logs:

- `start_time` : Displays the start of the cache or the start of a time period you specify. Results display as a UNIX timestamp, in nanoseconds. Pair with `end_time` to view logs within a time period.
- `end_time` : Displays the end of the cache or the end of a time period you specify. Results display as a UNIX timestamp, in nanoseconds. Pair with `start_time` to view logs within a time period.
- `envelope_types` : Filters by Envelope Type. The available filters are: `LOG` , `COUNTER` , `GAUGE` , `TIMER` , and `EVENT` . Set an envelope type filter to emit logs of only that type. Specify this parameter multiple times to include more types.
- `limit` : Sets a maximum number of envelopes to request. The max limit is 1000. This value defaults to 100.

More API parameters are available to customize retrieved app logs. For more information, see [Log Cache: RESTful API Gateway](#) [↗](#).

## Enable Syslog Forwarding

You can configure system logging in PAS to forward log messages from PAS component VMs to an external service. Pivotal recommends forwarding logs to an external service for use in troubleshooting.

 **Note:** The following instructions explain how to configure system logging for PAS component VMs. To forward logs from PCF tiles to an external service, you must also configure system logging in each tile. See the documentation for the given tiles for information about configuring system logging.

To configure system logging in PAS, do the following:

1. In the PAS **Settings** tab, select the **System Logging** pane. The following image shows the **System Logging** pane.

Optionally configure rsyslog to forward platform component logs to an external service. If you do not fill these fields, platform logs will not be forwarded but will remain available on the component VMs and for download via Ops Manager.

Address

Port

Transport Protocol

Encrypt syslog using TLS?\*

- ☒ No  
☐ Yes

Syslog Drain Buffer Size (# of messages) \*

☒ Include container metrics in SysLog Drains

☒ Enable Cloud Controller security event logging


☐ Use TCP for file forwarding local transport

☒ Don't Forward Debug Logs

Custom rsyslog Configuration


Save

2. For **Address**, enter the IP address of the syslog server.
3. For **Port**, enter the port of the syslog server. The default port for a syslog server is `514`.

 **Note:** The host must be reachable from the PAS network and accept UDP or TCP connections. Ensure the syslog server listens on external interfaces.

4. For **Transport Protocol**, select a transport protocol for log forwarding.
5. For **Encrypt syslog using TLS?**, select **Yes** to use TLS encryption when forwarding logs to a remote server.
  - a. For **Permitted Peer**, enter either the name or SHA1 fingerprint of the remote peer.
  - b. For **TLS CA Certificate**, enter the TLS CA certificate for the remote server.
6. For **Syslog Drain Buffer Size**, enter the number of messages from the Loggregator Agent that the Doppler server can store before it begins to drop messages. See the [Loggregator Guide for Cloud Foundry Operators](#) topic for more details.
7. Disable the **Include container metrics in Syslog Drains** checkbox to prevent the [CF Drain CLI plugin](#) from including app container metrics in syslog drains. This feature is enabled by default.

8. Enable the **Enable Cloud Controller security event logging** checkbox to include security events in the log stream. This feature logs all API requests, including the endpoint, user, source IP address, and request result, in the Common Event Format (CEF).
9. Enable the **Use TCP for file forwarding local transport** checkbox to transmit logs over TCP. This prevents log truncation, but may cause performance issues.
10. Disable the **Don't Forward Debug Logs** checkbox to forward DEBUG syslog messages to an external service. This checkbox is enabled by default.

 **Note:** Some PAS components generate a high volume of DEBUG syslog messages. Enabling the **Don't Forward Debug Logs** checkbox prevents PAS components from forwarding the DEBUG syslog messages to external services. However, PAS still writes the messages to the local disk.

11. For **Custom rsyslog Configuration**, enter a custom syslog rule. For more information about adding custom syslog rules, see [Customizing Syslog Rules](#).
12. Click **Save**.

To configure Ops Manager for system logging, see the [Settings](#) section in the *Using the Ops Manager Interface* topic.

## Include Container Metrics in Syslog Drains

Developers can monitor container metrics over the syslog protocol using the [CF Drain CLI plugin](#). With the CF Drain CLI plugin, you can use the Cloud Foundry Command Line Interface (cf CLI) tool to set the app container to deliver container metrics to a syslog drain. Developers can then monitor the app container based on those metrics.

In PAS, the **Include container metrics in Syslog Drains** checkbox is enabled by default in the **System Logging** pane. If you have security concerns about streaming container metrics from your app, you can disable this checkbox.

For more information, see [Including Container Metrics in Syslog Drains](#) in *Application Logging in Cloud Foundry*.

## Scale Loggregator


Apps constantly generate app logs and PCF platform components constantly generate component metrics. The Loggregator system combines these data streams and handles them as follows. See [Overview of the Loggregator System](#) for more information.


- The [Metron](#) agent running on each component or application VM collects and sends this data out to Doppler components.
- [Doppler](#) components temporarily buffer the data before periodically forwarding it to the Traffic Controller. When the log and metrics data input to a Doppler exceeds its buffer size for a given interval, data can be lost.
- The [Traffic Controller](#) serves the aggregated data stream through the Firehose WebSocket endpoint.

Follow the instructions below to scale the Loggregator system. For guidance on monitoring and capacity planning, see [Monitoring Pivotal Cloud Foundry](#).

## Add Component VM Instances

1. From the PAS tile, select **Resource Config**.
2. Increase the number in the **Instances** column of the component you want to scale. You can add instances for the following Loggregator components:
  - **Loggregator Traffic Controller**

 **Note:** The [Reverse Log Proxy \(RLP\)](#) BOSH job is colocated on the Traffic Controller VM. If you want to scale Loggregator to handle more logs for syslog drains, you can add instances of the Traffic Controller.

 **Note:** The [BOSH System Metrics Forwarder](#) job is colocated on the Traffic Controller VM. If you want to scale Loggregator to handle more BOSH component metrics, you can add instances of the Traffic Controller.

- **Syslog Adapter**
- **Doppler Server**

|                               |              |      |                                                  |                                     |
|-------------------------------|--------------|------|--------------------------------------------------|-------------------------------------|
| Loggregator Trafficcontroller | Automatic: 3 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 1 GB) | <input checked="" type="checkbox"/> |
| Syslog Adapter                | Automatic: 3 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 1 GB) | <input checked="" type="checkbox"/> |
| Syslog Scheduler              | Automatic: 1 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 1 GB) | <input checked="" type="checkbox"/> |
| Doppler Server                | Automatic: 3 | None | Automatic: micro (cpu: 1, ram: 1 GB, disk: 1 GB) | <input checked="" type="checkbox"/> |

3. Click **Save**.
4. Click **Apply Changes**.

## App Traffic Logging

App traffic logging generates logs when app containers communicate with each other directly, or attempt to communicate, as allowed by [container-to-container networking \(C2C\) policies](#) and [Application Security Groups \(ASGs\)](#).

App traffic logging lets network security teams audit C2C traffic, by seeing allowed and denied packets, without needing access to the Cloud Controller or the apps themselves.

### Enable App Traffic Logging

To enable app traffic logging, do the following:

1. From Ops Manager, navigate to the **Pivotal Application Service** tile > **Networking** pane.
2. Under **Log traffic for all accepted/denied application packets**, select **Enable (will increase log volume)** or **Disable** to enable or disable app traffic logging.

Log traffic for all accepted/denied application packets. \*

☒ Enable (will increase log volume)

Denied logging interval (packets/second) \*

UDP logging interval (packets/second) \*

☐ Disable

### App Logging Behavior

App traffic logging generates log messages as follows:

- **TCP traffic** - Logs the first packet of every new TCP connection.
- **UDP traffic** - Logs UDP packets sent and received, up to a maximum per-second rate for each container. Set this rate limit in the **UDP logging interval** field (default: 100).
- **Packets denied** - Logs packets blocked by either a container-specific [networking policy](#) or by [Application Security Group](#) (ASG) rules applied across the space, org, or deployment. Logs packet denials up to a maximum per-second rate for each container, set in the **Denied logging interval** field (default: 1).

### App Traffic Log Format and Contents

App traffic logs are formatted as described in the [cf-networking-release Traffic logging](#) [documentation](#), following the `iptables-logger` format but without line breaks. For example, the first part of an app traffic log line looks like:



```
{ "timestamp": "1500924070.182554722", "source": "cfnetworking.iptables", "message": "cfnetworking.iptables.ingress-allowed", "log_level": 1, "data": { "destination": { "container_id": "d5978989-1401-49ff-46cd-33e5", "app_guid": "bc6f229d-5e4a-4c41-a63f-e8795496c283",
```

Each log message includes the following:

- Timestamp
- The GUID for the source or destination app that sent or was designated to receive the packet
- The protocol of the communication, `TCP` or `UDP`
- GUIDs for the container, space, and org running the source or destination app
- IP addresses and ports for both source and destination apps
- A `message` field recording whether the packet was allowed or denied, with one of the following four possibilities:
  - ASG allowed packet to exit source app container
  - C2C policy allowed packet to enter destination app container
  - ASG prevented packet from exiting source app container
  - C2C policy prevented packet from entering destination app container
- Additional information described in the [cf-networking-release](#).

## Denied Packet Causes

You can determine whether a denied-packet log resulted from a container networking policy or an ASG rule as follows:

- **Container networking policy:** Log `message` string includes `ingress-denied` and `packet direction` is `ingress`.
- **ASG rule:** Log `message` string includes `egress-denied` and `packet direction` is `egress`.

## Global vs. ASG-Level App Traffic Logging

PCF supports two mechanisms for enabling app traffic logging. [Setting Log traffic](#) to **Enable** in Ops Manager enables app traffic logging globally for all ASGs and container policies. Setting the `log` property of an ASG to `true` enables app traffic logging at the individual ASG level.

Because these two mechanisms operate independently, PCF generates duplicate logs when app traffic logging is enabled globally and an ASG's `log` property is set to `true`. To avoid duplicate logs, Pivotal recommends setting the `log` property to `false` for all ASGs, or leaving it out entirely, when app traffic logging is [enabled globally](#).

To focus on specific ASGs for log analysis, Pivotal recommends enabling app traffic logs globally and using a logging platform to filter traffic logs by ASG, rather than setting `log` at the individual ASG level.

## Configuring UAA Password Policy

Page last updated:

If your Pivotal Cloud Foundry (PCF) deployment uses the internal user store for authentication, you can configure its password policy within the Pivotal Application Service (PAS) tile.

### Open the Internal UAA Configuration

1. In a browser, navigate to the fully qualified domain name (FQDN) of your Ops Manager and log in.
2. Click the **Pivotal Application Service** tile.
3. Select **Authentication and Enterprise SSO** on the **Settings** tab.

Configure your user store access, which can be an internal user store (managed by Cloud Foundry's UAA) or an external user store (LDAP or SAML). You can also adjust the lifetimes of authentication tokens.

Configure your UAA user account store with either internal or external authentication mechanisms\*

☒ Internal UAA (provided by Elastic Runtime; configure your password policy below)

Minimum Password Length \*

0

Minimum Uppercase Characters Required for Password \*

0

Minimum Lowercase Characters Required for Password \*

0

Minimum Numerical Digits Required for Password \*

0

Minimum Special Characters Required for Password \*

0

Maximum Password Entry Attempts Allowed \*

5

4. Confirm that the **Internal UAA** option is selected.

### Set Password Requirements and Entry Attempts

1. For **Minimum Password Length**, enter the minimum number of characters for a valid password.
2. For **Minimum Uppercase Characters Required for Password**, enter the minimum number of uppercase characters required for a valid password.
3. For **Minimum Lowercase Characters Required for Password**, enter the minimum number of lowercase characters required for a valid password.
4. For **Minimum Numerical Digits Required for Password**, enter the minimum number of digits required for a valid password.
5. For **Minimum Special Characters Required for Password**, enter the minimum number of special characters required for a valid password.

6. For **Maximum Password Entry Attempts Allowed**, enter the maximum number of failures allowed to enter a password within a five-minute timespan before the account is locked.

## Managing Internal MySQL for PAS

This topic is a reference for the concepts and procedures related to internal MySQL for Pivotal Application Service (PAS).


See the following topics:

- [Scaling Internal MySQL for PAS](#)
- [Migrating to Internal Percona MySQL](#)
- [Running mysql-diag](#)
- [Recovering From MySQL Cluster Downtime](#)
- [Using the MySQL Proxy](#) [↗](#)
- [MySQL Network Communications](#)

## Scaling Internal MySQL for PAS


This topic describes two procedures for managing the internal MySQL databases used by Pivotal Application Service (PAS) system components: scaling down your MySQL cluster, and migrating the cluster to a database stack that uses TLS encryption. It also provides example sizing data from two environments that have significant load on their MySQL clusters.

For additional resources about scaling Internal MySQL, see the following documentation:

- *Deployments Using Internal MySQL* section of [Scaling PAS](#)
- *Scalable Components* section of [High Availability in Cloud Foundry](#) 



**Note:** The procedures do not apply to databases configured as external in the PAS tile **Databases** pane.

PAS components that use system databases include the Cloud Controller, Diego brain, Gorouter, and the User Authorization and Authentication (UAA) server. See [Cloud Foundry Components](#) .

## Scale Down Your MySQL Cluster

This procedure explains how to safely scale your MySQL cluster down to a single node. If you are already running the MySQL cluster with a single node, you do not need to perform these steps.

By default, internal MySQL deploys as a single node. To take advantage of the high availability features of MySQL, you may have scaled the configuration up to three or more server nodes.

### Check the Health of Your Cluster

Before scaling down your MySQL cluster, perform the following actions to ensure the cluster is healthy.

1. Use the Cloud Foundry Command Line Interface (cf CLI) to target the API endpoint of your Pivotal Cloud Foundry (PCF) deployment:

```
$ cf api api.YOUR-SYSTEM-DOMAIN
Setting api endpoint to api.YOUR-SYSTEM-DOMAIN...
OK

API endpoint: https://api.YOUR-SYSTEM-DOMAIN... (API version: 2.54.0)
Not logged in. Use 'cf login' to log in.
```

2. Log in with your User Account and Authentication (UAA) Administrator user credentials. Obtain these credentials by clicking the **Credentials** tab of the Pivotal Application Service (PAS) tile, locating the **Admin Credentials** entry in the **UAA** section, and clicking **Link to Credential**.

```
$ cf login -u admin
API endpoint: https://api.YOUR-SYSTEM-DOMAIN

Password>
Authenticating...
OK
```

3. Create a test organization to verify the database across all nodes:

```
$ cf create-org data-integrity-test-organization
Creating org data-integrity-test-organization as admin...
OK

Assigning role OrgManager to user admin in org data-integrity-test-organization ...
OK

TIP: Use 'cf target -o data-integrity-test-organization' to target new org
```

4. Obtain the IP addresses of your MySQL server:
  - a. From the PCF **Installation Dashboard**, click the **Pivotal Application Service** tile.

- b. Click the **Status** tab.
- c. Record the IP addresses for all instances of the **MySQL Server** job.

5. Retrieve Cloud Controller database credentials from CredHub using the Ops Manager API:

- a. Perform the procedures in the [Using the Ops Manager API](#) topic to authenticate and access the Ops Manager API.
- b. Use the `GET /api/v0/deployed/products` endpoint to retrieve a list of deployed products, replacing `UAA-ACCESS-TOKEN` with the access token recorded in the previous step:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

- c. In the response to the above request, locate the product with an `installation_name` starting with `cf-` and copy its `guid`.
- d. Run the following `curl` command, replacing `PRODUCT-GUID` with the value of `guid` from the previous step:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products/PRODUCT-GUID/variables?name=cc-db-credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

- e. Record the Cloud Controller database `username` and `password` from the response to the above request.
6. SSH into the Ops Manager VM. Because the procedures vary by IaaS, review the [SSH into Ops Manager](#) section of the Advanced Troubleshooting with the BOSH CLI topic for specific instructions.
7. For each of the MySQL server IP addresses recorded above, perform the following steps from the Ops Manager VM:
- a. Query the new organization with the following command, replacing `YOUR-IP` with the IP address of the MySQL server and `YOUR-IDENTITY` with the `identity` value of the CCDB credentials obtained above:

```
$ mysql -h YOUR-IP -u YOUR-IDENTITY -D ccdb -p -e "select created_at, name from organizations where name = 'data-integrity-test-organization'"
```

- b. When prompted, provide the `password` value of the CCDB credentials obtained above.
- c. Examine the output of the `mysql` command and verify the `created_at` date is recent.

```
+-----+-----+
| created_at | name |
+-----+-----+
| 2016-05-28 01:11:42 | data-integrity-test-organization |
+-----+-----+
```

8. If each MySQL server instance does not return the same `created_at` result, contact [Pivotal Support](#) before proceeding further or making any changes to your deployment. If each MySQL server instance does return the same result, then you can safely proceed to scaling down your cluster to a single node by performing the steps in the following section.

## Set Server Instance Count to 1

1. From the PCF **Installation Dashboard**, click the **Pivotal Application Service** tile.
2. Select **Resource Config**.
3. Use the drop-down menu to change the **Instances** count for **MySQL Server** to `1`.
4. Click **Save** and **Apply Changes** to apply the changes.
5. Delete your test organization with the following cf CLI command:

```
$ cf delete-org data-integrity-test-organization
```

## Migrating to Internal Percona MySQL

In PAS v2.1 and earlier, internal system MySQL databases ran [MariaDB](#) with cluster nodes communicating over plaintext. PAS v2.2 offers a second option for internal databases: a [Percona Server](#) that uses TLS to encrypt communication between server cluster nodes.

For more information on migrating PAS internal MySQL databases from the less secure MariaDB infrastructure to a TLS-encrypted Percona stack, see


## MySQL Cluster Sizing Examples

This topic describes two sizing examples for internal MySQL in Pivotal App Service (PAS).

Use this data as guidance to ensure your MySQL Clusters are scaled to handle the number of app instances running on your deployment.

### Example 1: Pivotal Web Services Production Environment

The data in this section comes from the Pivotal-managed Cloud Foundry deployment, Pivotal Web Services (PWS).

 **Note:** This deployment differs from most PCF deployments in that the MySQL database is used for Diego, but not the Cloud Controller. This means that while there are a large number of queries per second, most of them are reading data, and the number of writes is not realistically reflected.

- **IAAS:** AWS
- **App Instances:** ~23,000
- **Average SQL Queries Per Minute:** ~308,000
- **Average IOPS:** 220
- **Storage Volume Usage:** 80%

#### VM Sizing

The following table displays MySQL VM settings for this environment.

| Setting             | Value      |
|---------------------|------------|
| VM Type             | c4.2xlarge |
| Storage Volume Type | io1        |
| Storage Volume Size | 98GB       |
| Storage Volume IOPS | 2000       |

### Example 2: Cloud Foundry Diego Test Environment

The data in this section comes from an environment used by the Cloud Foundry Diego team to test the MySQL cluster with a high load similar to one generated large deployment.

- **IAAS:** GCP
- **App Instances:** 250,000
- **Average SQL Queries Per Minute:** ~5,100,000
- **Average IOPS:**
  - **Reads:** 3.63
  - **Writes:** 363.98

#### VM Sizing

The following table displays MySQL VM settings for this environment.

| Setting             | Value          |
|---------------------|----------------|
| VM Type             | n1-standard-16 |
| Storage Volume Type | pd-ssd         |
| Storage Volume Size | 1TB            |





## Migrating to Internal Percona MySQL

This topic describes the procedure for migrating Pivotal Application Service (PAS) internal MySQL databases from the less secure MariaDB infrastructure to a TLS-encrypted Percona stack.

In PAS v2.1 and earlier, internal system MySQL databases ran [MariaDB](#) with cluster nodes communicating over plaintext. PAS v2.2 offers a second option for internal databases: a [Percona Server](#) that uses TLS to encrypt communication between server cluster nodes.

**⚠ warning:** This procedure causes temporary downtime of PAS system functions, as described in [Effects of MySQL Downtime](#) and [MySQL Migration Downtime](#). It does not interrupt apps hosted by PAS, unless they use TCP routing. Applications using TCP routes will not be routable during the migration.

## Effects of MySQL Downtime

During internal MySQL server downtime, the Cloud Controller and other platform components that use system databases become unavailable. This prevents users from pushing apps, scaling apps, and running other cf CLI commands.

If the PAS UAA is configured to use an internal database, then the UAA also becomes unavailable. This outage temporarily prevents users from signing into PAS orgs and spaces, Apps Manager, and other PAS interfaces.

PAS UAA downtime caused by internal MySQL migration also temporarily prevents users from logging into any PAS apps that use the [Single Sign-On \(SSO\)](#) service.

## Procedure

To migrate your internal MySQL databases from MariaDB to Percona, do the following:

1. Run `mysql-diag` to check the state of your MySQL cluster and determine whether it is safe to migrate. For more information, see [Running mysql-diag](#).
2. If your internal databases MySQL cluster runs three or more nodes, scale it down horizontally to a single node before you migrate. In the PAS tile > **Resource Config** > **MySQL Server** settings, set **Instances** to `1`. Click **Save**.

**💡 Note:** Do not click **Review Pending Changes** and **Apply Changes** yet.

3. Migrating the database can demand up to 3 times the normal disk space on the MySQL server. To ensure that the single remaining MySQL server node currently uses at most `30%` of its persistent disk, do the following:
  - a. Check the persistent disk usage of the MySQL Server job in the **Status** tab of the PAS tile.
  - b. If the MySQL Server job disk usage exceeds 30%, scale it up vertically by increasing its persistent disk.
4. In the PAS tile > **Databases** pane, under **Choose the location of your system databases**, select **Internal Databases - MySQL - Percona XtraDB Cluster**. Click **Save**.

Choose the location of your system databases. Please consult the documentation for migrating existing installations from MariaDB to Percona. \*

- ☒ Internal Databases - MySQL - Percona XtraDB Cluster
- ☐ Internal Databases - MySQL - MariaDB Galera Cluster (deprecated - planned to be removed in PAS 2.4)
- ☐ External Databases - (e.g. AWS RDS)

Save

5. Return to the **Installation Dashboard**, click **Review Pending Changes**, and click **Apply Changes** to re-deploy PAS with the new internal database. Consider the following when performing this step:
  - You do not need to run any errands for this step.
  - Internal system databases become temporarily unavailable to PAS components during this migration step, but PAS apps continue to run. See [MySQL Migration Downtime](#) for details.

- You can see that the change is being applied when you see this in Ops Manager's output after clicking **Apply Changes**:

```
instance_groups:
 name: database
 jobs:
 name: pxc-mysql
 properties:
 pxc_enabled: "PXC-CLUSTER-NAME"
 pxc_enabled: "PXC-CLUSTER-NAME"
 name: mysql
 properties:
 cf_mysql_enabled: "CF-MYSQL-CLUSTER-NAME"
 cf_mysql_enabled: "CF-MYSQL-CLUSTER-NAME"
```


- You can measure the disk space used in the `/var/vcap/store/pxc-mysql` directory as the migration is running by SSHing into the database node and running the following command: `watch -n 5 du -sh /var/vcap/store/pxc-mysql`. As the migration is running, disk usage increases:

```
2.9G pxc-mysql
```

For more information on SSH, see [Accessing Apps with SSH](#).

6. In the `/var/vcap/sys/log/pxc-mysql` directory, open `galera-init.log` to see that Percona has started normally:

```
{"timestamp":"1555115911.754334211","source":"/var/vcap/packages/galera-init/bin/galera-init","message":"/var/vcap/packages/galera-init/bin/galera-init
started","log_level":1,"data":{}} {"timestamp":"1555115911.754334211","source":"/var/vcap/packages/galera-init/bin/galera-init","message":"/var/vcap/packages/galera-init/bin/galera-
init.galera-init started","log_level":1,"data":{}}
```

 **Note:** The file `/var/vcap/store/migrated-successfully` is created upon successful migration. Do not delete this file.

Additionally, running `monit` shows that the `mariadb_ctrl` job has been replaced by `galera-init` and the `galera-healthcheck` job has been replaced by `galera-agent`.

7. If you want to scale the database cluster back up to multiple server nodes, increase the instance count under **Resource Config > MySQL Server**. Then click **Save** to save the change and **Review Pending Changes** and **Apply Changes** in the Installation Dashboard to re-deploy.
8. Run `mysql-diag` again to check the status of your new Percona cluster.

## MySQL Migration Downtime

Upgrading existing internal system databases to the new option of **Internal Databases - MySQL - Percona XtraDB Cluster** causes temporary downtime of PAS system functions. It does not interrupt apps hosted by PAS.

The length of downtime depends on multiple factors, including database size, persistent disk type, CPU and disk capacity of VMs, and PAS configuration. There are two downtime events:

- **When you scale down and migrate the database:** During the migration, PAS updates the single node and migrates the data.
- **When you scale back up:** PAS updates the first node to make it part of a three-node cluster.

During migration, BOSH orphans the two disks used by the scaled-down nodes. This does not increase the risk of losing data written before the migration, and these orphaned disks can act as a backup, should the migration fail. If the migration fails, contact [Pivotal Support](#).

## Migration Length

To estimate how long a database migration takes, perform a manual backup without saving the backup file.

To perform a manual backup, run the following command:

```
time /var/vcap/packages/mariadb/bin/mysqldump --defaults-file=/var/vcap/jobs/mysql/config/mylogin.cnf --all-databases > /dev/null
```

BOSH runs additional processes before and after a MySQL migration, but the total time the migration takes is not much longer than the manual backup.

## Delete MariaDB Migration Artifact

When you migrate your database from MariaDB to Percona, Percona preserves a backup of the MariaDB database as a migration artifact, so you can return


to using the MariaDB database if something goes wrong during migration. Upon successful migration, the migration artifact is no longer needed and only takes up disk space.

To delete the MariaDB migration artifact, do the following:

1. In the `/var/vcap/sys/log/pxc-mysql` directory, open `galera-init.log` to ensure that Percona has started normally:  


```
{ "timestamp": "1555115911.754334211", "source": "/var/vcap/packages/galera-init/bin/galera-init", "message": "/var/vcap/packages/galera-init/bin/galera-init started", "log_level": 1, "data": {} } { "timestamp": "1555115911.754334211", "source": "/var/vcap/packages/galera-init/bin/galera-init", "message": "/var/vcap/packages/galera-init/bin/galera-init galera-init started", "log_level": 1, "data": {} }
```

 You can see that the `/var/vcap/store/migrated-successfully` file is present in that directory.
2. Delete the migration artifact in `/var/vcap/store/mysql-migration-backup`.

 **Note:** Do not delete the new copy of the data in `/var/vcap/sys/log/pxc-mysql`.

## Recover MariaDB Data After Migration Failure

If the migration to Percona fails, you can recover your MariaDB data.

 **Note:** You may still lose some of your MariaDB data if Percona has already started and served any traffic.

To recover your MariaDB data, do the following:

1. Ensure that the `/var/vcap/store/mysql-migration-backup` backup artifact is on the `mysql/0` indexed node. If not, you may lose data, because the backup artifact is only stored on one node. If the backup artifact is on a different node, copy it to the `mysql/0` node.
2. Scale your database cluster down to one node.
3. Move `/var/vcap/store/mysql-migration-backup` back to `/var/vcap/store/mysql` by running the following command: `mv /var/vcap/store/mysql-migration-backup /var/vcap/store/mysql`
4. If it exists, delete the `/var/vcap/store/migrated-successfully` file.
5. In the PAS tile > **Databases** pane, under **Choose the location of your system databases**, select **Internal Databases - MySQL - MariaDB Galera Cluster**. Click **Save**.
6. Return to the **Installation Dashboard**, click **Review Pending Changes**, and click **Apply Changes**.

## Running mysql-diag

This topic discusses how to use the `mysql-diag` tool in MySQL for Pivotal Cloud Foundry (PCF). `mysql-diag` prints the state of your MySQL highly available (HA) cluster and suggests solutions if your node fails. Pivotal recommends running this tool against your HA cluster before all deployments.

`mysql-diag` checks the following information about the status of your HA cluster:

- Membership status of all nodes
- Size as it appears to all nodes
- If it needs to be bootstrapped
- If replication is working
- Used disk space and inodes per server

## Run mysql-diag Using the BOSH Command Line Interface (CLI)

To use the BOSH CLI to run `mysql-diag`, do the following:

1. Obtain the information needed to use the BOSH CLI by doing the procedure in [Gather Credential and IP Address Information](#).
2. SSH into your Ops Manager VM by doing the procedure in [Log in to the Ops Manager VM with SSH](#) for your IaaS.
3. Log in to your BOSH Director by doing the procedure in [Log in to the BOSH Director](#).
4. Identify the VM to log in to with SSH by running the following command:

```
bosh -e MY-ENV -d MY-DEPLOYMENT vms
```

Where:

- `MY-ENV` is the name of your environment.
- `MY-DEPLOYMENT` is the name of your deployment.

5. Record the GUID associated with the `mysql-monitor` VM, also known as the jumpbox VM.
6. SSH into your `mysql-monitor` VM by running the following command:

```
bosh -e MY-ENV -d MY-DEP ssh mysql-monitor/GUID
```

Where:

- `MY-ENV` is the name of your environment.
- `MY-DEPLOYMENT` is the name of your deployment.
- `GUID` is the GUID you recorded in the previous step.

7. View the status of your HA cluster by running the following command:

```
mysql-diag
```

## Example Healthy Output

The `mysql-diag` command returns the following message if your canary status is healthy:

```
Checking canary status...healthy
```

Here is a sample `mysql-diag` output after the tool identified a healthy HA cluster:

```
mysql-monitor/5faae86a-a325-44fa-a8ab-24e736e42390:~$ mysql-diag
Wed Jul 19 19:03:54 UTC 2017
Checking canary status...
Checking canary status... healthy
Checking cluster status of mysql/fe6cd1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2...
Checking cluster status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2...
Checking cluster status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2...
Checking cluster status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2... done
Checking cluster status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2... done
Checking cluster status of mysql/fe6cd1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2... done
+-----+-----+-----+-----+-----+-----+-----+
| HOST | NAME/UUID | WSREP LOCAL STATE | WSREP CLUSTER STATUS | WSREP CLUSTER SIZE |
+-----+-----+-----+-----+-----+-----+
| 10.244.7.2 | mysql/32665833 | Synced | Primary | 3 |
| 10.244.8.2 | mysql/026d5b79 | Synced | Primary | 3 |
| 10.244.9.2 | mysql/fe6cd1e | Synced | Primary | 3 |
+-----+-----+-----+-----+-----+-----+
I don't think bootstrap is necessary
Checking disk status of mysql/fe6cd1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2...
Checking disk status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2...
Checking disk status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2...
Checking disk status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2... done
Checking disk status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2... done
Checking disk status of mysql/fe6cd1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2... done
+-----+-----+-----+-----+-----+-----+
| HOST | NAME/UUID | PERSISTENT DISK USED | EPHEMERAL DISK USED |
+-----+-----+-----+-----+-----+-----+
| 10.244.8.2 | mysql/026d5b79 | 28.9% of 9G (0.0% of 0.61M inodes) | 28.3% of 157.4G (6.4% of 10.49M inodes) |
| 10.244.7.2 | mysql/32665833 | 28.7% of 9G (0.0% of 0.61M inodes) | 28.3% of 157.4G (6.4% of 10.49M inodes) |
| 10.244.9.2 | mysql/fe6cd1e | 28.9% of 9G (0.0% of 0.61M inodes) | 28.3% of 157.4G (6.4% of 10.49M inodes) |
+-----+-----+-----+-----+-----+-----+
```

[View a larger version of this image.](#)

## Example Unhealthy Output

The `mysql-diag` command returns the following message if your canary status is unhealthy:

```
Checking canary status...unhealthy
```

In the event of a broken HA cluster, running `mysql-diag` outputs actionable steps meant to expedite the recovery of that HA cluster. Below is a sample `mysql-diag` output after the tool identified an unhealthy HA cluster:

```
mysql-monitor/5faae86a-a325-44fa-a8ab-24e736e42390:~$ mysql-diag
Wed Jul 19 17:59:43 UTC 2017
Checking canary status...
Checking canary status... healthy
Checking cluster status of mysql/feeced1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2...
Checking cluster status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2...
Checking cluster status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2...
Checking cluster status of mysql/feeced1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2... dial tcp 10.244.9.2:3306: getsockopt: connection refused
Checking cluster status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2... dial tcp 10.244.7.2:3306: getsockopt: connection refused
Checking cluster status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2... dial tcp 10.244.8.2:3306: getsockopt: connection refused
+-----+
| HOST | NAME/UUID | WSREP LOCAL STATE | WSREP CLUSTER STATUS | WSREP CLUSTER SIZE |
+-----+
| 10.244.9.2 | mysql/feeced1e | N/A - ERROR | N/A - ERROR | N/A - ERROR |
| 10.244.7.2 | mysql/32665833 | N/A - ERROR | N/A - ERROR | N/A - ERROR |
| 10.244.8.2 | mysql/026d5b79 | N/A - ERROR | N/A - ERROR | N/A - ERROR |
+-----+
Checking disk status of mysql/feeced1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2...
Checking disk status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2...
Checking disk status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2...
Checking disk status of mysql/32665833-6a66-45dc-bad1-7a6476787d59 at 10.244.7.2... done
Checking disk status of mysql/026d5b79-6844-4227-9e6a-923dd24de9a6 at 10.244.8.2... done
Checking disk status of mysql/feeced1e-83ce-4f7d-96f1-fb658b69cc81 at 10.244.9.2... done
+-----+
| HOST | NAME/UUID | PERSISTENT DISK USED | EPHEMERAL DISK USED |
+-----+
| 10.244.7.2 | mysql/32665833 | 28.7% of 9G (0.0% of 0.61M inodes) | 28.2% of 157.4G (6.3% of 10.49M inodes) |
| 10.244.8.2 | mysql/026d5b79 | 28.9% of 9G (0.0% of 0.61M inodes) | 28.2% of 157.4G (6.3% of 10.49M inodes) |
| 10.244.9.2 | mysql/feeced1e | 28.9% of 9G (0.0% of 0.61M inodes) | 28.2% of 157.4G (6.3% of 10.49M inodes) |
+-----+

[CRITICAL] You must bootstrap the cluster. Follow these instructions: http://docs.pivotal.io/p-mysql/bootstrapping.html

[CRITICAL] Run the download-logs command:
$ download-logs -d /tmp/output -n 10.244.7.2 -n 10.244.8.2 -n 10.244.9.2
For full information about how to download and use the download-logs command see https://discuss.pivotal.io/hc/en-us/articles/221504408

[WARNING] NOT RECOMMENDED
Do not perform the following unless instructed by Pivotal Support:
- Do not scale down the cluster to one node then scale back. This puts user data at risk.
- Avoid "bosh recreate" and "bosh cck". These options remove logs on the VMs making it harder to diagnose cluster issues.
```

[View a larger version of this image.](#)


## Recovering From MySQL Cluster Downtime

Page last updated:

This topic describes the procedure for recovering a terminated Pivotal Application Service (PAS) MySQL cluster using the bootstrapping process.

You can bootstrap your cluster by using one of two methods:

- Run the bootstrap errand. See [Run the Bootstrap Errand](#) below.
- Bootstrap manually. See [Bootstrap Manually](#) below.

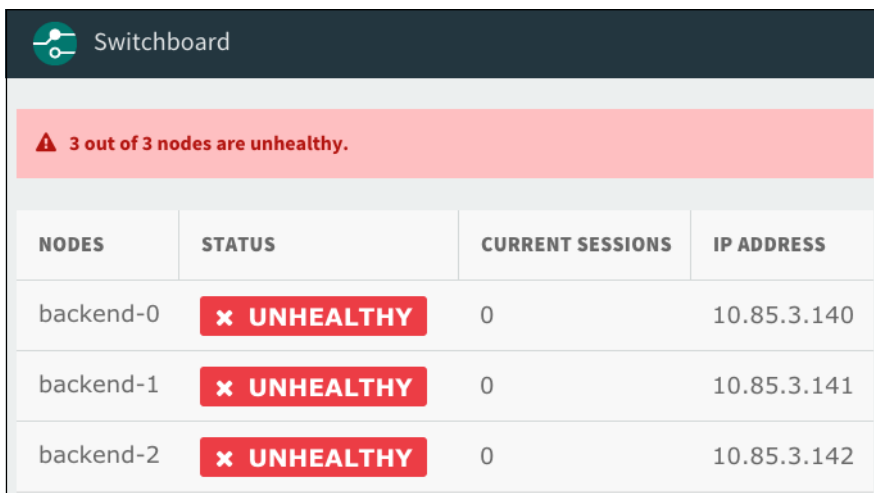
 **Note:** The procedures below assume you are using BOSH CLI v2 or later. For more information about BOSH v2, see [Commands](#) in the BOSH documentation.

### When to Bootstrap

You must bootstrap a cluster that loses quorum. A cluster loses quorum when less than half of the nodes can communicate with each other for longer than the configured grace period. If a cluster does not lose quorum, individual unhealthy nodes automatically rejoin the cluster after resolving the error, restarting the node, or restoring connectivity.

You can detect lost quorum through the following symptoms:

- All nodes appear “Unhealthy” on the proxy dashboard, viewable at `https://BOSH-JOB-INDEX-proxy-p-mysql-ert.YOUR-SYSTEM-DOMAIN`:



| NODES     | STATUS             | CURRENT SESSIONS | IP ADDRESS  |
|-----------|--------------------|------------------|-------------|
| backend-0 | <b>✖ UNHEALTHY</b> | 0                | 10.85.3.140 |
| backend-1 | <b>✖ UNHEALTHY</b> | 0                | 10.85.3.141 |
| backend-2 | <b>✖ UNHEALTHY</b> | 0                | 10.85.3.142 |

- All responsive nodes report the value of `wsrep_cluster_status` as `non-Primary`:

```
mysql> SHOW STATUS LIKE 'wsrep_cluster_status';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| wsrep_cluster_status | non-Primary |
+-----+-----+
```

- All responsive nodes respond with `ERROR 1047` when queried with most statement types:

```
mysql> select * from mysql.user;
ERROR 1047 (08S01) at line 1: WSREP has not yet prepared node for application use
```

See the [Cluster Scaling, Node Failure, and Quorum](#) topic for more details about determining cluster state.

### Run the Bootstrap Errand

The following sections describe what the bootstrap errand is and how to use it based on the type of cluster failure.

## About the Bootstrap Errand

The bootstrap errand automates the steps described in the [Manual Bootstrapping](#) section below. It finds the node with the highest transaction sequence number and asks it to start up by itself in bootstrap mode. Finally, it asks the remaining nodes to join the cluster.

In most cases, running the errand recovers your cluster. But certain scenarios require additional steps.

## Determine Type of Cluster Failure

To determine which set of instructions to follow, do the following:

1. Run the following command.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT instances
```

Where:

- `YOUR-ENV` is the environment where you deployed the cluster.
- `YOUR-DEPLOYMENT` is the deployment cluster name.

For example:

```
$ bosh -e prod -d mysql instances
```

2. Find and record the `Process State` for your MySQL instances. In the following example output, the MySQL instances are in the `failing` process state.

| Instance                                                            | Process State | AZ            | IPs       |
|---------------------------------------------------------------------|---------------|---------------|-----------|
| backup-prepare/c635410e-917d-46aa-b054-86d222b6d1c0                 | running       | us-central1-b | 10.0.4.47 |
| bootstrap/a31af4ff-e1df-4ff1-a781-abc3c6320ed4                      | -             | us-central1-b | -         |
| broker-registrar/1a93e53d-af7c-4308-85d4-3b2b80d504e4               | -             | us-central1-b | 10.0.4.58 |
| cf-mysql-broker/137d52b8-a1b0-41f3-847f-c44f51f87728                | running       | us-central1-c | 10.0.4.57 |
| cf-mysql-broker/28b463b1-cc12-42bf-b34b-82ca7c417c41                | running       | us-central1-b | 10.0.4.56 |
| deregister-and-purge-instances/4cb93432-4d90-4f1d-8152-d0c238fa5aab | -             | us-central1-b | -         |
| monitoring/f7117dcb-1c22-495e-a99e-cf2add90dea9                     | running       | us-central1-b | 10.0.4.48 |
| mysql/220fe72a-9026-4e2e-9fe3-1f5c0b6b09b                           | failing       | us-central1-b | 10.0.4.44 |
| mysql/28a210ac-cb98-4ab4-9672-9f4c661c57b8                          | failing       | us-central1-f | 10.0.4.46 |
| mysql/c1639373-26a2-44ce-85db-c9fe5a42964b                          | failing       | us-central1-c | 10.0.4.45 |
| proxy/87c5683d-12f5-426c-b925-62521529f64a                          | running       | us-central1-b | 10.0.4.60 |
| proxy/b0115ccd-7973-42d3-b6de-edb5ae53c63e                          | running       | us-central1-c | 10.0.4.61 |
| rejoin-unsafe/8ce9370a-e86b-4638-bf76-e103f858413f                  | -             | us-central1-b | -         |
| smoke-tests/e026aaef-efd9-4644-8d14-0811cb1ba733                    | -             | us-central1-b | 10.0.4.59 |

3. Choose your scenario:

- If your MySQL instances are in the `failing` state, continue to [Scenario 1](#).
- If your MySQL instances are in the `-` state, continue to [Scenario 2](#).

## Scenario 1: Virtual Machines Running, Cluster Disrupted

In this scenario, the VMs are running, but the jobs are failing.

To bootstrap in this scenario, do the following:

1. Run the bootstrap errand.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT run-errand bootstrap
```

 **Note:** The errand runs for a long time, during which no output is returned.

The command returns many lines of output, eventually with the following successful output:



```
Bootstrap errand completed
[stderr]
echo 'Started bootstrap errand ...'
JOB_DIR=/var/vcap/jobs/bootstrap
CONFIG_PATH=/var/vcap/jobs/bootstrap/config/config.yml
/var/vcap/packages/bootstrap/bin/cf-mysql-bootstrap -configPath=/var/vcap/jobs/bootstrap/config/config.yml
echo 'Bootstrap errand completed'
exit 0
Errand 'bootstrap' completed successfully (exit code 0)
```

2. If the errand fails, run the bootstrap errand command again after a few minutes. The bootstrap errand may not work immediately.
3. If the errand fails after several tries, bootstrap your cluster manually. See [Bootstrap Manually](#) below.

## Scenario 2: Virtual Machines Terminated or Lost

In severe circumstances, such as a power failure, it is possible to lose all your VMs. You must recreate them before you can begin recovering the cluster.

When MySQL instances are in the `-` state, the VMs are lost. The procedures in this scenario bring the instances from a `-` state to a `failing` state. Then you run the bootstrap errand similar to [Scenario 1](#) above and restore configuration.

To recover terminated or lost VMs, do the procedures in the sections below:

1. [Recreate the Missing VMs](#): Bring MySQL instances from a `-` state to a `failing` state.
2. [Run the Bootstrap Errand](#): Since your instances are now in the `failing` state, you continue similarly to [Scenario 1](#) above.
3. [Restore the BOSH Configuration](#): Go back to unignoring all instances and redeploy. This is a critical and mandatory step.

**⚠ warning:** If you do not set each of your ignored instances to `unignore`, your instances are not updated in future deploys. You must perform the procedure in the final section of *Scenario 2*, [Restore the BOSH Configuration](#).

### Recreate the Missing VMs

The procedure in this section uses BOSH to recreate the VMs, install software on them, and try to start the jobs.

The procedure below allows you to do the following:

- Redeploy your cluster while expecting the jobs to fail.
- Instruct BOSH to ignore the state of each instance in your cluster. This allows BOSH to deploy the software to each instance even if the instance is failing.

To recreate your missing VMs, do the following:

1. If BOSH resurrection is enabled, disable it.

```
bosh -e YOUR-ENV update-resurrection off
```

2. Download the current manifest.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT manifest > /tmp/manifest.yml
```

3. Redeploy and expect one of the MySQL VMs to fail. Deploying causes BOSH to create new VMs and install the software. Forming a cluster is in a subsequent step.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT deploy /tmp/manifest.yml
```

4. Run the following command and record the instance GUID of the VM that attempted to start. Your instance GUID is the string after `mysql/` in your BOSH instances output.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT instances
```

- Tell BOSH to ignore your MySQL instance. Ignoring the state allows BOSH to deploy software to the failed instance.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT ignore mysql/INSTANCE_GUID
```

Where:

- `YOUR-ENV` is the environment where you deployed the cluster.
- `YOUR-DEPLOYMENT` is the deployment cluster name.
- `INSTANCE-GUID` is the string after `mysql/` in your BOSH instances output. For example:

```
$ bosh -e prod -d mysql ignore mysql/220fe72a-9026-4e2c-9fe3-1f5c0b6bf09b
```

- Repeat steps 3 through 5 until all MySQL instances have attempted to start.
- Re-enable BOSH resurrection if you disabled it in the first step.

```
bosh -e YOUR-ENV update-resurrection on
```

- See that your MySQL instances have gone from the `-` state to the `failing` state.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT instances
```

## Run the Bootstrap Errand

All MySQL instances have a `failing` process state, but they now have the MySQL code installed on them. In this section, the bootstrap process recovers the cluster.

To bootstrap, do the following:

- Run the bootstrap errand.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT run-errand bootstrap
```



**Note:** The errand runs for a long time, during which no output is returned.

The command returns many lines of output, eventually with the following successful output:

```
Bootstrap errand completed
[stderr]
echo 'Started bootstrap errand ...'
JOB_DIR=/var/vcap/jobs/bootstrap
CONFIG_PATH=/var/vcap/jobs/bootstrap/config/config.yml
/var/vcap/packages/bootstrap/bin/cf-mysql-bootstrap -configPath=/var/vcap/jobs/bootstrap/config/config.yml
echo 'Bootstrap errand completed'
exit 0
Errand 'bootstrap' completed successfully (exit code 0)
```

- If the errand fails, run the bootstrap errand command again after a few minutes. The bootstrap errand may not work immediately.
- See that the errand completes successfully in the shell output and continue to [Restore the BOSH Configuration](#) below.



**Note:** After you complete the bootstrap errand, you may still see instances in the `failing` state. Continue to the next section anyway.

## Restore the BOSH Configuration

**Warning:** If you do not set each of your ignored instances to `unignore`, your instances are never updated in future deploys.

To restore your BOSH configuration to its previous state, this procedure unignores each instance that was previously ignored.

- Set each ignored instance to `unignore`.

```
bosh -e MY-ENV -d MY-DEP unignore mysql/INSTANCE_GUID
```

## 2. Redeploy.

```
bosh -e MY-ENV -d MY-DEP deploy
```

## 3. Validate that all `mysql` instances are in a `running` state.

```
bosh -e YOUR-ENV -d YOUR-DEPLOYMENT instances
```

## Bootstrap Manually

If the bootstrap errand is not able to automatically recover the cluster, you might need to do the steps manually.

**⚠ warning:** The following procedures are prone to user error and can result in lost data if followed incorrectly. Follow the procedure in [Bootstrap with the BOSH Errand](#) above first, and only resort to the manual process if the errand fails to repair the cluster.

Do the procedures in the sections below to manually bootstrap your cluster. Fresh installs of PCF v2.2 use a [Percona server](#) for their internal system MySQL databases (called MySQL or `mysqld` below), while installations of PCF v2.2 that were upgraded from PCF v2.1 use [MariaDB](#) if you did not migrate your databases to Percona. Use the commands below that are appropriate for your installation of PCF.

## Shut Down MariaDB or MySQL

Do the following for each node in the cluster:

1. SSH into the node. See the [BOSH CLI v2 instructions](#) for SSHing into BOSH-deployed VMs.
2. Shut down the `mariadb` or `mysqld` process on the node, depending on which database is running. Run either `monit stop mariadb_ctrl` (for `mariadb`) or `monit stop galera-init` (for `mysqld`).

Re-bootstrapping the cluster is not successful unless you shut down the `mariadb` or `mysqld` process on all nodes in the cluster.

## Choose Node to Bootstrap

To choose the node to bootstrap, you must find the node with the highest transaction sequence number `seqno`.

Do the following to find the node with the highest `seqno`:

1. Run one of the following commands.
  - **For MariaDB clusters:** `cat /var/vcap/store/mysql/grastate.dat | grep 'seqno:'`
  - **For Percona clusters:** `cat /var/vcap/store/pxc-mysql/grastate.dat | grep 'seqno:'`
2. If a node shut down gracefully, the `seqno` is in the Galera state file. Retrieve the `seqno` and continue to [Bootstrap the First Node](#).
  - a. If a node crashed or was killed, the `seqno` in the Galera state file is recorded as `-1`. In this case, the `seqno` might be recoverable from the database. Run the following command to start up the database, log the recovered `seqno`, and then exit:
    - **For MariaDB clusters:**

```
/var/vcap/packages/mariadb/bin/mysqld --defaults-file=/var/vcap/jobs/mysql/config/my.cnf --wsrep-recover
```
    - **For Percona clusters:**

```
/var/vcap/packages/pxc/bin/mysqld --defaults-file=/var/vcap/jobs/pxc-mysql/config/my.cnf --wsrep-recover
```
  - b. Scan the error log for the recovered `seqno`. It is the last number after the group id (`uuid`). For example:

```
$ grep "Recovered position" /var/vcap/sys/log/pxc-mysql/mysql.err.log | tail -1
150225 18:09:42 mysqld_safe WSREP: Recovered position e93955c7-b797-11e4-9faa-9a6f0b73eb46:15
```

- c. If the node never connected to the cluster before crashing, it may not even have a group ID (`uuid` in `grastate.dat`). In this case, there is nothing to recover. Unless all nodes crashed this way, do not choose this node for bootstrapping.

- After determining the `seqno` for all nodes in your cluster, identify the node with the highest `seqno`. If all nodes have the same `seqno`, you can choose any node as the new bootstrap node.

## Bootstrap the First Node

After determining the node with the highest `seqno`, do the following to bootstrap the node:

**Note:** Only run these bootstrap commands on the node with the highest `seqno`. Otherwise the node with the highest `seqno` is unable to join the new cluster unless its data is abandoned. Its `mariadb` or `mysqld` process exits with an error.

- On the new bootstrap node, update the state file and restart the `mariadb` or `mysqld` process. Run either of the following commands, depending on which database is running:

```
echo -n "NEEDS_BOOTSTRAP" > /var/vcap/store/mysql/state.txt
monit start mariadb_ctrl
```

```
echo -n "NEEDS_BOOTSTRAP" > /var/vcap/store/pxc-mysql/state.txt
monit start galera-init
```

- It can take up to ten minutes for `monit` to start the `mariadb` or `mysqld` process. To check if the `mariadb` or `mysqld` process has started successfully, run the following command:

```
watch monit summary
```

## Restart Remaining Nodes

- After the bootstrapped node is running, start the `mariadb` or `mysqld` process on the remaining nodes with `monit`. From the bootstrap node, run either `monit start mariadb_ctrl` (for `mariadb`) or `monit start galera-init` (for `mysqld`). If the node is prevented from starting by the [Interruptor](#), do the manual procedure to force the node to rejoin the cluster, documented in [Pivotal Knowledge Base](#).

**Warning:** Forcing a node to rejoin the cluster is a destructive procedure. Only do the procedure with the assistance of [Pivotal Support](#).

- If the `monit start` command fails, it might be because the node with the highest `seqno` is the lowest BOSH-indexed node (`mysql/0`). In this case, do the following:
  - From the Ops Manager VM, use the BOSH CLI to make BOSH ignore updating `mysql/0`: `bosh -e MY-ENV -d MY-DEP ignore mysql/0`
  - Navigate to Ops Manager in a browser, log in, and click **Apply Changes**.
  - When the deploy finishes, run the following command from the Ops Manager VM: `bosh -e MY-ENV -d MY-DEP unignore mysql/0`
- Verify that the new nodes have successfully joined the cluster. SSH into the bootstrap node and run the following command to output the total number of nodes in the cluster:

```
mysql> SHOW STATUS LIKE 'wsrep_cluster_size';
```

## Configuring Authentication and Enterprise SSO for PAS

Page last updated:

This topic describes [Pivotal Cloud Foundry](#) (PCF) Pivotal Application Service (PAS) authentication and single sign-on configuration with Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML).


Refer to the instructions below to configure your deployment with SAML or LDAP.

Connecting PAS to either the LDAP or SAML external user store allows the User Account and Authentication (UAA) server to delegate authentication to existing enterprise user stores.

If your enterprise user store is exposed as a SAML or LDAP Identity Provider for single sign-on (SSO), you can configure SSO to allow users to access the Apps Manager and Cloud Foundry Command Line Interface (cf CLI) without creating a new account or, if using SAML, without re-entering credentials.

See the [Adding Existing SAML or LDAP Users to a PCF Deployment](#) topic for information about managing user identity and pre-provisioning user roles with SAML or LDAP in PCF.

For an explanation of the process used by the UAA Server when it attempts to authenticate a user through LDAP, see [Configuring LDAP Integration with Pivotal Cloud Foundry](#) in the Pivotal Knowledge Base.

 **Note:** When integrating with an external identity provider, such as LDAP, authentication within the UAA becomes chained. An authentication attempt with a user's credentials is first attempted against the UAA user store before the external provider, LDAP. For more information, see [Chained Authentication](#) in the *User Account and Authentication LDAP Integration* GitHub documentation.

## Configure PAS to Use a SAML Identity Provider

In SAML terminology, the SAML protocol communicates user data between an identity provider (IdP) and a service provider (SP).

To connect PAS with SAML, do the following:

- [Configure PAS as a Service Provider for SAML](#)
- [Configure SAML as an Identity Provider for PAS](#)

### Configure PAS as a Service Provider for SAML

To configure PAS to use a SAML IdP, do the following:

1. From the **Installation Dashboard**, click the PAS tile.
2. Select the **Domains** tab and record your system domain.

[Installation Dashboard](#)

## Pivotal Elastic Runtime

Settings
Status
Credentials
Logs

✓ Assign AZs and Networks

✓ Domains

✓ Networking

✓ Application Containers

✓ Application Developer Controls

✓ Application Security Groups

✓ Authentication and Enterprise SSO

✓ Databases

Elastic Runtime hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain \*

Apps Domain \*

Save

Default parent domain that pushed apps use for their hostnames. This domain also requires a wildcard DNS record. Use the Cloud Foundry command line interface (cf CLI) to add or delete subdomains assigned to individual apps.

3. Select **Authentication and Enterprise SSO**.

SAML Identity Provider

Provider Name \*

Name of Identity Provider. Allowed characters are alphanumeric, plus ` \_ `, and ` - `.

Display Name \*

Provider Metadata (if you would rather provide an SSO endpoint URL, skip to the next field)

(OR) Provider Metadata URL

Name ID Format \*

Email Address

Email Domain(s)

First Name Attribute

Last Name Attribute

Email Attribute

External Groups Attribute

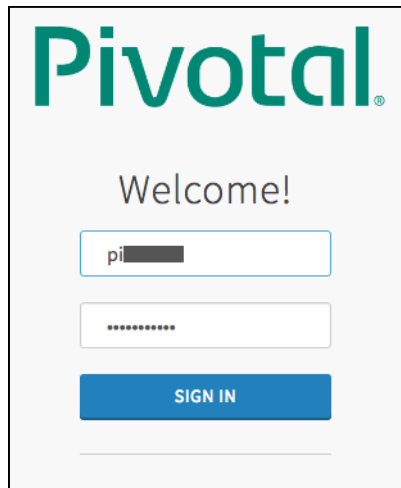
☒ Sign Authentication Requests

☐ Require Signed Assertions

4. Select **SAML Identity Provider**.

5. Set the **Provider Name**. This is a unique name you create for the Identity Provider. This name can include only alphanumeric characters, `+`, `_`, and `-`. You should not change this name after deployment because all external users use it to link to the provider.

6. Enter a **Display Name**. Your provider display name appears as a link on your Pivotal login page, which you can access at <https://login.YOUR-SYSTEM->



DOMAIN.

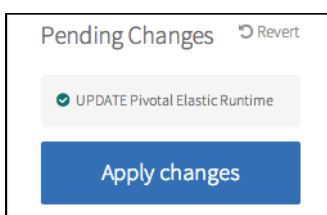
7. Retrieve the metadata from your Identity Provider and copy it into either the **Provider Metadata** or the **Provider Metadata URL** fields, depending on whether your Identity Provider exposes a Metadata URL or not. Refer to the [Configure SAML as an Identity Provider for PAS](#) section of this topic for more information. Pivotal recommends that you use the Provider Metadata URL rather than Provider Metadata because the metadata can change. You can do this in either of the following ways:

- If your Identity Provider exposes a Metadata URL, provide the Metadata URL.
- Download your Identity Provider metadata and paste this XML into the **Provider Metadata** area.

**Note:** You only need to select one of the above configurations. If you configure both, your Identity Provider defaults to the (OR) **Provider Metadata URL**.

**Note:** See [Adding Existing SAML or LDAP Users to a PCF Deployment](#) for information about on-boarding SAML users and mapping them to PAS user roles.

8. Select the **Name ID Format** for your SAML Identity Provider. This translates to `username` on PAS. The default is `Email Address`.
9. For **Email Domain(s)**, enter a comma-separated list of the email domains for external users who will receive invitations to Apps Manager.
10. For **First Name Attribute** and **Last Name Attribute**, enter the attribute names in your SAML database that correspond to the first and last names in each user record, for example `first_name` and `last_name`. This field is case sensitive.
11. For **Email Attribute**, enter the attribute name in your SAML assertion that corresponds to the email address in each user record, for example `EmailID`. This field is case sensitive.
12. For **External Groups Attribute**, enter the attribute name in your SAML database that defines the groups that a user belongs to, for example `group_memberships`. To map the groups from the SAML assertion to admin roles in PAS, follow the instructions in the [Grant Admin Permissions to an External Group \(SAML or LDAP\)](#) section of the *Creating and Managing Users with the UAA CLI (UAA C)* topic. This field is case sensitive.
13. By default, all SAML Authentication Request from PAS are signed. To change this, disable the **Sign Authentication Requests** checkbox and configure your Identity Provider to verify SAML authentication requests.
14. To validate the signature for the incoming SAML assertions, enable the **Required Signed Assertions** checkbox and configure your Identity Provider to send signed SAML assertions.
15. Click **Save**.
16. Return to the **Installation Dashboard** by clicking the link.
17. On the Installation Dashboard, click **Apply Changes**.





## Configure SAML as an Identity Provider for PAS

To configure a SAML IdP to designate PAS as an SP, do the following:

Download the Service Provider Metadata from <https://login.YOUR-SYSTEM-DOMAIN/saml/metadata>. Consult the documentation from your Identity Provider for configuration instructions.

Refer to the table below for information about certain industry-standard Identity Providers and how to integrate them with PAS:

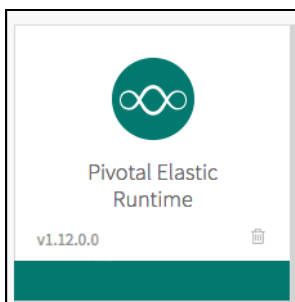
| Solution Name                                                          | Integration Guide    |
|------------------------------------------------------------------------|----------------------|
| <a href="#">CA Single Sign-On aka CA SiteMinder</a> <a href="#">↗</a>  | <a href="#">Link</a> |
| <a href="#">Ping Federate</a> <a href="#">↗</a>                        | <a href="#">Link</a> |
| <a href="#">Active Directory Federation Services</a> <a href="#">↗</a> | <a href="#">Link</a> |

**Note:** Some Identity Providers allow uploads of Service Provider Metadata. Other providers require you to manually enter the Service Provider Metadata into a form. If your Identity Provider requires manual entry but is not listed above, see the [CA SiteMinder SSO Integration Guide](#).

## Configure LDAP as an Identity Provider for PAS

To integrate the UAA with one or more LDAP servers, configure PAS with your LDAP endpoint information as follows:

1. Log into the Operations Manager web interface.
2. On the Product Dashboard, select the PAS tile.



3. In the left navigation menu, select **Authentication and Enterprise SSO**.

LDAP Server

Server URL \*

ldaps://example.com

LDAP Credentials \*

Username

Password

User Search Base \*

ou=Groups,dc=example,dc=com

User Search Filter \*

cn={0}

Group Search Base

ou=Groups,dc=example,dc=com

Group Search Filter \*

member={0}

Server SSL Cert


Server SSL Cert AltName


First Name Attribute

4. Under **Configure your UAA**, select **LDAP Server**.

- For **Server URL**, enter the URL that point your LDAP server. With multiple LDAP servers, separate their URLs with spaces. Each URL must include one of the following protocols:
  - `ldap://`: This specifies that the LDAP server uses an unencrypted connection.
  - `ldaps://`: This specifies that the LDAP server uses SSL for an encrypted connection and requires that the LDAP server holds a trusted certificate or that you import a trusted certificate to the JVM truststore.
- For **LDAP Credentials**, enter the LDAP Distinguished Name (DN) and password for binding to the LDAP Server. Example DN:
 

cn=administrator,ou=Users,dc=example,dc=com

 **Note:** Pivotal recommends that you provide LDAP credentials that grant read-only permissions on the LDAP Search Base and the LDAP Group Search Base. In addition to this, if the bind user belongs to a different search base, you must use the full DN.

 **Warning:** Pivotal recommends against reusing LDAP service accounts across environments. LDAP service accounts should not be subject to manual lockouts, such as lockouts that result from users utilizing the same account. Also, LDAP service accounts should not be subject to automated deletions, since disruption to these service accounts could prevent user logins.


- For **User Search Base**, enter the location in the LDAP directory tree from which any LDAP User search begins. The typical LDAP Search Base matches your domain name.

For example, a domain named “cloud.example.com” typically uses the following LDAP User Search Base: `ou=Users,dc=example,dc=com`

- For **User Search Filter**, enter a string that defines LDAP User search criteria. These search criteria allow LDAP to perform more effective and efficient searches. For example, the standard LDAP search filter `cn=Smith` returns all objects with a common name equal to `Smith`.

In the LDAP search filter string that you use to configure PAS, use `{0}` instead of the username. For example, use `cn={0}` to return all LDAP objects with the same common name as the username.

In addition to `cn`, other attributes commonly searched for and returned are `mail`, `uid` and, in the case of Active Directory, `sAMAccountName`.

 **Note:** For instructions for testing and troubleshooting your LDAP search filters, see [Configuring LDAP Integration with Pivotal Cloud Foundry](#) in the Pivotal Support Knowledge Base.

- For **Group Search Base**, enter the location in the LDAP directory tree from which the LDAP Group search begins.

For example, a domain named “cloud.example.com” typically uses the following LDAP Group Search Base: `ou=Groups,dc=example,dc=com`

Follow the instructions in the [Grant Admin Permissions to an External Group \(SAML or LDAP\)](#) section of *Creating and Managing Users with the UAA CLI (UAAC)* to map the groups under this search base to admin roles in PAS.

 **Note:** See [Adding Existing SAML or LDAP Users to a PCF Deployment](#) to on-board individual LDAP users and map them to PAS Roles.

- For **Group Search Filter**, enter a string that defines LDAP Group search criteria. The standard value is `member={0}`.
- For **Server SSL Cert**, paste in the root certificate from your CA certificate or your self-signed certificate.
- For **First Name Attribute** and **Last Name Attribute**, enter the attribute names in your LDAP directory that correspond to the first and last names in each user record, for example `cn` and `sn`.
- For **Email Attribute**, enter the attribute name in your LDAP directory that corresponds to the email address in each user record, for example `mail`.
- For **Email Domain(s)**, enter a comma-separated list of the email domains for external users who will receive invitations to Apps Manager.

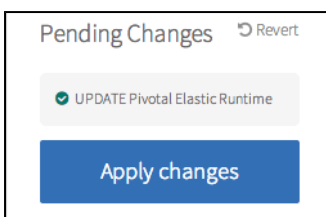
1. For **LDAP Referrals**, select how the UAA handles LDAP server referrals out to other external user stores. The UAA can:

- Automatically follow any referrals.
- Ignore referrals and return parital result.
- Throw exception for each referral and abort.

2. Click **Save**.

3. Return to the **Installation Dashboard** by clicking the link.

4. On the Installation Dashboard, click **Apply Changes**.



## Configuring ADFS as an Identity Provider

Page last updated:

This topic describes the process of configuring Active Directory Federation Services (ADFS) as your identity provider (IdP) in Pivotal Cloud Foundry (PCF) and ADFS.

### Configure SAML Integration in PCF

You can use ADFS as your SAML IdP for Ops Manager and Pivotal Application Service (PAS):

- If you want to use ADFS as your SAML IdP for Ops Manager, do the following:
  - [Configure SAML Integration in Ops Manager](#)
  - [Configure SAML Integration in ADFS](#)
- If you want to use ADFS as your SAML IdP for PAS, do the following:
  - [Configure SAML Integration in PAS](#)
  - [Configure SAML Integration in ADFS](#)

### Configure SAML Integration in Ops Manager

To configure Ops Manager to use ADFS as your SAML IdP, do the following:

1. Download your IdP metadata from `https://YOUR-ADFS-HOSTNAME/federationmetadata/2007-06/federationmetadata.xml`.
2. Perform the steps in the *Use an Identity Provider* section of the BOSH Director configuration topic for your IaaS:
  - [Configuring BOSH Director on AWS](#)
  - [Configuring BOSH Director on Azure Manually](#)
  - [Configuring BOSH Director on GCP](#)
  - [Configuring BOSH Director on OpenStack](#)
  - [Configuring BOSH Director on vSphere](#)

 **Note:** You can set up SAML access for Ops Manager during the initial PCF installation or later by navigating to **Settings** in the user menu on the Ops Manager Installation Dashboard, configuring the **Authentication Method** pane, and then clicking **Apply Changes**.

### Configure SAML Integration in PAS

To configure PAS to use ADFS as your SAML IdP, do the following:

1. Download your IdP metadata from `https://YOUR-ADFS-HOSTNAME/federationmetadata/2007-06/federationmetadata.xml`.
2. Perform the steps in the [Configure PCF as a Service Provider for SAML](#) section of the *Configuring Authentication and Enterprise SSO for PAS* topic.

### Configure SAML Integration in ADFS

To designate PCF as your SAML service provider (SP) in ADFS, do the following:

1. Download your SP metadata from `https://login.YOUR-SYSTEM-DOMAIN/saml/metadata`.
2. Open your **ADFS Management** console and add a relying party trust as follows:
  - a. Click **Add Relying Party Trust...** in the **Actions** pane.
  - b. On the Welcome step, click **Start**.
  - c. Select **Import data about the relying party from a file**, import the downloaded SP metadata file, and click **Next**.
  - d. Enter a **Display name** for the new relying party trust and click **Next**.
  - e. Leave the default multi-factor authentication selection and click **Next**.

- f. Select **Permit all users to access this relying party** and click **Next**.
- g. Review your settings and click **Next**.
- h. Click **Close** to finish the wizard.

3. Modify your relying party trust as follows:

- a. Double-click the new relying party trust.
- b. Select the **Encryption** tab and click **Remove** to remove the encryption certificate you imported.
- c. In the **Advanced** tab, select **SHA256** for the **Secure hash algorithm**.

4. (Optional) If you are using a self-signed certificate and want to disable CRL checks, do the following:

- a. Open **Windows Powershell** as an Administrator.
- b. Run the following command:

```
set-ADFSRelyingPartyTrust -TargetName "RELYING-PARTY-TRUST" -SigningCertificateRevocationCheck None
```

5. To add claim rules for your relying party trust, select your relying party trust and click **Edit Claim Rules...**

6. In the **Issuance Transform Rules** tab, create two claim rules as follows:

- a. Click **Add Rule**.
- b. Select **Send LDAP Attributes as Claims** for **Claim rule template** and click **Next**.
- c. Enter a **Claim rule name**.
- d. Select **Active Directory** for **Attribute store**.
- e. Select **E-Mail-Addresses** for **LDAP Attribute** and **E-Mail Address** for **Outgoing Claim Type**. Alternatively, if you do not have the email attribute configured for users, you can select **User-Principle-Name** under **LDAP Attribute**.
- f. Click **Finish**.

- g. Click **Add Rule**.
- h. Select **Transform an Incoming Claim** for **Claim rule template** and click **Next**.
- i. Enter a **Claim rule name**.
- j. Select **E-Mail Address** for **Incoming claim type**.
- k. Select **Name ID** for **Outgoing claim type**.
- l. Select **Email** for **Outgoing name ID format**.
- m. Click **Finish**.

7. To permit access to users based on a security group, navigate to the **Issuance Authorization Rules** tab and create an authorization claim rule as follows:

- a. Click **Add Rule**.
- b. Select **Permit or Deny Users Based on an Incoming Claim** for **Claim rule template** and click **Next**.
- c. Enter a **Claim rule name**.
- d. Select **Group SID** for **Incoming claim type**.
- e. Click **Browse** and locate the security group in your domain that PCF developers are a part of and click **OK**.
- f. Ensure **Permit access to users with this incoming claim** is selected.
- g. Click **Finish**.

## Configuring CA as an Identity Provider

This topic explains how to configure single sign-on (SSO) between CA and Pivotal Cloud Foundry (PCF).

### Overview

Partnership creation between CA and PCF involves the following steps:

1. Installing and configuring the prerequisites
2. Configuring CA Single Sign-On as an Identity Provider
3. Configuring the Service Provider

### Prerequisites

- CA Single Sign-On v12.52 installation
- User store and Session store configuration
- Creation of Signed Certificate by a Certificate Authority
- Protect Identity Provider URL with CA SSO by creating the following objects:
  - Authentication scheme
  - Domain
  - Realm
  - Rules and policy
- PCF Environment at <https://console.YOUR-SYSTEM-DOMAIN> [↗](#)



**Note:** Replace YOUR-SYSTEM-DOMAIN with the name of your PCF installation.

## Configuring CA as the SAML 2.0 Identity Provider on PCF


1. Download the service provider metadata.
  - a. Navigate `https://login.YOUR-SYSTEM-DOMAIN/saml/metadata` and log in to CA SSO.
  - b. Navigate to **Federation**.
  - c. Select **Partnership Federation**
  - d. In the Actions menu, select **Export Metadata**.
  - e. Save the exported metadata in an XML file.
2. Follow the steps in [Configuring Authentication and Enterprise SSO for Elastic Runtime](#) to set the identity provider metadata on PCF.
3. Paste the contents of the XML file into the **Identity Provider Metadata** field.
4. Click **Save**.
5. Click **Apply Changes**.

## Configuring PCF as the SAML 2.0 Service Provider on CA Single Sign-On

### Configure Identity Provider and Service Provider Entities

1. Navigate to `https://login.YOUR-SYSTEM-DOMAIN/` and log in to CA SSO.
2. Navigate to **Federation**.


3. Click **Partnership Federation**.
4. Click **Entity**.
5. Click **Create Entity**.
6. To create a local entity, use the values below:
  - o **Entity Location:** Local
  - o **Entity Type:** SAML2 IDP
  - o **Entity ID:** Enter an ID for your local identity provider. For example, `https://ca-technologies.xxx.com`.
  - o **Entity Name:** Create a name for your local identity provider.
  - o **Base URL:** Enter the fully-qualified domain name for the host service CA SSO Federation Web Services.
  - o **Signing Private Key Alias:** Select the private key alias or import a private key.
  - o **Signed Authentication Requests Required:** Select **No**.
  - o **Supported NameID format:** Enter `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` and `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` to select both email address and unspecified as supported NameID formats.
7. To create a remote entity, click **Import Metadata Button** and do the following:
  - a. Download the service provider metadata from <https://login.{systemdomain}/saml/metadata> and save to an XML file.
  - b. Browse and select the saved XML Metadata you downloaded in the previous step.
  - c. Provide a name for the Remote Service Provider Entity.
  - d. Provide an alias for the Signing Certificate imported from the Metadata.

 **Note:** PCF signs the outgoing SAML authentication requests.


- e. Click **Save**.

## Configure Partnership Between CA SSO and PCF

1. Navigate to `https://login.YOUR-SYSTEM-DOMAIN/` and log in to CA SSO.
2. Navigate to **Federation**.
3. Click **Partnership Federation**.
4. Click **Create Partnership**.
5. To configure the partnership, use the values below to fill in the fields:
  - o **Add Partnership Name:** Enter a name for your partnership.
  - o (optional) **Description:** Enter a relevant description for your partnership.
  - o **Local IPD ID:** Enter the Local Service Provider ID you created in the [Configure Identity Provider and Service Provider Entities](#) section.
  - o **Remote SP ID:** Enter the Remote SP ID you created in the [Configure Identity Provider and Service Provider Entities](#) section.
  - o **Base URL:** This field will be pre-populated.
  - o **Skew Time:** Enter any skew time required by your environment.
  - o **User Directories and Search Order:** Select the required directories in the required search order.
6. Click **Next**.
7. On the Federation Users page, accept the default values.
8. Click **Next**.
9. To complete the Name ID Format section:
  - a. Select **Email Address** from the Name ID Format dropdown.
  - b. Select **User Attribute** from the Name ID Type dropdown.

 **Note:** PCF does not support processing SAML Assertion Attributes at this time. You can skip filling out the Assertion Attributes fields.

10. Click **Next**.
11. To complete the SSO and SLO section:

- a. Enter the Authentication URL that is protected by CA SSO under prerequisites.
- b. For SSO Binding, click **HTTP-POST**.
- c. In the Audience field, enter <http://login.YOUR-SYSTEM-DOMAIN> .



**Note:** The **Audience** field requires `http://` instead of `https://`. This is only a naming convention within the schema and does not determine connection security.

- d. Select **Both IDP and DP Initiated** from the Transactions Allowed dropdown.
- e. The Assertion Consumer Service URL field will be pre-populated using information from the service provider entity.

12. Click **Next**.

13. To complete the Configure Signature and Encryption section:

- a. In the **Signing Private Key Alias** dropdown, verify that the correct Private Key Alias is selected.
- b. Verify that the correct Verification Certificate Alias is selected in the **Verification Certificate Analysis** dropdown. This alias should be the same certificate created when you import the [Remote Service Provider Entity ID](#).
- c. Select **Sign Both** from the Post Signature Options dropdown.



**Note:** PCF does not support encryption options at this time.

- d. Click **Finish**.

14. To activate the partnership, expand the Action dropdown for your partnership and click **Activate**.



## Configuring PingFederate as an Identity Provider

Page last updated:

This topic explains how to configure single sign-on (SSO) between PingFederate and Pivotal Application Service (PAS).

## Configuring PingFederate as the SAML 2.0 Identity Provider on PAS

1. Download your Identity Provider Metadata from PingFederate Server. Click **Metadata Export** under **Administrative Functions** on the Main Menu of the PingFederate Administrative Console. If your PingFederate server is configured to act as both an Identity Provider (IdP) and a service provider (SP), indicate which type of configuration you want to export and click **Next**. The Signing key can be exported. You can skip the options related to Encryption Keys and Metadata Attribute Contract because they are not supported at this time.
2. Follow the steps in [Configuring Authentication and Enterprise SSO for PAS](#) to set your IdP metadata on PAS.

## Configuring PAS as the SAML 2.0 Service Provider on PingFederate

1. Download your Service Provider Metadata from `https://login.YOUR-SYSTEM-DOMAIN/saml/metadata`.
2. Import the Service Provider Metadata to PingFederate. Navigate to **Main Menu** → **IdP Configuration** → **SP Connection** and click **Import**. In the **Import Connection** screen, browse and select the `.xml` file downloaded in the previous step. Click **Import** and **Done**.
3. PAS expects the NameID format to be an email address (for example, `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`) and the value to be the email address of the currently logged in user. The SSO does not function without this setting.
  - a. Click the connection name on **Main Menu**. To see a full list of connections, click **Manage All SP**.
  - b. Click **Browser SSO** under the **SP Connection** tab.
  - c. Click **Configure Browser SSO**.
  - d. Click **Assertion Creation** under the **Browser SSO** tab.
  - e. Click **Configure Assertion Creation**.
  - f. Click **Identity Mapping** on the **Summary** screen.
  - g. Select **Standard** as the option and map the NameID format to be an email address and the value to be the email address of the user.
4. Select the Authentication Source.
  - a. Click **Browser SSO** under the **SP Connection** tab.
  - b. Click **Configure Browser SSO**.
  - c. Click **Assertion Creation** under the **Browser SSO** tab.
  - d. Click **Configure Assertion Creation**.
  - e. Click **IdP Adapter Mapping** on the **Summary** screen.
  - f. Click **Adapter Instance Name**.
  - g. Click **Adapter Instance** on the **Summary** screen.
5. Enable the SSO Browser Profiles.
  - a. Click **Browser SSO** under the **SP Connection** tab.
  - b. Click **Configure Browser SSO**.
  - c. Click **SAML Profiles** on the **Summary** screen.
  - d. Ensure that IdP & SP initiated SSO are selected.



**Note:** PAS does not support SLO profiles at this time, and you can leave them unchecked.

6. Activate the SP Connection.

## Switching Application Domains

Page last updated:

This topic describes how to change the domain of an existing [Pivotal Cloud Foundry](#) (PCF) installation, using an example domain change from

`myapps.mydomain.com` to `newapps.mydomain.com`.

1. In PCF Ops Manager, select the **Pivotal Application Service** tile.
2. Select **Domains** from the menu to see the current **Apps Domain** for your Pivotal Application Service (PAS) deployment. In the following example it is `myapps.mydomain.com`.

Elastic Runtime hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain \*

`mysystem.mydomain.com`

Apps Domain \*

`myapps.mydomain.com`

Default parent domain that pushed apps use for their hostnames. This domain also requires a wildcard DNS record. Use the Cloud Foundry command line interface (cf CLI) to add or delete subdomains assigned to individual apps.

Save

3. In the terminal, run `cf login -a YOUR_API_ENDPOINT`. The cf CLI prompts you for your PCF username and password, as well as the org and space you want to access. See [Identifying the API Endpoint for your PAS Instance](#) if you don't know your API endpoint.
4. Run `cf domains` to view the domains in the space. If you have more than one shared domain, ensure that the domain you want to change is at the top of the list before you apply the new domain to your PAS tile configuration. You can delete and re-create the other shared domains as necessary to push the domain you want to change to the top of the list. If you do this, make sure to [re-map the routes for each domain](#).

```
$ cf domains
Getting domains in org my-org as admin...

name status
myapps.mydomain.com shared
```

5. Run `cf routes` to confirm that your apps are assigned to the domain you plan to change.

```
$ cf routes
Getting routes as admin ...

space host domain apps
my-space myapp myapps.mydomain.com myapp
```

6. Run `cf create-shared-domain YOUR_DESIRED_NEW_DOMAIN` to create the new domain you want to use:

```
$ cf create-shared-domain newapps.mydomain.com


Creating shared domain newapps.mydomain.com as admin...
OK
```

7. Run `cf map-route APP_NAME NEW_DOMAIN -n HOST_NAME` to map the new domain to your app. In this example both the `NEW_DOMAIN` and `HOST_NAME` arguments are `myapp`, since this is both the name of the app to which we are mapping a route, and the intended hostname for the URL.

```
$ cf map-route myapp newapps.mydomain.com -n myapp

Creating route myapp.newapps.mydomain.com for org my-org / space my-space as admin...
OK
Adding route myapp.newapps.mydomain.com to app myapp in org my-org / space my-space as admin...
OK
```

- Repeat the previous step for each app in this space. Afterwards, check Apps Manager to confirm that the route URL has updated correctly for each app:

| SPACE<br>my-space                                                                 |                                    |           |
|-----------------------------------------------------------------------------------|------------------------------------|-----------|
| APPLICATIONS <a href="#">Learn More</a>                                           |                                    |           |
| STATUS                                                                            | APP                                | INSTANCES |
|  | myapp<br>myapp.newapps.mydomain... | 1         |

- Repeat the above steps for each space in your PCF installation except for the System org, beginning with logging into the org and space and ending with confirming the URL update.

**Note:** Ordinarily the System org contains only PCF apps that perform utility functions for your installation. Pivotal does not recommend pushing apps to this org. However, if you have pushed apps to System, you must also repeat the above steps for these apps.

- Once you have confirmed that every app in every space has been mapped to the new domain, delete the old domain by running `cf delete-shared-domain OLD_DOMAIN_TO_DELETE`:

```
$ cf delete-shared-domain myapps.mydomain.com
Deleting domain myapps.mydomain.com as admin...

This domain is shared across all orgs.
Deleting it will remove all associated routes, and will make any app with this domain unreachable.
Are you sure you want to delete the domain myapps.mydomain.com?
> yes
OK
```

- Configure your PAS tile to use the new domain, and apply changes. Apps that you push after your update finishes use this new domain.

Elastic Runtime hosts applications at subdomains under its apps domain and assigns system components to subdomains under its system domain. You need to configure a wildcard DNS for both the apps domain and system domain. The two domains can be the same, although this is not recommended.

System Domain \*

This domain is for system-level PCF components, such as Apps Manager, service brokers, etc. You must set up a wildcard DNS record for this domain that points to your entry point load balancer or HAProxy.

Apps Domain \*

Save




## Scaling PAS

Page last updated:

This topic discusses how to scale Pivotal Application Service (PAS) for different deployment scenarios. To increase the capacity and availability of the Pivotal Cloud Foundry (PCF) platform, and to decrease the chances of downtime, you can scale a deployment up using the instructions below.

If you want to make a PCF configuration highly available, see the [High Availability in Cloud Foundry](#) topic.

 **Note:** In PCF v1.11 and later, PAS defaults to a highly available resource configuration.

## Scaling Recommendations

The following table provides recommended instance counts for a high-availability deployment and the minimum instances for a functional deployment:

| Pivotal Application Service (PAS) Job | Recommended Instance Number for HA | Minimum Instance Number | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Diego Cell                            | $\geq 3$                           | 1                       | The optimal balance between CPU/memory sizing and instance count depends on the performance characteristics of the apps that run on Diego cells. Scaling vertically with larger Diego cells makes for larger points of failure, and more apps go down when a cell fails. On the other hand, scaling horizontally decreases the speed at which the system rebalances apps. Rebalancing 100 cells takes longer and demands more processing overhead than rebalancing 20 cells. |
| Diego Brain                           | $\geq 2$                           | 1                       | For high availability, use at least one per AZ, or at least two if only one AZ.                                                                                                                                                                                                                                                                                                                                                                                              |
| Diego BBS                             | $\geq 2$                           | 1                       | For high availability in a multi-AZ deployment, use at least one instance per AZ. Scale Diego BBS to at least two instances for high availability in a single-AZ deployment.                                                                                                                                                                                                                                                                                                 |
| Consul                                | $\geq 3$                           | 1                       | Set this to an odd number equal to or one greater than the number of AZs you have, in order to maintain quorum. Distribute the instances evenly across the AZs, at least one instance per AZ.                                                                                                                                                                                                                                                                                |
| MySQL Internal Load Balancer          | 1                                  | 0                       | A load balancer distributes SQL traffic across two redundant MySQL proxies.                                                                                                                                                                                                                                                                                                                                                                                                  |
| MySQL Proxy                           | 2                                  | 1                       | If you use an <a href="#">external database</a> in your deployment, then you can set the MySQL Proxy instance count to <code>0</code> .                                                                                                                                                                                                                                                                                                                                      |
| MySQL Server                          | 3                                  | 1                       | If you use an <a href="#">external database</a> in your deployment, then you can set the MySQL Server instance count to <code>0</code> . For instructions about scaling down an internal MySQL cluster, see <a href="#">Scaling Down Your MySQL Cluster</a> .                                                                                                                                                                                                                |
| NATS Server                           | $\geq 2$                           | 1                       | In a high availability deployment, you might run a single NATS instance if your deployment lacks the resources to deploy two stable NATS servers. Components using NATS are resilient to message failures and the BOSH resurrector recovers the NATS VM quickly if it becomes non-responsive.                                                                                                                                                                                |
| Cloud Controller                      | $\geq 2$                           | 1                       | Scale the Cloud Controller to accommodate the number of requests to the API and the number of apps in the system.                                                                                                                                                                                                                                                                                                                                                            |
| Clock Global                          | $\geq 2$                           | 1                       | For a high availability deployment, scale the Clock Global job to a value greater than 1 or to the number of AZs you have.                                                                                                                                                                                                                                                                                                                                                   |
| Router                                | $\geq 2$                           | 1                       | Scale the router to accommodate the number of incoming requests. Additional instances increase available bandwidth. In general, this load is much less than the load on Diego cells.                                                                                                                                                                                                                                                                                         |
| HAProxy                               | 0 or $\geq 2$                      | 0 or 1                  | For environments that require high availability, you can scale HAProxy to <code>0</code> and then configure a high-availability load balancer (LB) to point directly to each Gorouter instance. Alternately, you can also configure the high availability LB to point to HAProxy instance scaled at $\geq 2$ . Either way, an LB is required to host Cloud Foundry domains at a single IP address.                                                                           |
| UAA                                   | $\geq 2$                           | 1                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Doppler Server                        | $\geq 2$                           | 1                       | Deploying additional Doppler servers splits traffic across them. For a high availability deployment, Pivotal recommends at least two per Availability Zone.                                                                                                                                                                                                                                                                                                                  |
| Loggregator Trafficcontroller         | $\geq 2$                           | 1                       | Deploying additional Loggregator Traffic Controllers allows you to direct traffic to them in a round-robin manner. For a high availability deployment, Pivotal recommends at least two per Availability Zone.                                                                                                                                                                                                                                                                |
| Syslog                                | $\geq 2$                           | 1                       | The Syslog Scheduler is a scalable component. For high availability, use at least one instance per AZ,                                                                                                                                                                                                                                                                                                                                                                       |

Scheduler | | or at least two instances if only one AZ is present.


## Scaling Up PAS

To scale up PAS instances, do the following:

1. Navigate to the Pivotal Cloud Foundry Operations Manager Installation Dashboard.
2. Click the PAS tile in the Installation Dashboard.
3. Select **Resource Config**.

| Resource Config               |              |                      |                                                           |
|-------------------------------|--------------|----------------------|-----------------------------------------------------------|
| JOB                           | INSTANCES    | PERSISTENT DISK TYPE | VM TYPE                                                   |
| Consul                        | Automatic: 3 | Automatic: 1 GB      | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| NATS                          | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| File Storage                  | Automatic: 1 | Automatic: 100 GB    | Automatic: medium.mem (cpu: 1, ram: 6 GB, disk: 8 GB)     |
| MySQL Proxy                   | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| MySQL Server                  | Automatic: 3 | Automatic: 100 GB    | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 64 GB)    |
| Backup Prepare Node           | Automatic: 1 | Automatic: 200 GB    | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Diego BBS                     | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| UAA                           | Automatic: 2 | None                 | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB)   |
| Cloud Controller              | Automatic: 2 | None                 | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB)   |
| HAProxy                       | Automatic: 1 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Router                        | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| MySQL Monitor                 | Automatic: 1 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Clock Global                  | Automatic: 1 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Cloud Controller Worker       | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Diego Brain                   | Automatic: 3 | Automatic: 1 GB      | Automatic: small (cpu: 1, ram: 2 GB, disk: 8 GB)          |
| Diego Cell                    | Automatic: 3 | None                 | Automatic: xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB) |
| Loggregator Trafficcontroller | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Syslog Adapter                | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Syslog Scheduler              | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Doppler Server                | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| TCP Router                    | Automatic: 1 | Automatic: 1 GB      | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| CredHub                       | Automatic: 2 | None                 | Automatic: large (cpu: 2, ram: 8 GB, disk: 16 GB)         |

4. To scale your deployment horizontally, increase the number of **Instances** of a job. See [Scaling Recommendations](#) for guidance about the number of job instances required to ensure high availability.

 **Note:** In PCF v1.12, you cannot scale the Autoscaler job to greater than one instance.

5. To scale your deployment vertically, adjust the **Persistent Disk Type** and **VM Type** of a job to allocate more disk space and memory. If you choose **Automatic** from the dropdown, PAS uses the recommended amount of resources for the job.
6. Click **Save**.
7. Return to the **Installation Dashboard** and click **Apply Changes**.

## Scaling Down PAS

If you are deploying a PCF configuration that does not need to be highly available, Pivotal recommends scaling down job instances to the minimum number required for a functional deployment.

To scale down your deployment, do the following:

1. Navigate to the Pivotal Cloud Foundry Operations Manager Installation Dashboard.
2. Click the PAS tile in the Installation Dashboard.
3. Select **Resource Config**.

| JOB                           | INSTANCES    | PERSISTENT DISK TYPE | VM TYPE                                                   |
|-------------------------------|--------------|----------------------|-----------------------------------------------------------|
| Consul                        | Automatic: 3 | Automatic: 1 GB      | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| NATS                          | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| File Storage                  | Automatic: 1 | Automatic: 100 GB    | Automatic: medium.mem (cpu: 1, ram: 6 GB, disk: 8 GB)     |
| MySQL Proxy                   | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| MySQL Server                  | Automatic: 3 | Automatic: 100 GB    | Automatic: large.disk (cpu: 2, ram: 8 GB, disk: 64 GB)    |
| Backup Prepare Node           | Automatic: 1 | Automatic: 200 GB    | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Diego BBS                     | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| UAA                           | Automatic: 2 | None                 | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB)   |
| Cloud Controller              | Automatic: 2 | None                 | Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB)   |
| HAProxy                       | Automatic: 1 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Router                        | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| MySQL Monitor                 | Automatic: 1 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Clock Global                  | Automatic: 1 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Cloud Controller Worker       | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Diego Brain                   | Automatic: 3 | Automatic: 1 GB      | Automatic: small (cpu: 1, ram: 2 GB, disk: 8 GB)          |
| Diego Cell                    | Automatic: 3 | None                 | Automatic: xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB) |
| Loggregator Trafficcontroller | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Syslog Adapter                | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Syslog Scheduler              | Automatic: 2 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| Doppler Server                | Automatic: 3 | None                 | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| TCP Router                    | Automatic: 1 | Automatic: 1 GB      | Automatic: micro (cpu: 1, ram: 1 GB, disk: 8 GB)          |
| CredHub                       | Automatic: 2 | None                 | Automatic: large (cpu: 2, ram: 8 GB, disk: 16 GB)         |

4. In the **Resource Config** screen, decrease the number of **Instances** for each job. Choose the suggested values outlined in [Scaling Recommendations](#), or in the [Scaling Recommendations for Specific Deployment Configurations](#) and click **Save**.
5. Return to the **Installation Dashboard** and click **Apply Changes**.

## Scaling Down Jobs with Persistent Disk

If you scale down or delete a job that uses persistent disk, PAS marks the disk as **orphaned**. Orphaned disks are not attached to any job, and PAS deletes them after five days.

Use the BOSH CLI to list and recover orphaned disks. Follow the instructions in the [Prepare to Use the BOSH CLI](#) section of the *Advanced Troubleshooting with the BOSH CLI* topic to log in to the BOSH Director, and then follow the procedures in [Orphaned Disks](#) in the BOSH documentation.

## Scaling Recommendations for Specific Deployment Configurations

If you use one of the following configurations, choose the values in the corresponding table to scale instances for your particular deployment:

- [Deployments Using External Databases](#)
- [Deployments Using Internal MySQL](#)
- [Deployments Using an External Blobstore](#)
- [Deployments Using External Load Balancers](#)

### Deployments Using External Databases

If you use an external database, you can scale down the instance counts for internal MySQL jobs.

Select the following values in the Resource Config:

| Job          | Instance Count |
|--------------|----------------|
| MySQL Server | 0              |
| MySQL Proxy  | 0              |


## Deployments Using Internal MySQL


If you use the internal MySQL database on a clean install, or on an upgrade from a configuration that previously used internal MySQL databases, you do not need to change the default values shown in the table below.

If you need to change back to this configuration, choose the values shown below in the Resource Config.

 **Note:** Changing back to this configuration deletes any data written to your other database option.

| Job          | Instance Count |
|--------------|----------------|
| MySQL Server | 3              |
| MySQL Proxy  | 2              |

 **Note:** Apps that do not use MySQL for PCF are not affected by the scaling process when you redeploy PAS. In addition, redeploying PAS with the MySQL cluster means that the PCF API will not be available for a brief period of time. For example, you are not able to push apps or query their state during this time.

 **Note:** For MySQL high availability, you need to configure an external load balancer. For more information about configuring a load balancer for MariaDB-based deployments, see the [Configure a Load Balancer](#) section of the *Installing MySQL for PCF* topic.

## Deployments Using an External Blobstore

If you use an external blobstore, choose the following value in the Resource Config:

| Job          | Instance Count |
|--------------|----------------|
| File Storage | 0              |

## Deployments Using External Load Balancers

If you use an external load balancer, choose the following values in the Resource Config:

| Job         | Instance Count |
|-------------|----------------|
| HAProxy     | 0              |
| Router      | ≥ 1            |
| Diego Brain | ≥ 1            |

For more information about configuring load balancers in the Resource Config section of PAS, see the [PAS installation topic for your IaaS](#).






- If you are modifying an existing Ops Manager installation, return to the Ops Manager Installation Dashboard and click **Apply Changes**.

After configuration, BOSH propagates your CA certificate to all application containers in your deployment. You can then push and pull images from your Docker registries.

## Use an IP Address Whitelist

If you choose not to provide a CA certificate, you must provide the IP address of your Docker registry.

 **Note:** Using a whitelist skips SSL validation. If you want to enforce SSL validation, enter the IP address of the Docker registry in the **No proxy** field described [below](#).

1. Navigate to the Ops Manager Installation Dashboard.
2. Click the **Pivotal Application Service** tile, and navigate to the **Application Containers** tab.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC
- ☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888

Docker Images Disk-Cleanup Scheduling on Cell VMs\*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) \*

10240

3. Select **Allow SSH access to app containers** to enable app containers to accept SSH connections. If you use a load balancer instead of HAProxy, you must open port `2222` on your load balancer to enable SSH traffic. To open an SSH connection to an app, a user must have Space Developer privileges for the space where the app is deployed. Operators can grant those privileges in Apps Manager or using the cf CLI.
4. For **Private Docker Insecure Registry Whitelist**, provide the hostname or IP address and port that point to your private Docker registry. For example, enter `198.51.100.1:80` or `mydockerregistry.com:80`. Enter multiple entries in a comma-delimited sequence. SSL validation is ignored for private Docker image registries secured with self-signed certificates at these locations.
5. Under **Docker Images Disk-Cleanup Scheduling on Cell VMs**, choose one of the options listed below. For more information about these options, see [Configuring Docker Images Disk-Cleanup Scheduling](#).
  - **Never clean up Cell disk-space**
  - **Routinely clean up Cell disk-space**
  - **Clean up disk-space once threshold is reached.** If you choose this option, enter the amount of disk space limit the Cell must reach before disk cleanup initiates under **Threshold of Disk-Used (MB)**.

6. Click **Save**.

7. Choose one of the following:

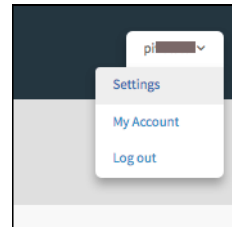
- If you are configuring Pivotal Application Service (PAS) for the first time, return to your specific IaaS installation instructions ([AWS](#), [Azure](#), [GCP](#), [OpenStack](#), [vSphere](#)) to continue the installation process.
- If you are modifying an existing PAS installation, return to the Ops Manager Installation Dashboard and click **Apply Changes**.

After configuration, PAS allows Docker images to pass through the specified IP address without checking certificates.

## Configure PCF to Access Proxies for Docker Registries

If you have proxies already set up for Docker registries, you should configure PCF to access your Docker registries through a proxy.

To configure PCF to access a Docker registry through a proxy, do the following:



1. On the Installation Dashboard, navigate to USERNAME > **Settings** > **Proxy Settings**.

2. On the **Update Proxy Settings** pane, complete one of the following fields:

- **HTTP proxy:** If you have an HTTP proxy server for your Docker registry, enter its IP address.
- **HTTPS proxy:** If you have an HTTPS proxy server for your Docker registry, enter its IP address.
- **No proxy:** If you do not use a proxy server, enter the IP address for the Docker registry. This field may already contain proxy settings for the BOSH Director.

Enter multiple IP addresses as a comma-separated list.

 A screenshot of the 'Update Proxy Settings' form within the Pivotal Settings panel. The left sidebar shows navigation options: 'Decryption Passphrase', 'Authentication Method', 'External API Access', 'Proxy Settings' (highlighted), 'Export Installation Settings', and 'Advanced'. The main content area is titled 'Update Proxy Settings' and contains three input fields: 'Http proxy' (with a placeholder 'Http proxy'), 'Https proxy' (with a placeholder 'Https proxy'), and 'No proxy' (containing the text '10.10.10.4, 10.10.10.5'). An 'Update' button is located at the bottom of the form.

3. Click **Update**.

4. Return to the Ops Manager dashboard and click **Apply Changes**.

## Configuring Cell Disk Cleanup Scheduling

Page last updated:

This topic describes how to configure disk cleanup scheduling on Diego cells in Pivotal Cloud Foundry (PCF).

### What is Disk Cleanup

PCF isolates application instances (AIs) from each other using containers that run inside Diego cells. Containers enforce a set of isolation layers including file system isolation. A PCF container file system can either be a PCF stack or the result of pulling a Docker image.

For performance reasons, the cells cache the Docker image layers and the PCF stacks used by running AIs. When PCF destroys an AI or reschedules an AI to a different cell, a chance exist that certain Docker image layers or an old PCF stack becomes unused. If PCF does not clean these unused layers, the cell ephemeral disk will slowly fill.

Disk cleanup is the process of removing unused layers from the cell disk. The disk cleanup process removes all unused Docker image layers and old PCF Stacks, regardless of their size or age.

To perform a detailed analysis of disk usage in your PAS deployment, see [Examining GrootFS Disk Usage](#).

### Options for Disk Cleanup

PCF provides the following options for scheduling the disk cleanup process on Diego cells:

- **Never clean up the Cell Disk:** Pivotal does not recommend using this option for production environments.
- **Routinely clean up the Cell Disk:** This option makes the cell schedule a disk cleanup whenever a container is created. Running the disk cleanup process this frequently can result in a negative impact on the cell performance.
- **Clean up Disk space once a threshold is reached:** This option makes the cell schedule the disk cleanup process only when a configurable disk space threshold is reached or exceeded.

See the [Configure Disk Cleanup Scheduling](#) section of this topic to select one of these options.

### Recommendations

Selecting the best option for disk cleanup depends on the workload that the Diego cells run.

For PCF installations that primarily run buildpack-based apps, Pivotal recommends selecting the **Routinely clean up Cell Disk space** option. The **Routinely clean up Cell Disk space** option ensures that when a new stack becomes available on a cell, the old stack is dropped immediately from the cache.

For PCF installations that primarily run Docker images, or both Docker images and buildpack-based apps, Pivotal recommends selecting the **Clean up Disk space once a threshold is reached** option with a reasonable threshold.

### Calculating a Threshold

To calculate a realistic value when configuring the disk cleanup threshold, you must identify some of the most frequently used Docker images in your PCF installation. Docker images tend to be constructed by creating layers over existing, base, images. In some cases, you may find it easier to identify which base Docker images are most frequently used.

Follow the steps below to calculate the disk cleanup threshold:

1. Identify the most frequently used Docker images or base Docker images.
2. Using the Docker CLI, measure the size of those images.

For example, you may determine the most frequently used images in a test deployment are `openjdk:7`, `nginx:1.13`, and `php:7-apache`. In this case, you can run the following commands to pull the identified images locally, then measure their sizes:

```
$> docker pull openjdk:7
$> docker pull nginx:1.13
$> docker pull php:7-apache
```

```
$> docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
php 7-apache 2720c02fc079 2 days ago 391 MB
openjdk 7 f45207c01009 5 days ago 586 MB
nginx 1.13 3448f27c273f 5 days ago 109 MB
...
```

3. Calculate the threshold as the sum of the frequently used image sizes plus a 15-20% buffer.

For example, using the output above, the sample threshold calculation is:  $(391 \text{ MB} + 586 \text{ MB} + 109 \text{ MB}) * 1.2 = 1303.2 \text{ MB}$

## Configure Disk Cleanup Scheduling

1. Navigate to the PCF Operations Manager **Installation Dashboard**.
2. Click the Pivotal Application Service (PAS) tile, and navigate to the **Application Containers** tab.

Enable microservice frameworks, private Docker registries, and other services that support your applications at a container level.

- ☒ Enable Custom Buildpacks
- ☒ Allow SSH access to app containers
- ☒ Enable SSH when an app is created
- ☒ Enable the GrootFS container image plugin for Garden RunC
- ☐ Router uses TLS to verify application identity

Private Docker Insecure Registry Whitelist

10.10.10.10:8888,example.com:8888

Docker Images Disk-Cleanup Scheduling on Cell VMs\*

- ☐ Never clean up Cell disk-space
- ☐ Routinely clean up Cell disk-space
- ☒ Clean up disk-space once threshold is reached

Threshold of Disk-Used (MB) (min: 1) \*

10240

3. Under **Docker Images Disk-Cleanup Scheduling on Cell VMs**, select an option.
4. If you select **Clean up Disk space once threshold is reached**, you must complete the **Threshold of Disk Used (MB)** field. Enter the disk space threshold amount in MB that you calculated for your deployment, as described in [Calculating a Threshold](#).
5. Click **Save**.

## Next Steps

If you are configuring PAS for the first time, return to your specific IaaS configuration to continue the installation process.

If you are modifying an existing PAS installation, return to the **PCF Ops Manager Installation Dashboard** and click **Apply Changes**.

## Custom Branding Apps Manager

This topic describes how Pivotal Cloud Foundry operators can visually brand Apps Manager by changing certain text, colors, and images of the interface. Developers view the customized interface when logging in, creating an account, resetting a password, or using Apps Manager.

Operators customize Apps Manager by configuring the **Custom Branding** and **Apps Manager Config** pages of the Pivotal Application Service (PAS) tile.

## Custom Branding Page

1. In a browser, navigate to the fully qualified domain name (FQDN) of your Ops Manager and log in.
2. Click **Pivotal Application Service**.
3. Click the **Custom Branding** tab.

Company Name

Defaults to 'Pivotal'

Accent Color

Enter a hexadecimal color code like '#71ffda'

Main Logo (PNGs only)

Enter a base64-encoded PNG image string, but leave out the mime-type (data:image/png;base64,) string. Only enter the base64 encoded data.

Square Logo (PNGs only)

Enter a base64-encoded PNG image string, but leave out the mime-type (data:image/png;base64,) string. Only enter the base64 encoded data.

Favicon (PNGs only)

Enter a base64-encoded PNG image string, but leave out the mime-type (data:image/png;base64,) string. Only enter the base64 encoded data.

Footer Text

Defaults to 'Pivotal Software Inc. All rights reserved.'

Footer Links

You may configure up to three links in the Apps Manager footer.

Classification Header/Footer Background Color

Enter a hexadecimal color code like '#71ffda'

Classification Header/Footer Text Color

Enter a hexadecimal color code like '#71ffda'

Classification Header Content

Plain text or HTML Markup

Classification Footer Content

Plain text or HTML Markup

Save



4. For **Company Name**, enter the name of your organization. If left blank, the name defaults to **Pivotal**.
5. For **Accent Color**, enter the hexadecimal code for the color used to accent various visual elements, such as the currently selected space in the sidebar. For example, `#71ffda`.
6. For **Main Logo**, enter a Base64-encoded URL string for a PNG image to use as your main logo. The image can be square or wide. For example, `data:image/png;base64,iVBORw0...`. If left blank, the image defaults to the Pivotal Logo.
7. For **Square Logo**, enter a Base64-encoded URL string for a PNG image to use in the Apps Manager header and in places that require a smaller logo. For example, `data:image/png;base64,iVBORw0...`. If left blank, the image defaults to the Pivotal Logo.
8. For **Favicon**, enter a Base64-encoded URL string for a PNG image to use as your favicon. For example, `data:image/png;base64,iVBORw0...`. If left blank, the image defaults to the Pivotal Logo.
9. For **Footer Text**, enter a string to be displayed as the footer. If left blank, the footer text defaults to **Pivotal Software Inc. All rights reserved..**
10. To add up to three footer links that appear to the right of the footer text, complete the following steps:
  - Click **Add**.
  - For **Link text**, enter a label for the link.
  - For **Url**, enter an external or relative URL. For example, `http://docs.pivotal.io` or `/tools.html`.
11. For special notification purposes such as governmental or restricted usage, use the Classification fields to create a special Header and Footer. Enter values in the following fields:
  - For **Classification Header/Footer Background Color**, enter the hexadecimal code for the desired background color of the header and footer.
  - For **Classification Header/Footer Text Color**, enter the hexadecimal code for the desired color of header and footer text.
  - For **Classification Header Content**, enter content for the header in either plain text or HTML. If you enter HTML content, eliminate white spaces and new lines. If you do not provide any content, the custom header will not appear.
  - For **Classification Footer Content**, enter content for the footer in either plain text or HTML. If you enter HTML content, eliminate white spaces and new lines. If you do not provide any content, the custom footer will not appear. The Classification footer appears below the normal footer, which you can customize in the **Footer Text** and **Footer Links** fields.



**Note:** The Header and Footer do not appear on the [User Account and Authentication \(UAA\)](#) login page.

## Apps Manager Config Page

1. In a browser, navigate to the fully qualified domain name (FQDN) of your Ops Manager and log in.
2. Click **Pivotal Application Service**.
3. Click the **Apps Manager Config** tab.

## Configure Apps Manager

☒ Enable Invitations
   
☐ Display Marketplace Service Plan Prices
   
 Supported currencies as JSON <sup>\*</sup>
  

{"usd": "\$", "eur": "€"}

  
Product Name
  
  
Marketplace Name
  
  

Customize Sidebar Links

Add

You may configure up to 10 links in the Apps Manager sidebar.

▶ Marketplace

▶ Docs

▶ Tools

  
Apps Manager Memory Usage (MB) ( min: 128 )
  
  
Invitations Memory Usage (MB) ( min: 256 )
  
  
Apps Manager Polling Interval <sup>\*</sup>
  


30

Apps manager polling interval in seconds. As a workaround to reduce load on the Cloud Controller API, increase the polling interval or set to 0 to stop polling. Values between 0 and 30 will default to 30 seconds.

Save


- For **Product Name**, enter text to replace **Apps Manager** in the header and the title of Apps Manager. This text defaults to **Apps Manager** if left blank.
- For **Marketplace Name**, enter text to replace the header in the Marketplace pages. This text defaults to **Marketplace** if left blank.
- By default, Apps Manager includes three sidebar links: **Marketplace**, **Docs**, and **Tools**. You can edit existing sidebar links by clicking the name of the link and editing the **Link text** and **Url** fields. Or, you can remove the link by clicking the trash icon next to its name. If you want to add a new sidebar link, click **Add** and complete the **Link text** and **Url** fields.

 **Note:** Removing any of the default links will remove them from the sidebar for all users.

- (Optional) Enter your desired **Apps Manager Memory Usage** in MBs. The minimum number you can enter is `128`.
- (Optional) Enter your desired **Invitations Memory Usage** in MBs. This is the memory limit used to deploy the Invitations app. The minimum number you can enter is `256`.
- The **Apps Manager Polling Interval** field provides a temporary fix if Apps Manager usage degrades Cloud Controller response times. In this case, you can use this field to reduce the load on the Cloud Controller and ensure Apps Manager remains available while you troubleshoot the Cloud

Controller. Pivotal recommends that you do not keep this field modified as a long term fix because it can degrade Apps Manager performance. You can optionally do the following:

- Increase the polling interval above the default of `30` seconds.

 **Note:** If you enter a value between `0` and `30`, the field is automatically set to `30`.

- Disable polling by entering `0`.

## Reporting App, Task, and Service Instance Usage

Page last updated:

This topic describes how to use the Cloud Foundry Command Line Interface (cf CLI) to retrieve historical system- and org-level usage information about your apps, tasks, and service instances through the Cloud Controller and Usage Service APIs.

Usage reports are compiled from the `/v2/app_usage_events` endpoint. For more information, see [List all App Usage Events](#) in the Cloud Foundry API documentation.

You can also access usage information by using Apps Manager. For more information, see the [Reporting Instance Usage with Apps Manager](#) topic.

To retrieve current app and event information from the Cloud Controller, see [Retrieving App and Event Information](#) in the open-source Cloud Foundry documentation.

## Obtain System Usage Information

You can obtain the following system usage information:

- [App Usage](#)
- [Task Usage](#)
- [Service Usage](#)

### App Usage

Use `curl` to make a request to `/system_report/app_usages` on the Usage Service endpoint to show system-wide app usage data:

```
$ curl "https://app-usage.YOUR-SYSTEM-DOMAIN/system_report/app_usages" -k -v \
-H "authorization: 'cf oauth-token'"
{
 "report_time": "2017-04-11 22:28:24 UTC",
 "monthly_reports": [
 {
 "month": 4,
 "year": 2017,
 "average_app_instances": 17855.256153713308,
 "maximum_app_instances": 18145,
 "app_instance_hours": 4686533.080277303
 }
]
 "yearly_reports": [
 {
 "year": 2017,
 "average_app_instances": 16184.9,
 "maximum_app_instances": 18145,
 "app_instance_hours": 39207433.0802773
 }
]
}
```

The following table describes the data generated by this report:

| Value                              | Calculation Method                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>app_instance_hours</code>    | The total number of hours app instances have been running on the foundation for the month or year.                                                                                                                                                                                                                                                                                                                      |
| <code>average_app_instances</code> | <p>The total <code>app_instance_hours</code> on the foundation for the month or year divided by the total hours for that time period.</p> <p><b>Example:</b> For the month of January, 100 apps run for 300 hours each, generating a value of 30000 for <code>app_instance_hours</code>. When divided by 744, the total number of hours in January, you get a value of 40.3 for <code>average_app_instances</code>.</p> |
| <code>maximum_app_instances</code> | The highest concurrent number of app instances running on the foundation for the month or year.                                                                                                                                                                                                                                                                                                                         |

## Task Usage

Use `curl` to make a request to `/system_report/task_usages` on the Usage Service endpoint to show system-wide task usage data:

```
$ curl "https://app-usage.YOUR-SYSTEM-DOMAIN/system_report/task_usages" -k -v \
-H "authorization: 'cf oauth-token'"
{
 "report_time": "2017-04-11T22:33:48.971Z",
 "monthly_reports": [
 {
 "month": 4,
 "year": 2017,
 "total_task_runs": 235,
 "maximum_concurrent_tasks": 7,
 "task_hours": 43045.201944444445
 }
]
 "yearly_reports": [
 {
 "year": 2017,
 "total_task_runs": 2894,
 "maximum_concurrent_tasks": 184,
 "task_hours": 45361.266944444445
 }
]
}
```

## Service Usage

Use `curl` to make a request to `/system_report/service_usages` on the Usage Service endpoint to show system-wide service usage data:

```
$ curl "https://app-usage.YOUR-SYSTEM-DOMAIN/system_report/service_usages" -k -v \
-H "authorization: 'cf oauth-token'"
{
 "report_time": "2017-05-11 18:29:14 UTC",
 "monthly_service_reports": [
 {
 "service_name": "fake-service-0507f1fd-2340-49a6-9d43-a347a5f5f6be",
 "service_guid": "177defde-cd51-4058-bd86-b98015c295f5",
 "usages": [
 {
 "month": 1,
 "year": 2017,
 "duration_in_hours": 0,
 "average_instances": 0,
 "maximum_instances": 0
 },
 {
 "month": 2,
 "year": 2017,
 "duration_in_hours": 0,
 "average_instances": 0,
 "maximum_instances": 0
 },
 {
 "month": 3,
 "year": 2017,
 "duration_in_hours": 4.182222222222227,
 "average_instances": 0,
 "maximum_instances": 2
 },
 {
 "month": 4,
 "year": 2017,
 "duration_in_hours": 2176.9622222222186,
 "average_instances": 3,
 "maximum_instances": 7
 },
 {
 "month": 5,
 "year": 2017,
 "duration_in_hours": 385.61388888888854,
 "average_instances": 1.5,
 "maximum_instances": 3
 }
],
 "plans": [
 {

```

```
"usages": [
 {
 "month": 1,
 "year": 2017,
 "duration_in_hours": 0,
 "average_instances": 0,
 "maximum_instances": 0
 },
 {
 "month": 2,
 "year": 2017,
 "duration_in_hours": 0,
 "average_instances": 0,
 "maximum_instances": 0
 },
 {
 "month": 3,
 "year": 2017,
 "duration_in_hours": 4.182222222222227,
 "average_instances": 0,
 "maximum_instances": 2
 },
 {
 "month": 4,
 "year": 2017,
 "duration_in_hours": 1465.6388888888941,
 "average_instances": 2,
 "maximum_instances": 5
 },
 {
 "month": 5,
 "year": 2017,
 "duration_in_hours": 385.61388888888854,
 "average_instances": 1.5,
 "maximum_instances": 3
 }
],
"service_plan_name": "fake-plan",
"service_plan_guid": "ac09f607-f4e5-4807-af16-e95856061bd7"
}
```

## Obtain Org Usage Information

You can obtain the following org usage information:

- [App Usage](#)
- [Task Usage](#)
- [Service Usage](#)

You must have the GUID of the org you want to obtain information about in order to perform the procedures in this section. To retrieve your org GUID, run the `cf org` command:

```
$ cf org YOUR-ORG --guid
```

## App Usage


Use `curl` to make a request to `/app_usages` on the Usage Service endpoint to show app usage in an org. You must complete the placeholders in `start=YYYY-MM-DD&end=YYYY-MM-DD` to define a date range.

```
$ curl "https://app-usage.YOUR-SYSTEM-DOMAIN/organizations/YOUR-ORG-GUID/app_usages?start=YYYY-MM-DD&end=YYYY-MM-DD" \
-k -v \
-H "authorization: `cf oauth-token`"
{
 "organization_guid": "8d83362f-587a-4148-806b-4407428887b5",
 "period_start": "2016-06-01T00:00:00Z",
 "period_end": "2016-06-13T23:59:59Z",
 "app_usages": [
 {
 space_guid: "44435fd6-fbac-5049-bbfc-92d1603a5e98"
 space_name: "outer-space"
 app_guid: "00ecd7ce-1dd0-4b3f-63b9-744c9de42afc"
 app_name: "your-app"
 instance_count: 6
 memory_in_mb_per_instance: 64
 duration_in_seconds: 76730
 }
]
}
```

## Task Usage

Use `curl` to make a request to `/task_usages` on the Usage Service endpoint to show task usage in an org. You must complete the placeholders in `start=YYYY-MM-DD&end=YYYY-MM-DD` to define a date range.

```
$ curl "https://app-usage.YOUR-SYSTEM-DOMAIN/organizations/YOUR-ORG-GUID/task_usages?start=YYYY-MM-DD&end=YYYY-MM-DD" \
-k -v \
-H "authorization: `cf oauth-token`"
{
 "organization_guid": "8f88362f-547c-4158-808b-4605468387d5",
 "period_start": "2014-01-01",
 "period_end": "2017-04-04",
 "spaces": {
 "e6445eb3-fdac-4049-bafc-94d1703d5e78": {
 "space_name": "smoketest",
 "task_summaries": [
 {
 "parent_application_guid": "04cd29d5-1f9e-4900-ac13-2e903f6582a9",
 "parent_application_name": "task-dummy-app",
 "memory_in_mb_per_instance": 256,
 "task_count_for_range": 54084,
 "concurrent_task_count_for_range": 5
 "total_duration_in_seconds_for_range": 37651415
 },
]
 },
 "b66665e4-873f-4482-acf1-89307ba9c6e4": {
 "space_name": "smoketest-experimental",
 "task_summaries": [
 {
 "parent_application_guid": "d941b689-4a27-44ec-91d3-1f97434dbed9",
 "parent_application_name": "console-blue",
 "memory_in_mb_per_instance": 256,
 "task_count_for_range": 14,
 "concurrent_task_count_for_range": 2
 "total_duration_in_seconds_for_range": 20583
 }
]
 }
]
}
```

 **Note:** In the `/task_usages` endpoint, `memory_in_mb_per_instance` is the memory of the task.

## Service Usage

Use `curl` to make a request to `/service_usages` on the Usage Service endpoint to show service usage in an org. You must complete the placeholders in `start=YYYY-MM-DD&end=YYYY-MM-DD` to define a date range.

```
$ curl "https://app-usage.YOUR-SYSTEM-DOMAIN/organizations/cf org YOUR-ORG --guid/service_usages?start=YYYY-MM-DD&end=YYYY-MM-DD" -k -v -H "authorization: `cf oauth`"
{
 "organization_guid": "8d83362f-587a-4148-806b-4407428887b5",
 "period_start": "2016-06-01T00:00:00Z",
 "period_end": "2016-06-13T23:59:59Z",
 "service_usages": [
 {
 deleted: false
 duration_in_seconds: 1377982.52
 service_guid: "02802293-b769-44cc-807f-eee331ba9b2b"
 service_instance_creation: "2016-01-20T18:48:16.000Z"
 service_instance_deletion: null
 service_instance_guid: "b25b4481-19aa-4504-82c9-f303e7e9ed6e"
 service_instance_name: "something-usage-db"
 service_instance_type: "managed_service_instance"
 service_name: "my-mysql-service"
 service_plan_guid: "70915a70-7311-4f3e-ab0d-4a7dfd3ef2d9"
 service_plan_name: "20gb"
 space_guid: "e6445eb3-fdac-4049-bafc-94d1703d5e78"
 space_name: "outer-space"
 }
]
}
```

## Example: Autogenerated Database Usage Reports

For security compliance and recordkeeping, some PCF customers create Concourse CI/CD pipelines that regularly run JavaScript scripts to do the following:

1. Call the `app-usage` APIs in the above sections of this topic, as well as the [Security Event Logging](#) topic, to collect data about service instances from a PCF foundation. This data includes database instance information such as tile or database type, database creator, and date of creation or deletion.
2. Merge and format the data about services instances into a JSON output file and save it to an S3 bucket.
3. Input the file to another process that does the following:
  - a. Parses the data
  - b. Eliminates duplicate entries from previous reports
  - c. Sends the data to a database compliance system through APIs



## Reporting Instance Usage with Apps Manager

Page last updated:

This topic describes how to retrieve app, task, and service instance usage information using Apps Manager.

You can also retrieve app, task, and service instance usage information using the Usage service API, or the [Cloud Foundry API](#) from the Cloud Foundry Command Line Interface (cf CLI). For more information, see the [Monitoring App, Task, and Service Instance Usage](#) topic.

There are two ways to monitor app, task, and service instance usage from Apps Manager. The Accounting Report provides a summarized report, and the Usage Report provides a more detailed view of the data.

### View the Accounting Report

The Accounting Report displays instance usage information for all orgs in your [Pivotal Cloud Foundry](#) (PCF) deployment except the **system** org. The Accounting Report provides a high-level overview of your usage by displaying your monthly count of app, task, and service instances.

Follow the steps below to access the Accounting Report.

1. [Log into the Apps Manager](#) as an admin.
2. From the left navigation of Apps Manager, select **Accounting Report**.
3. Under **App Statistics** and **Service Usage**, view the average and maximum instances in use per month.

**Max Concurrent** displays the largest number of instances in use at a time over the indicated time period. The Accounting Report calculates these values from the `start`, `stop`, and `scale` app usage events in Cloud Controller.

| Accounting Report                                                                 |      |         |          |       |       |
|-----------------------------------------------------------------------------------|------|---------|----------|-------|-------|
| Monthly count of App Instances in use for all orgs (not including the system org) |      |         |          |       |       |
| APP STATISTICS                                                                    | 2017 | JANUARY | FEBRUARY | MARCH | APRIL |
| Avg Instances                                                                     | 0.0  | 0       | 0        | 0.0   | -     |
| Max Concurrent                                                                    | 2.0  | 0       | 0        | 2.0   | -     |
| Apps                                                                              | 2.0  | 0       | 0        | 2.0   | -     |
| Tasks                                                                             | 0.0  | 0       | 0        | 0.0   | -     |
| Instance Hours                                                                    | 0.0  | 0       | 0        | 0.0   | -     |
| Apps                                                                              | 0.0  | 0       | 0        | 0.0   | -     |
| Tasks                                                                             | 0.0  | 0       | 0        | 0.0   | -     |
| SERVICE USAGE                                                                     | 2017 | JANUARY | FEBRUARY | MARCH | APRIL |

### View the Usage Report

The Usage Report provides a more granular view of your usage by detailing app, task, and service instance usage information for all spaces in a particular org, excluding the **system** org.

Follow the steps below to access the Usage Report.

1. [Log into the Apps Manager](#) as an admin, or as an account with the **Org Manager** or **Org Auditor** role. For more information about managing roles, see the [Managing User Accounts and Permissions Using the Apps Manager](#) topic.
2. From the dropdown on the left, select the org for which you want to view a usage report.

3. Click **Usage Report** in the upper right.

ORG

My-Org

QUOTA

1.37 GB / 10 GB

14%

Usage Report

Spaces (3)

Domains (2)

Members (8)

Settings

The top of the Usage Report displays total **App + Task Instance Hours**, **App + Task Memory**, and **Service Instance Hours** by all spaces in the org.

Usage Report

Period

May 1st - Current

DOWNLOAD ZIP

Org

My-Org

App + Task Instance Hours

576.7 hrs

App + Task Memory

111.4 GB hrs

Service Instance Hours

486.7 hrs

The report provides total usage information for each of your spaces.

|                    |                           |                   |                        |
|--------------------|---------------------------|-------------------|------------------------|
| <div>+</div> Space | App + Task Instance Hours | App + Task Memory | Service Instance Hours |
| development        | 74.1 hrs                  | 74.1 GB hrs       | 120.1 hrs              |
| <div>+</div> Space | App + Task Instance Hours | App + Task Memory | Service Instance Hours |
| production         | 0.0 hrs                   | 0.0 GB hrs        | 120.0 hrs              |
| <div>+</div> Space | App + Task Instance Hours | App + Task Memory | Service Instance Hours |
| staging            | 0.0 hrs                   | 0.0 GB hrs        | 0.0 hrs                |

To display more detailed information about app, task, and service instance usage in a space, click the name of the space for an expanded view.

|                         |                           |     |                         |       |                        |            |
|-------------------------|---------------------------|-----|-------------------------|-------|------------------------|------------|
| <div>•</div> Space      | App + Task Instance Hours |     | App + Task Memory       |       | Service Instance Hours |            |
| development             | 74.1 hrs                  |     | 74.1 GB hrs             |       | 120.1 hrs              |            |
| Apps(1)                 | App Instance Count (#)    |     | Task Instance Count (#) |       | Instance Time (hrs)    |            |
|                         | Avg                       | Max | Max Concurrent          | Total | App Total              | Task Total |
| spring-music-sample-app | 0.2                       | 1   | 1                       | 3     | 74.0                   | 0.0        |
| Services (1)            | Plan                      |     | Instance Hours          |       |                        |            |
| app-autoscaler (1)      |                           |     | 120.1                   |       |                        |            |
| my-autoscaler           | standard                  |     | 120.1                   |       |                        |            |

## Providing a Certificate for Your TLS Termination Point

Page last updated:


This topic describes how to configure Transport Layer Security (TLS) termination for HTTP traffic in Pivotal Application Service (PAS) with a TLS certificate, as part of the process of configuring PAS for deployment.

### Configure TLS Termination

When you deploy PCF, you must configure the TLS termination for HTTP traffic in your PAS configuration. You can terminate TLS at all of the following points:

- Load Balancer
- Load Balancer and Gorouter
- Gorouter

Follow the guidance in [Securing Traffic into Cloud Foundry](#) to choose and configure the TLS termination option for your deployment.

 **Note:** If you are using HAProxy in a PCF deployment, you can choose to terminate SSL/TLS at HAProxy in addition to any of the SSL/TLS termination options above. For more information, see [Configuring SSL/TLS Termination at HAProxy](#).

### Obtain TLS Certificates

To secure traffic into PCF, you must obtain at least one TLS certificate. See [Certificate Requirements](#) for general certificate requirements for deploying PCF.

See the following sections for additional IaaS-specific certificate requirements:

- **AWS:** [Certificate Requirements on AWS](#)
- **GCP:** [Certificate Requirements on GCP](#)

### Creating a Wildcard Certificate for PCF Deployments

This section describes how to create or generate a certificate for your PAS environment. If you are deploying to a production environment, you should obtain a certificate from a trusted authority (CA).

For internal development or testing environments, you have two options for creating a required TLS certificates.

- You can create a self-signed certificate, or
- You can have [PAS generate the certificate](#) for you.

To create a certificate, you can use a wide variety of tools including OpenSSL, Java's keytool, Adobe Reader, and Apple's Keychain to generate a Certificate Signing Request (CSR).

In either case for either self-signed or trusted single certificates, apply the following rules when creating the CSR:

- Specify your registered wildcard domain as the `Common Name`. For example, `*.yourdomain.com`.
- If you are using a split domain setup that separates the domains for `apps` and `system` components (recommended), then enter the following values in the `Subject Alternative Name` of the certificate:
  - `*.apps.yourdomain.com`
  - `*.system.yourdomain.com`
  - `*.login.system.yourdomain.com`
  - `*.uaa.system.yourdomain.com`
- If you are using a single domain setup, then use the following values as the `Subject Alternative Name` of the certificate:
  - `*.login.system.yourdomain.com`

- o \*.uaa.system.yourdomain.com

**Note:** TLS certificates generated for wildcard DNS records only work for a single domain name component or component fragment. For example, a certificate generated for \*.EXAMPLE.com does not work for \*.apps.EXAMPLE.com and \*.system.EXAMPLE.com. The certificate must have both \*.apps.EXAMPLE.com and \*.system.EXAMPLE.com attributed to it.

## Generating a RSA Certificate in PAS

1. Navigate to the Ops Manager Installation Dashboard.
2. Click the **Pivotal Application Service** tile in the Installation Dashboard.
3. Click **Networking**.
4. Click **Generate RSA Certificate** to populate the **Certificate and Private Key for HAProxy and Router** fields with RSA certificate and private key information.
5. If you are using a split domain setup that separates the domains for **apps** and **system** components (recommended), then enter the following domains for the certificate:

- o \*.yourdomain.com
- o \*.apps.yourdomain.com
- o \*.system.yourdomain.com
- o \*.login.system.yourdomain.com
- o \*.uaa.system.yourdomain.com

For example, \*.example.com, \*.apps.example.com, \*.system.example.com, \*.login.system.example.com, \*.uaa.system.example.com

**Generate RSA Certificate**

Example: \*.app.domain.com, \*.system.domain.com, my.webapp.com, \*.domain.com \*

Cancel

Generate


## Enabling NFS Volume Services

This topic describes how Pivotal Cloud Foundry (PCF) operators can deploy NFS volume services.

### Overview

A volume service gives apps access to a persistent filesystem, such as NFS. By performing the procedures in this topic, operators can add a volume service to the [Marketplace](#) that provides an NFSv3 filesystem.

Developers can then use the [Cloud Foundry Command Line Interface](#) (cf CLI) to create service instances of the volume service and bind them to their apps. For more information, see the [Using an External File System \(Volume Services\)](#) topic.

 **Note:** You must have an NFS server running to enable NFS volume services. If you want to use NFS and do not currently have a server available, you can [deploy the test NFS server](#) bundled with the NFS Volume release or enable NFS volume services with the NFS Broker Errand for Pivotal Application Service. You can enable this errand during PAS configuration.

### Security

When it comes to securing your NFS server against traffic apps running on PCF, you can use ASGs and LDAP:


- **Application Security Groups (ASGs)**  
Use Application Security Groups (ASGs) to prevent apps from sending traffic directly to your NFS ports. Apps should never need to use NFS ports directly. Pivotal recommends defining an ASG that blocks direct access to your NFS server IP, especially ports 111 and 2049. For more information on setting up ASGs, see [Application Security Groups](#).
- **LDAP**  
In addition to ASGs, LDAP secures the NFS volume service so that app developers cannot bind to the service using an arbitrary UID and gain access to sensitive data. With LDAP support enabled, app developers must provide credentials for any user they wish to bind as.

The Diego cells running on PCF must be able to reach your LDAP server on the port you use for connections, which are typically 389 or 636. You cannot limit which Diego cells have access to your NFS or LDAP servers.

## Enable Volume Services

To enable NFS volume services in PCF, do the following:

1. Navigate to the Ops Manager Installation Dashboard.
2. Click the **Pivotal Application Service** tile.
3. Click **Application Containers**.
4. Under **Enabling NFSv3 volume services**, select **Enable**.

 **Note:** In a clean install, NFSv3 volume services are enabled by default. In an upgrade, NFSv3 volume services match the setting of the previous deployment.

Enabling NFSv3 volume services will allow application developers to bind existing NFS volumes to their applications for shared file access. \*

☒ Enable

LDAP Service Account User

LDAP Service Account Password

LDAP Server Host

LDAP Server Port

LDAP User Fully-Qualified Domain Name

☐ Disable

☒ Enable the GrootFS container image plugin for Garden RunC

**Save**

5. (Optional) To configure LDAP for NFSv3 volume services, perform the following steps:

**Note:** If you already use an LDAP server with your network-attached storage (NAS) file server, enter its information below. This ensures that the identities known to the file server match those checked by the PCF NFS driver.

- For **LDAP Service Account User**, enter either the full domain name (DN) for the service account or the username of the service account that manages volume services, depending on how your LDAP server is configured. This value needs to be exactly what you would enter when binding the account to your LDAP server.
- For **LDAP Service Account Password**, enter the password for the service account.
- For **LDAP Server Host**, enter the hostname or IP address of the LDAP server.
- For **LDAP Server Port**, enter the LDAP server port number. If you do not specify a port number, Ops Manager uses 389.
- For **LDAP User Fully-Qualified Domain Name**, enter the full DN to the base organizational unit (OU) where your users exist in the LDAP tree. The NFS driver searches for users in this OU and the subtree beneath it using the search filter `(&(objectClass=User)(cn=USERNAME))`. This filter is not configurable.  
For example, if your users belong to an OU `users` and your domain is `example.com`, the full DN to enter would be:  
`OU=users,DC=example,DC=com`.

6. Click **Save**.

7. Return to the Ops Manager Installation Dashboard and click **Apply Changes** to redeploy.

8. Using the cf CLI, enable access to the service:

```
$ cf enable-service-access nfs
```

To limit access to a specific org, use the `-o` flag, followed by the name of the org where you want to enable access. For more information, see the [Access Control](#) topic.

9. (Optional) Enable access to the `nfs-experimental` service. See [NFS Volume Service](#) for details about the differences between the two `nfs` services.

```
$ cf enable-service-access nfs-experimental
```

After completing these steps, developers can use the cf CLI to create service instances of the `nfs` service and bind them to their apps.



## Rotating Runtime CredHub Encryption Keys

Page last updated:

This topic discusses how to rotate runtime CredHub encryption keys. Encryption keys are values that CredHub uses to obscure stored secrets. When an operator marks an additional key as primary, CredHub can rotate in that additional key as the encryption key.

During this credential rotation process, the initial encryption key is used to access the hidden value, That value is then stored again by the additional encryption key.

**⚠ warning:** If you remove an encryption key and click **Apply Changes** before the rotation completes, the deployment breaks. If this happens, you can no longer access data stored with the deleted key.

## Rotate PAS Encryption Keys

To rotate PAS encryption keys, do the following:

1. Navigate to the **Ops Manager Installation Dashboard**.
2. Click the **Pivotal Application Service** tile.
3. Select the **CredHub** tab.

Encryption Keys

Add

Name \*

Key \*

Secret

☐ Primary

Name of the encryption key.

4. In the **Encryption Keys** section, click **Add**.
5. For **Name**, enter the name of your new encryption key.
6. For **Key**, enter your new encryption key.
7. Select the **Primary** check box.
8. Click **Save**.
9. Navigate to the **Ops Manager Installation Dashboard**.
10. Click **Apply Changes**.

## Verify PAS Encryption Key Rotation

To verify that the rotation completes, do the following:

1. Click the **Pivotal Application Service** tile.
2. Select the **Status** tab.
3. Within the **CredHub** job, locate **Index 0**.



| JOB                           | INDEX | IPS       | AZ            | CID                                     | LOAD AVG15 | CPU  | MEMORY | SWAP | SYSTEM DISK | EPHEM. DISK | PERS. DISK | LOGS |
|-------------------------------|-------|-----------|---------------|-----------------------------------------|------------|------|--------|------|-------------|-------------|------------|------|
| Consul                        | 0     | 10.0.4.5  | us-central1-a | vm-dca0a175-3a56-4cb0-6b64-2d3f0a39ddc7 | 0.00       | 1.2% | 14%    | 0%   | 40%         | 3%          | 3%         |      |
| NATS                          | 0     | 10.0.4.6  | us-central1-a | vm-a5b7a6e3-d80d-44d2-54cc-a160d3f66916 | 0.00       | 1.1% | 14%    | 0%   | 40%         | 3%          | N/A        |      |
| File Storage                  | 0     | 10.0.4.7  | us-central1-a | vm-c4aa5642-54f9-436e-5c31-03b2607de077 | 0.00       | 1.0% | 4%     | 0%   | 40%         | 7%          | 3%         |      |
| MySQL Proxy                   | 0     | 10.0.4.8  | us-central1-a | vm-c6df54cc-128c-440b-4835-e2826b9502be | 0.00       | 0.3% | 15%    | 0%   | 40%         | 4%          | N/A        |      |
| MySQL Server                  | 0     | 10.0.4.9  | us-central1-a | vm-5ec3aa62-f066-42e0-60ec-ce4464cfd628 | 0.08       | 1.1% | 24%    | 0%   | 40%         | 3%          | 5%         |      |
| Backup Prepare Node           | 0     | 10.0.4.10 | us-central1-a | vm-55e93a88-ce00-4519-4cbb-39b12bd82495 | 0.00       | 0.3% | 19%    | 0%   | 40%         | 20%         | 0%         |      |
| Diego BBS                     | 0     | 10.0.4.11 | us-central1-a | vm-c95a4858-b9fb-460e-4693-1dfd1f3be88d | 0.03       | 1.1% | 20%    | 0%   | 40%         | 5%          | N/A        |      |
| UAA                           | 0     | 10.0.4.12 | us-central1-a | vm-9f5c1fdc-704e-484c-7e89-58c95a19a319 | 0.02       | 0.6% | 20%    | 0%   | 40%         | 3%          | N/A        |      |
| Cloud Controller              | 0     | 10.0.4.13 | us-central1-a | vm-6ec5f788-a390-45ed-4990-9cbd3f6ae6e6 | 0.07       | 1.0% | 27%    | 0%   | 40%         | 16%         | N/A        |      |
| HAProxy                       | 0     | 10.0.4.14 | us-central1-a | vm-9466dc03-d2bc-48f0-401b-d9082e0f8778 | 0.00       | 0.5% | 14%    | 0%   | 40%         | 3%          | 40%        |      |
| Router                        | 0     | 10.0.4.15 | us-central1-a | vm-32ba827f-564b-4462-7b20-46a658a8e8df | 0.00       | 1.2% | 16%    | 0%   | 40%         | 4%          | N/A        |      |
| MySQL Monitor                 | 0     | 10.0.4.16 | us-central1-a | vm-98c9c06c-e381-455f-517c-62e9ad9d70d1 | 0.00       | 0.2% | 11%    | 0%   | 40%         | 2%          | N/A        |      |
| Clock Global                  | 0     | 10.0.4.17 | us-central1-a | vm-65a93076-941e-4b4c-50a2-e067bfe2d0ed | 0.00       | 0.3% | 41%    | 1%   | 40%         | 86%         | N/A        |      |
| Cloud Controller Worker       | 0     | 10.0.4.18 | us-central1-a | vm-de45f832-e290-4e38-7692-236fa5b417d5 | 0.00       | 1.1% | 48%    | 1%   | 40%         | 9%          | N/A        |      |
| Diego Brain                   | 0     | 10.0.4.19 | us-central1-a | vm-247bcbf3-9241-49df-57fd-7c34d8bb9fef | 0.00       | 0.4% | 9%     | 0%   | 41%         | 6%          | 0%         |      |
| Diego Cell                    | 0     | 10.0.4.20 | us-central1-a | vm-99761423-b711-4871-7aa9-848537f5096e | 0.07       | 0.6% | 12%    | 0%   | 40%         | 8%          | N/A        |      |
| Loggregator Trafficcontroller | 0     | 10.0.4.21 | us-central1-a | vm-37c47f42-f226-4728-6acc-d4351a7d06cc | 0.00       | 1.4% | 18%    | 0%   | 40%         | 4%          | N/A        |      |
| Syslog Adapter                | 0     | 10.0.4.22 | us-central1-a | vm-9c577460-1a29-4741-7a0b-e70d6d93b286 | 0.00       | 1.1% | 14%    | 0%   | 40%         | 3%          | N/A        |      |
| Syslog Scheduler              | 0     | 10.0.4.23 | us-central1-a | vm-43a14a07-aaae-466d-6839-23767c3ce141 | 0.00       | 0.4% | 14%    | 0%   | 40%         | 3%          | N/A        |      |
| Doppler Server                | 0     | 10.0.4.24 | us-central1-a | vm-66359c07-0ef4-4a42-542c-2e7cee9e4be5 | 0.05       | 1.5% | 19%    | 0%   | 40%         | 4%          | N/A        |      |
| CredHub                       | 0     | 10.0.4.25 | us-central1-a | vm-84b31970-374a-4e0c-411c-3977b6a20ff1 | 0.00       | 0.2% | 12%    | 0%   | 40%         | 7%          | N/A        |      |
|                               | 1     | 10.0.4.26 | us-central1-b | vm-b67b89d6-0415-4021-7950-48c6c3aa2b14 | 0.00       | 0.2% | 12%    | 0%   | 40%         | 7%          | N/A        |      |

- Within the **Logs** column, click the correlating download icon.
- Select the **Logs** tab.
- Click the corresponding link to the retrieve the downloaded log file.
- Unzip the log file.
- Unzip the larger of the two nested directories.
- Ops Manager generates a compressed file for each CredHub VM that exists on your deployment. Unzip each of these compressed files.
- Open the `credhub` directory.
- Open the `credhub.log` file. If the PAS credential rotation completed successfully, the CredHub log contains the following string: `Successfully rotated NUMBER-OF-CREDENTIALS items`
- Remove the old encryption key.
- Click the trashcan icon that corresponds to the old encryption key.
- Click **Save**.
- Navigate to the **Ops Manager Installation Dashboard**.
- Click **Apply Changes**.

## Administrating PAS

This documentation describes administrating Pivotal Application Service (PAS). This includes procedures specific to managing the runtime, such as creating user accounts, modifying quota plans, and managing isolation segments.

See the following topics:

- [Managing the Runtime](#)
- [User Accounts and Communications](#)
- [Routing](#)
- [Isolation Segments](#)

## Managing the Runtime

The following topics provide information about managing Pivotal Application Service (PAS):

- [Stopping and Starting Virtual Machines](#)
- [Creating and Modifying Quota Plans](#)
- [Using Feature Flags](#)
- [Examining GrootFS Disk Usage](#)
- [Managing Custom Buildpacks](#)
- [Using Docker in Cloud Foundry](#)

## Stopping and Starting Virtual Machines

Page last updated:

*This topic assumes you are using [BOSH CLI version 2](#).*

This topic describes stopping and starting the component virtual machines (VMs) that make up a Pivotal Cloud Foundry (PCF) deployment.

In some cases you may want to stop all your VMs (for example, power down your deployment) or start all of your PAS VMs (for example, recover from a power outage.) You can stop or start all PAS VMs with a single `bosh` command.

If you want to shut down or start up a single VM in your deployment, you can use the [manual process](#) described on this page.

This procedure uses the BOSH Command Line Interface (BOSH CLI). See [Advanced Troubleshooting with the BOSH CLI](#) for more information about using this tool.

## Stopping and Starting All PAS VMs

This section describes how to stop and start all the VMs in your deployment.

### Stopping All PAS VMs

To shut down all the VMs in your deployment, perform the following steps:

1. Scale down the following jobs to one instance:
  - `consul_server`
  - `mysql`
2. Run the following command for each of the deployments listed in the previous step:

```
bosh -e MY-ENV -d MY-DEPLOYMENT stop --hard
```

Replace the text above with the following:

- `MY-ENV`: the alias you set for the BOSH Director.
- `MY-DEPLOYMENT`: the name of your deployment.

For example:

```
$ bosh -e prod -d mysql stop --hard
```

This command stops all VMs in the specified deployment. The `--hard` flag instructs BOSH to delete the VMs but retain any persistent disks.

### Starting All PAS VMs

Perform the following steps to start all the VMs in your deployment:

1. Select the product deployment for the VMs you want to shut down. You can run the following command to locate CF deployment manifests:

```
$ find /var/tempest/workspaces/default/deployments -name cf-*.yaml
```

2. Run the following command:

```
bosh -e MY-ENV -d MY-DEPLOYMENT start
```

Replace the text above with the following:

- `MY-ENV`: the alias you set for the BOSH Director.
- `MY-DEPLOYMENT`: the name of your deployment.

For example:

```
$ bosh -e prod -d mysql start
```

This command starts all VMs in the specified deployment.

3. If you require [high availability](#) in your deployment, scale up all instance groups to the original or desired counts.

## Stopping and Starting Individual PAS VMs

This section describes how to stop and start individual VMs in your deployment.

### Find the Names of Your PAS Virtual Machines

You need the full names of the VMs to stop and start them using the BOSH CLI. To find full names for the VMs running each component, run

```
bosh -e MY-ENV instances
```

, replacing `MY-ENV` with the alias you set for your BOSH Director. To filter the list of instances by deployment, run

```
bosh -e MY-ENV -d MY-DEPLOYMENT instances
```

For example:

```
$ bosh -e prod -d mysql instances
...
Deployment 'mysql'

Instance Process State AZ IPs
mysql/0123-abcd-4567ef89 running - 10.244.0.6
mysql/abcd-0123-ef4567ab running - 10.244.0.2

2 instances
...
```

You can see the full name of each VM in the `Instance` column of the terminal output. Each full name includes:

- A prefix indicating the component function of the VM.
- An identifier string specific to the VM.

For any component, you can look for its prefix in the `bosh instances` output to find the full name of the VM or VMs that run it.

### Stopping an Individual PAS VM

To stop a job, run the following command for the component in your PAS deployment, replacing `MY-ENV` with the alias you set for your BOSH Director and `MY-DEPLOYMENT` with the name of the deployment:

```
bosh -e MY-ENV -d MY-DEPLOYMENT stop VM-NAME
```

To delete the instance that contains the job, run the following command for the component in your PAS deployment:

```
bosh -e MY-ENV -d MY-DEPLOYMENT stop VM-NAME --hard
```

Use the full name of the component VM as listed in your `bosh instances` [terminal output](#) without the unique identifier string.

For example, the following command stops the Loggregator Traffic Controller job:

```
$ bosh -e prod -d loggregator stop loggregator_trafficcontroller
```

To stop a specific instance of a job, include the identifier string at the end of its full name.

For example, the following command stops the Loggregator Traffic Controller job on only one Diego cell instance:

```
$ bosh -e prod -d loggregator stop loggregator_trafficcontroller/0123-abcd-4567ef89
```

To delete the VM, include `--hard` at the end of the command. This command does not delete persistent disks.

For example, the following command deletes a specific Loggregator Traffic Controller instance:

```
$ bosh -e prod -d loggregator stop loggregator_trafficcontroller/0123-abcd-4567ef89 --hard
```

## Starting an Individual PAS VM

Run the following command for the component in your PAS deployment you wish to start, replacing `MY-ENV` with the alias you set for your BOSH Director and `MY-DEPLOYMENT` with the name of the deployment. Use the full name of the component VM as listed in your `bosh vms` [terminal output](#) without the unique identifier string.

```
bosh -e MY-ENV -d MY-DEPLOYMENT start VM-NAME
```

The following example command starts the Loggregator Traffic Controller VM:

```
$ bosh -e prod -d loggregator start loggregator_trafficcontroller
```

To start a specific instance of a VM, include the identifier string at the end of its full name.

For example, the following command starts the Loggregator Traffic Controller job on one Diego cell instance:

```
$ bosh -e prod -d loggregator start loggregator_trafficcontroller/0123-abcd-4567ef89
```

## Creating and Modifying Quota Plans

Page last updated:

Quota plans are named sets of memory, service, and instance usage quotas. For example, one quota plan might allow up to 10 services, 10 routes, and 2 GB of RAM, while another might offer 100 services, 100 routes, and 10 GB of RAM. Quota plans have user-friendly names, but are referenced in Cloud Foundry (CF) internal systems by unique GUIDs.

Quota plans are not directly associated with user accounts. Instead, every org has a list of available quota plans, and the account admin assigns a specific quota plan from the list to the org. Everyone in the org shares the quotas described by the plan. There is no limit to the number of defined quota plans an account can have, but only one plan can be assigned at a time.

You must set a quota plan for an [org](#), but you can choose whether to set a [space](#) quota.

### Org Quota Plan Attributes


| Name                       | Description                                                                                                                                                                                                              | Valid Values                                                                                                 | Example Value |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|---------------|
| name                       | The name you use to identify the plan                                                                                                                                                                                    | A sequence of letters, digits, and underscore characters. Quota plan names within an account must be unique. | silver_quota  |
| memory_limit               | Maximum memory usage allowed                                                                                                                                                                                             | An integer and a unit of measurement like M, MB, G, or GB                                                    | 2048M         |
| app_instance_limit         | Maximum app instances allowed.<br><br>Stopped apps do not count toward this instance limit. Crashed apps count toward the limit because their desired state is <code>starting</code> .                                   | An integer                                                                                                   | 25            |
| non_basic_services_allowed | Determines whether users can provision instances of non-free service plans. Does not control plan visibility. When false, non-free service plans may be visible in the marketplace but instances can not be provisioned. | <code>true</code> or <code>false</code>                                                                      | true          |
| total_routes               | Maximum routes allowed                                                                                                                                                                                                   | An integer                                                                                                   | 500           |
| total_reserved_route_ports | Maximum routes with reserved ports                                                                                                                                                                                       | An integer not greater than <code>total_routes</code>                                                        | 60            |
| total_services             | Maximum services allowed                                                                                                                                                                                                 | An integer                                                                                                   | 25            |
| trial_db_allowed           | Legacy Field. Value can be ignored.                                                                                                                                                                                      | <code>true</code> or <code>false</code>                                                                      | true          |

### Default Quota Plan for an Org

Cloud Foundry installs with a quota plan named `default` with the following values:

- Memory Limit: `10240 MB`
- Total Routes: `1000`
- Total Services: `100`
- Non-basic Services Allowed: `True`
- Trial DB Allowed: `True`

### Create a New Quota Plan for an Org

 **Note:** The org manager sets and manages quotas. See the [Orgs, Spaces, Roles, and Permissions](#) topic for more information.

You must set an org quota. You can create a new quota plan for org with `cf create-quota`.

## Use cf create-quota

In a terminal window, run the following command. Replace the placeholder attributes with the values for this quota plan:

```
cf create-quota QUOTA [-m TOTAL-MEMORY] [-i INSTANCE-MEMORY] [-r ROUTES] [-s SERVICE-INSTANCES] [--allow-paid-service-plans]
```

This command accepts the following flags:

- `-m`: Total amount of memory
- `-i`: Maximum amount of memory an application instance can have (`-1` represents an unlimited amount)
- `-r`: Total number of routes
- `-s`: Total number of service instances
- `--allow-paid-service-plans`: Can provision instances of paid service plans

Example:

```
$ cf create-quota small -m 2048M -i 1024M -r 10 -s 10 --allow-paid-service-plans
```

## Modify an Existing Quota Plan for an Org

### Use cf update-quota

1. Run `cf quotas` to find the names of all quota definitions available to your org. Record the name of the quota plan to be modified.

```
$ cf quotas
Getting quotas as admin@example.com...
OK
```

| name  | total memory limit | instance memory limit | routes | service instances | paid service plans |
|-------|--------------------|-----------------------|--------|-------------------|--------------------|
| free  | 0                  | 0                     | 1000   | 0                 | disallowed         |
| paid  | 10G                | 0                     | 1000   | -1                | allowed            |
| small | 2G                 | 0                     | 10     | 10                | allowed            |
| trial | 2G                 | 0                     | 1000   | 10                | disallowed         |

2. Run the following command, replacing QUOTA with the name of your quota.

```
cf update-quota QUOTA [-i INSTANCE-MEMORY] [-m MEMORY] [-n NEW-NAME] [-r ROUTES] [-s SERVICE-INSTANCES] [--allow-paid-service-plans | --disallow-paid-service-plans]
```

This command accepts the following flags:

- `-i`: Maximum amount of memory an application instance can have (`-1` represents an unlimited amount)
- `-m`: Total amount of memory a space can have
- `-n`: New name
- `-r`: Total number of routes
- `-s`: Total number of service instances
- `--allow-paid-service-plans`: Can provision instances of paid service plans
- `--disallow-paid-service-plans`: Can not provision instances of paid service plans

Example:

```
$ cf update-quota small -i 2048M -m 4096M -n medium -r 20 -s 20 --allow-paid-service-plans
```

## Create and Modify Quota Plans for a Space



For each org, Org Managers create and modify quota plans for spaces in the org. If an Org Manager allocates a space quota, CF verifies that resources do not exceed the allocated space limit. For example, when a Space Developer deploys an application, CF first checks the memory allocation at the space level, then at the org level.

Perform the following procedures to create and modify quota plans for individual spaces within an org.

## Create a New Quota Plan for a Space

In a terminal window, run the following command to create a quota for a space. Replace the placeholder attributes with the values for this quota plan:

```
cf create-space-quota QUOTA [-i INSTANCE-MEMORY] [-m MEMORY] [-r ROUTES] [-s SERVICE-INSTANCES] [--allow-paid-service-plans]
```

Example:

```
$ cf create-space-quota big -i 1024M -m 4096M -r 20 -s 20 --allow-paid-service-plans
```

## Modify a Quota Plan for a Space

Run `cf space-quotas` to find the names of all space quota available to your org. Record the name of the quota plan to be modified.

```
$ cf space-quotas
Getting quotas as admin@example.com...
OK
```

| name  | total memory limit | instance memory limit | routes | service instances | paid service plans |
|-------|--------------------|-----------------------|--------|-------------------|--------------------|
| big   | 2G                 | unlimited             | 0      | 10                | allowed            |
| trial | 2G                 | 0                     | 0      | 10                | allowed            |

To modify that quota, use the `update-space-quota` command. Replace the placeholder attributes with the values for this quota plan.

```
cf update-space-quota SPACE-QUOTA-NAME [-i MAX-INSTANCE-MEMORY] [-m MEMORY] [-n NEW-NAME] [-r ROUTES] [-s SERVICES] [--allow-paid-service-plans | --disallow-paid-service-plans]
```

Example:

```
$ cf update-space-quota big -i 20 -m 4096M -n bigger -r 20 -s 20 --allow-paid-service-plans
```

## Run cf help

For more information regarding quotas, run `cf help` to view a list and brief description of all cf CLI commands. Scroll to view org and space quotas usage and information.

```
$ cf help
...
ORG ADMIN:
 quotas List available usage quotas
 quota Show quota info
 set-quota Assign a quota to an org

 create-quota Define a new resource quota
 delete-quota Delete a quota
 update-quota Update an existing resource quota

 share-private-domain Share a private domain with an org
 unshare-private-domain Unshare a private domain with an org

SPACE ADMIN:
 space-quotas List available space resource quotas
 space-quota Show space quota info
 create-space-quota Define a new space resource quota
 update-space-quota update an existing space quota
 delete-space-quota Delete a space quota definition and unassign the space quota from all spaces
 set-space-quota Assign a space quota definition to a space
 unset-space-quota Unassign a quota from a space
```

## Using Feature Flags

Page last updated:

This topic describes how Cloud Foundry (CF) administrators can set feature flags using the Cloud Foundry Command Line Interface (cf CLI) to enable or disable the features available to users.

## View and Edit Feature Flags

To perform the following procedures, you must be logged in to your deployment as an administrator using the cf CLI.

1. Use the `cf feature-flags` command to list the feature flags:

```
$ cf feature-flags

Features State
user_org_creation disabled
private_domain_creation enabled
app_bits_upload enabled
app_scaling enabled
route_creation enabled
service_instance_creation enabled
diego_docker disabled
set_roles_by_username enabled
unset_roles_by_username enabled
task_creation enabled
env_var_visibility enabled
space_scoped_private_broker_creation enabled
space_developer_env_var_visibility enabled
service_instance_sharing disabled
hide_marketplace_from_unauthenticated_users disabled
```

For descriptions of the features enabled by each feature flag, see the [Feature Flags](#) section below.

2. To view the status of a feature flag, use the `cf feature-flag FEATURE-FLAG-NAME` command:

```
$ cf feature-flag user_org_creation

Retrieving status of user_org_creation as admin...
OK

Features State
user_org_creation disabled
```

3. To enable a feature flag, use the `cf enable-feature-flag FEATURE-FLAG-NAME` command:

```
$ cf enable-feature-flag user_org_creation
```

4. To disable a feature flag, use the `cf disable-feature-flag FEATURE-FLAG-NAME` command:

```
$ cf disable-feature-flag user_org_creation
```

## Feature Flags

Only administrators can set feature flags. All flags are enabled by default except `user_org_creation` and `diego_docker`. When disabled, these features are only available to administrators.

The following list provides descriptions of the features enabled or disabled by each flag, and the minimum Cloud Controller API (CC API) version necessary to use the feature. To determine your CC API version, follow the instructions in [Identifying the API Endpoint for your PAS Instance](#).

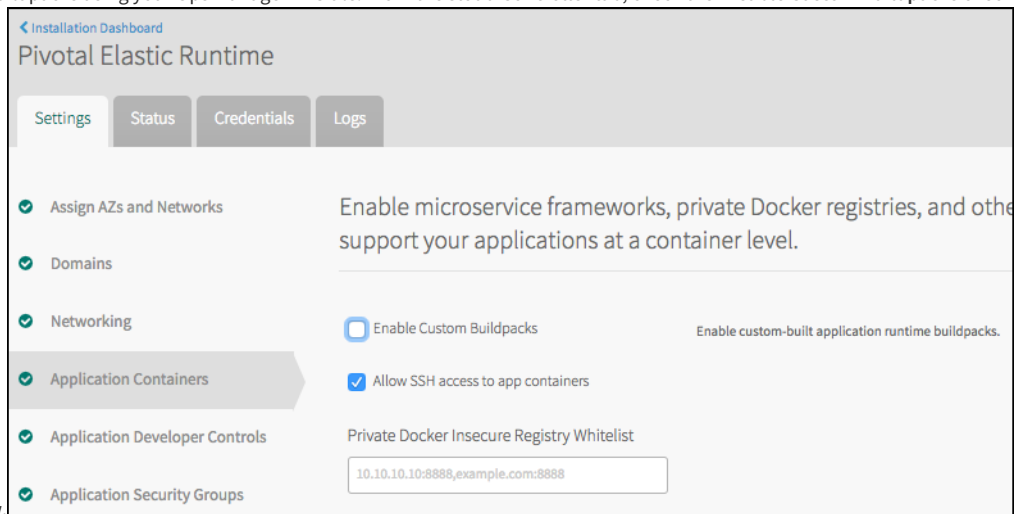
- `user_org_creation`: Any user can create an organization. If enabled, this flag activates the **Create a New Org** link in the dropdown menu of the left navigation menu in Apps Manager. Minimum CC API version: 2.12.
- `private_domain_creation`: An Org Manager can create private domains for that organization. Minimum CC API version: 2.12.

- `app_bits_upload` : Space Developers can upload app bits. Minimum CC API version: 2.12.
- `app_scaling` : Space Developers can perform scaling operations (i.e. change memory, disk, or instances). Minimum CC API version: 2.12.
- `route_creation` : Space Developers can create routes in a space. Minimum CC API version: 2.12.
- `service_instance_creation` : Space Developers can create service instances in a space. Minimum CC API version: 2.12.
- `diego_docker` : Space Developers can push Docker apps. Minimum CC API version 2.33.
- `set_roles_by_username` : Org Managers and Space Managers can add roles by username. Minimum CC API version: 2.37.
- `unset_roles_by_username` : Org Managers and Space Managers can remove roles by username. Minimum CC API version: 2.37.
- `task_creation` : Space Developers can create tasks on their application. Minimum CC API version: 2.47.
- `env_var_visibility` : All users can view environment variables. Minimum CC API version: 2.58.
- `space_scoped_private_broker_creation` : Space Developers can create space-scoped private service brokers. Minimum CC API version: 2.58.
- `space_developer_env_var_visibility` : Space Developers can view their v2 environment variables. Org Managers and Space Managers can view their v3 environment variables. Minimum CC API version: 2.58.
- `service_instance_sharing` : Space Developers can share service instances between two spaces (across orgs) in which they have the Space Developer role.
- `hide_marketplace_from_unauthenticated_users` : Do not allow unauthenticated users to see the service offerings available in the marketplace.

For more information about feature flag commands, see the **Feature Flags** section of the [Cloud Foundry API documentation](#).

## Disabling Custom Buildpacks

You can disable custom buildpacks using your Ops Manager PAS tile. From the **Cloud Controller** tab, check the **Disable Custom Buildpacks** checkbox, as



shown in the image below.

By default, the cf CLI gives developers the option of using a custom buildpack when they deploy apps to PAS. To do so, they use the `-b` option to provide a custom buildpack URL with the `cf push` command. The **Disable Custom Buildpacks** checkbox prevents the `-b` option from being used with external buildpack URLs.


For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.

## Examining GrootFS Disk Usage

Page last updated:

This topic describes how to analyze GrootFS disk space usage in Pivotal Application Service.

You run the commands in this topic as root on any BOSH-deployed VM that hosts the Garden job in a PAS deployment.

 **Note:** This topic provides different commands depending on whether you are using privileged or unprivileged containers in your deployment. By default, all deployments use unprivileged containers. For more information about these container types, see [Container Security](#).

For more information about the GrootFS concepts, see [GrootFS Disk Usage](#).

## Reconcile Container Disk Usage and Host Disk Usage

To reconcile disk allocations for containers with the actual disk usage on the host VM, you need to understand how GrootFS uses its disk.

Command line tools such as `du` and `df` can provide misleading information because of the way container file systems work.

For example, the following situations can occur:

| If...                                                                                                                                                                               | Then...                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| the Diego cell rep appears to be out of disk capacity, but the actual disk usage on the Garden host is low                                                                          | Diego does not schedule containers on the cell.                          |
| the Diego cell rep appears to have available disk capacity, but the combined space used by containers and system components prevents Diego from allocating the remaining disk space | Diego continues to place containers on the cell, but they fail to start. |

## About Container Disk Usage

On disk, the read-write layer for each container can be found at `/var/vcap/data/grootfs/store/unprivileged/images/CONTAINER-ID/diff`.

When GrootFS calls on the built-in XFS quota tooling to get disk usage for a container, it takes into account data written to that directory and not the data in the read-only volumes.

Running `grootfs stats` returns the following values:

- `total_bytes_used`: This is the disk usage of the container **including** the rootfs image volumes.
- `exclusive_bytes_used`: This is the disk usage of the container **not including** the rootfs image volumes.

## Retrieve Disk Usage Stats for a Single Container

To obtain the disk usage stats of a single container, perform the following steps:

- In your PAS deployment, use `bosh ssh` to connect to the BOSH-deployed VM running the Garden job.
- On the VM, run the following command to look up the container ID:

```
ls /var/vcap/data/garden/depot/
```

The command above returns a container ID in the following format:

```
55afb65-5cbf-49c6-4461-f803
```

- Based on the container type used in your deployment, run one of the following commands on the VM:
  - For unprivileged containers, run the following command:

```
/var/vcap/packages/grootfs/bin/grootfs --config \
/var/vcap/jobs/garden/config/grootfs_config.yml stats CONTAINER-ID
```

Where `CONTAINER-ID` corresponds to the container ID you obtained in step 2.

For example:

```
$ /var/vcap/packages/grootfs/bin/grootfs --config \
/var/vcap/jobs/garden/config/grootfs_config.yml stats 55afb65-5cbf-49c6-4461-f803
```

- For privileged containers, run the following command:

```
/var/vcap/packages/grootfs/bin/grootfs --config \
/var/vcap/jobs/garden/config/privileged_grootfs_config.yml stats CONTAINER-ID
```

Where `CONTAINER-ID` corresponds to the container ID you obtained in step 2.

For example:

```
$ /var/vcap/packages/grootfs/bin/grootfs --config \
/var/vcap/jobs/garden/config/privileged_grootfs_config.yml stats 55afb65-5cbf-49c6-4461-f803
```

The commands above return output in the following format:

```
{"disk_usage":{"total_bytes_used":23448093,"exclusive_bytes_used":8192}}
```

## Retrieve Exclusive Disk Usage Stats for All Running Containers

To check the disk usage of all running containers, perform the following steps:

- In your PAS deployment, use `bosh ssh` to connect to the BOSH-deployed VM running the Garden job.
- Based on the container type used in your deployment, run one of the following commands on the VM:
  - For unprivileged containers, run the following command:

```
ls /var/vcap/data/garden/depot/ \
| xargs -I{} /var/vcap/packages/grootfs/bin/grootfs --config \
/var/vcap/jobs/garden/config/grootfs_config.yml stats {} \
| cut -d: -f4 | cut -d} -f1 | awk '{sum += $1} END {print sum}'
```

- For privileged containers, run the following command:

```
ls /var/vcap/data/garden/depot/ \
| xargs -I{} /var/vcap/packages/grootfs/bin/grootfs --config \
/var/vcap/jobs/garden/config/privileged_grootfs_config.yml stats {} \
| cut -d: -f4 | cut -d} -f1 | awk '{sum += $1} END {print sum}'
```

The commands above return the total disk usage in bytes for all running containers.

## About Volumes in GrootFS

Underlying layers are known as `volumes` in GrootFS.

They are read-only and their changesets are layered together through an **OverlayFS** mount to create the rootfs for containers. When GrootFS writes each file system volume to disk, it also stores the number of bytes written to a file in the `meta` directory.

## Check Volume Disk Size

To find out the size of an individual volume, you can read the corresponding metadata file or run `du` on the volume itself. Perform the following steps:

- In your PAS deployment, use `bosh ssh` to connect to the BOSH-deployed VM running the Garden job.
- Based on the container type used in your deployment, run one of the following commands on the VM:

- For unprivileged containers, run the following command on the VM:

```
cat /var/vcap/data/grootfs/store/unprivileged/meta/volume-VOLUME-SHA
```

Where `VOLUME-SHA` corresponds to the SHA value of the volume.

- For privileged containers, run the following command:

```
cat /var/vcap/data/grootfs/store/privileged/meta/volume-VOLUME-SHA
```

Where `VOLUME-SHA` corresponds to the SHA value of the volume.

The `cat` commands above return the volume size in bytes in the following format:

```
{"Size":5607885}
```

- Alternatively, use `du` and pass the absolute path to the volume. Run one of the following commands on the VM:

- For unprivileged containers, run the following command:

```
du -sch /var/vcap/data/grootfs/store/unprivileged/volumes/VOLUME-SHA/
```

Where `VOLUME-SHA` corresponds to the SHA value of the volume.

- For privileged containers, run the following command:

```
du -sch /var/vcap/data/grootfs/store/privileged/volumes/VOLUME-SHA/
```

Where `VOLUME-SHA` corresponds to the SHA value of the volume.

The `du` commands above return the volume size in the following format:

```
5.4M /var/vcap/data/grootfs/store/unprivileged/volumes/VOLUME-SHA/
```

## Determine Disk Usage and Reclaimable Disk Space

This section describes how to calculate the amount of disk space is in use and estimate how much space is reclaimable.

### Calculate Disk Use by All Active Volumes

For each container, GrootFS mounts the underlying volumes using overlay to a point in the `images` directory. This point is the rootfs for the container and is read-write.

GrootFS also stores the SHA of each underlying volume used by an image in the `meta` folder.

You can determine the bytes of all active volumes on disk by running one of the following commands:

💡 If you do not have `python3` is not installed, replace `python3` with `python` in the commands below.

- For unprivileged containers, run the following command:

```
for image in $(ls /var/vcap/data/grootfs/store/unprivileged/meta/dependencies/image*;*.json); \
do cat $image | python3 -c 'import json,sys;obj=json.load(sys.stdin); \
print("\n".join(obj))'; done | sort -u \
| xargs -l {} cat /var/vcap/data/grootfs/store/unprivileged/meta/volume-{} \
| cut -d : -f 2 | cut -d } -f 1 \
| awk '{sum += $1} END {print sum}'
```

- For privileged containers, run the following command:

```
for image in $(ls /var/vcap/data/grootfs/store/privileged/meta/dependencies/image:*.*json); \
do cat $image | python3 -c 'import json,sys;obj=json.load(sys.stdin); \
print("\n".join(obj))' ; done | sort -u \
| xargs -l {} cat /var/vcap/data/grootfs/store/privileged/meta/volume-{} \
| cut -d : -f 2 | cut -d } -f 1 \
| awk '{sum += $1} END {print sum}'
```

The commands above return the total number of bytes used by all active volumes on disk.

## Calculate GrootFS Store Disk Usage

To determine how much total disk space the store is using, run the following command:

```
df | grep -E "/var/vcap/data/grootfs/store/(privileged|unprivileged)$" \
| awk '{sum += $3} END {print sum}'
```

The command above returns the total number of bytes used by the store.

## Calculate Reclaimable Disk Space

You can use values gathered from the commands above to calculate how much space can be cleared in GrootFS. Garbage collection reclaims disk space by pruning unused volumes.

The overall formula to calculate reclaimable disk space is to subtract the total disk in use by the store from the total disk used by active volumes.

For example, perform the following steps:

1. Calculate how much disk space the store is using by following the instructions in [Calculate GrootFS Store Disk Usage](#). For example, your result might be:

```
Total disk store = 5607885 bytes
```

2. Calculate how much disk space active volumes are using by following the instructions in [Calculate Disk Use by All Active Volumes](#). For example, your result might be:

```
Active volumes = 3212435 bytes
```

3. Subtract the amount of space used by active volumes from the space used by the store. For example, your result might be:

```
5607885 - 3212435 = 2395450 bytes
```

In this example, you can reclaim 2395450 bytes through garbage collection.

## How GrootFS Reclaims Disk Space

The thresholder component calculates and sets a value so that GrootFS's garbage collector can attempt to ensure that a small reserved space is kept free for other jobs. GrootFS only tries to garbage collect or reclaim space when that threshold is reached. However, if all the rootfs layers are actively in use by images, then garbage collection cannot occur and that space is used up.

If you determine that there is not enough reclaimable disk and more space is needed on disk, you should scale up your VMs to a larger size or add more VMs to provide more disk space.

Alternatively, you can configure a lower threshold for cell disk cleanup in Pivotal Application Service (PAS). For more information, see [Configuring Disk Cell Cleanup](#).

## Other Categories of GrootFS Disk Usage

There may be categories of GrootFS disk usage other than those listed in the above sections. However, the bulk of disk usage is stored in the



`images/CONTAINER-ID/diff` and `volumes` directories, so these are rarely taken into consideration when calculating store usage.

You can find these directories under `/var/vcap/data/grootfs/store/unprivileged` for unprivileged containers and `/var/vcap/data/grootfs/store/privileged` for privileged containers.

GrootFS also stores information in the following directories:

- `1` : link directories. Shorter directory names are symlinked to volume directories to allow Groot to union mount more file paths.
- `locks` : file system lock directory to ensure safety during concurrent cleans and creates.
- `meta` : per image and volume metadata.
- `projectids` : empty numbered directories used to track image quotas.
- `tmp` : normal temporary directory contents.

These directories typically use less than 2 MB disk in total.


## Managing Custom Buildpacks

Page last updated:

This topic describes how an admin can manage additional buildpacks in Cloud Foundry using the Cloud Foundry Command Line Interface tool (cf CLI). If your application uses a language or framework that the Cloud Foundry system buildpacks do not support, you can take one of the following actions:

- [Write your own buildpack](#)
- Customize an existing buildpack
- Use a [Cloud Foundry Community Buildpack](#) [↗](#)
- Use a [Heroku Third-Party Buildpack](#) [↗](#)

## Add a Buildpack

 **Note:** You must be a Cloud Foundry admin user to run the commands discussed in this section.

To add a buildpack, run the `cf create-buildpack BUILDPACK PATH POSITION [--enable|--disable]` command. The arguments to [cf create-buildpack](#) [↗](#) specify the following:

- **BUILDPACK** specifies the buildpack name.
- **PATH** specifies the location of the buildpack. PATH can point to a zip file, the URL of a zip file, or a local directory.
- **POSITION** specifies where to place the buildpack in the detection priority list. For more information, see the [Buildpack Detection](#) [↗](#) topic.
- **enable** or **disable** specifies whether to allow apps to be pushed with the buildpack. This argument is optional, and defaults to enable. When a buildpack is disabled, app developers cannot push apps using that buildpack.

To confirm that you have successfully added a buildpack, run `cf buildpacks`.

The following example shows the output from running the `cf buildpacks` command after an administrator adds a Python buildpack:

```
$ cf buildpacks
Getting buildpacks...

buildpack position enabled locked filename
ruby_buildpack 1 true false buildpack_ruby_v46-245-g2fc4ad8.zip
nodejs_buildpack 2 true false buildpack_nodejs_v8-177-g2b0a5cf.zip
java_buildpack 3 true false buildpack_java_v2.1.zip
python_buildpack 4 true false buildpack_python_v2.7.6.zip
```

## Rename a Buildpack

To rename a buildpack, run `cf rename-buildpack BUILDPACK-NAME NEW-BUILDPACK-NAME`. Replace `BUILDPACK-NAME` with the original buildpack name, and `NEW-BUILDPACK-NAME` with the new buildpack name.

For more information about renaming buildpack, see the [cf CLI documentation](#) [↗](#).

## Update a Buildpack

```
$ cf update-buildpack BUILDPACK [-p PATH] [-i POSITION] [-s STACK] [--enable|--disable] [--lock|--unlock]
```

For more information about updating buildpacks, see the [cf CLI documentation](#) [↗](#).

## Delete a Buildpack

```
$ cf delete-buildpack BUILDPACK [-s STACK] [-f]
```

For more information about deleting buildpacks, see the [cf CLI documentation](#).

## Lock and Unlock a Buildpack

Every new version of Cloud Foundry includes an updated buildpack. By default, your deployment applies the most recent buildpack when you upgrade. In some cases, however, you may want to preserve an existing buildpack, rather than upgrade to the latest version. For example, if an app you deploy depends on a specific component in Buildpack A that is not available in Buildpack B, you may want to continue using Buildpack A.

The `--lock` flag lets you continue to use your existing buildpack even after you upgrade. Locked buildpacks are not updated when PCF updates. You must manually unlock them to update them.

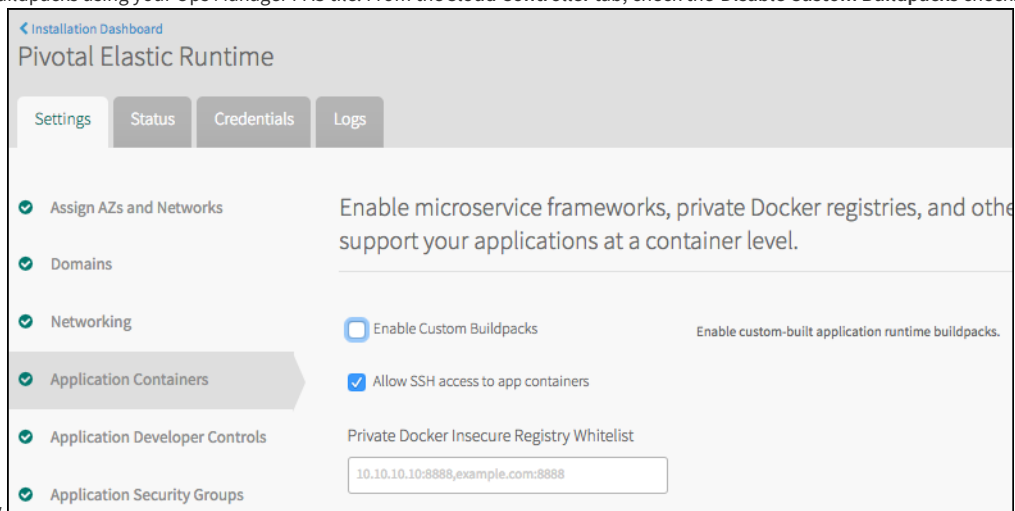
If you elect to use the `--unlock` flag, your deployment will apply the most recent buildpack when you upgrade PCF.

```
cf update-buildpack BUILDPACK [-p PATH] [-i POSITION] [-s STACK] [--enable|--disable] [--lock|--unlock]
```

This feature is also available through the API. For more information, see [Lock or unlock a Buildpack](#) in the [Cloud Foundry API](#) documentation.

## Disabling Custom Buildpacks

You can disable custom buildpacks using your Ops Manager PAS tile. From the **Cloud Controller** tab, check the **Disable Custom Buildpacks** checkbox, as



shown in the image below.

By default, the cf CLI gives developers the option of using a custom buildpack when they deploy apps to PAS. To do so, they use the `-b` option to provide a custom buildpack URL with the `cf push` command. The **Disable Custom Buildpacks** checkbox prevents the `-b` option from being used with external buildpack URLs.

For more information about custom buildpacks, refer to the [buildpacks](#) section of the PCF documentation.

## Using Docker in Cloud Foundry

Page last updated:

This topic describes how Cloud Foundry (CF) operators can enable CF developers to run their apps in Docker containers, and explains how Docker works in Cloud Foundry.

For information about Diego, the Cloud Foundry component that manages application containers, see the [Diego Architecture](#) topic. For information about how CF developers push apps with Docker images, see [Deploy an App with Docker](#).

### Enable Docker

By default, apps deployed with the `cf push` command run in standard Cloud Foundry Linux containers. With Docker support enabled, Cloud Foundry can also deploy and manage apps running in Docker containers.

To deploy apps to Docker, developers run `cf push` with the `--docker-image` option and the location of a Docker image to create the containers from. See the [Push a Docker Image](#) topic for information about how CF developers push apps with Docker images.

To enable Docker support on a CF deployment, an operator must do the following:

- [Enable](#) the `diego_docker` feature flag.
- [Configure](#) access to any Docker registries that developers want to use images from.

### Enable and Disable the `diego_docker` Feature Flag

The `diego_docker` feature flag governs whether a CF deployment supports Docker containers.

To enable Docker support, run:

```
$ cf enable-feature-flag diego_docker
```

To disable Docker support, run:

```
$ cf disable-feature-flag diego_docker
```



**Note:** Disabling the `diego_docker` feature flag stops all Docker-based apps in your deployment within a few convergence cycles, on the order of a minute.

### Configure Docker Registry Access

To support Docker, Pivotal Cloud Foundry needs the ability to access Docker registries using either a Certificate Authority or an IP address whitelist. The [Using Docker Registries](#) topic explains how to configure this access.

### Docker Image Contents

A Docker image consists of a collection of layers. Each layer consists of one or both of the following:

- Raw bits to download and mount. These bits form the file system.
- Metadata that describes commands, users, and environment for the layer. This metadata includes the `ENTRYPOINT` and `CMD` directives, and is specified in the Dockerfile.

### How Garden-runC Creates Containers

Diego currently uses Garden-runC to construct Linux containers.

Both Docker and Garden-runC use libraries from the [Open Container Initiative \(OCI\)](#) [↗](#) to build Linux containers. After creation, these containers use name space isolation, or *namespaces*, and control groups, or *cgroups*, to isolate processes in containers and limit resource usage. These are common kernel resource isolation features used by all Linux containers.

 **Note:** PAS versions v1.8.8 and above use Garden-runC instead of Garden-Linux.

Before Garden-runC creates a Linux container, it creates a file system that is mounted as the root file system of the container. Garden-runC supports mounting Docker images as the root file systems for the containers it creates.

When creating a container, both Docker and Garden-runC perform the following actions:

- Fetch and cache the individual layers associated with a Docker image
- Combine and mount the layers as the root file system

These actions produce a container whose contents exactly match the contents of the associated Docker image.


Earlier versions of Diego used Garden-Linux. For more information, see the [Garden](#) topic.

## How Diego Runs and Monitors Processes

After Garden-runC creates a container, Diego runs and monitors the processes inside of it.

To determine which processes to run, the [Cloud Controller](#) fetches and stores the metadata associated with the Docker image. The Cloud Controller uses this metadata to perform the following actions:

- Runs the start command as the user specified in the Docker image
- Instructs Diego and the [Gorouter](#) to route traffic to the lowest-numbered port [exposed](#) [↗](#) in the Docker image, or port 8080 if the Dockerfile does not explicitly expose a listen port.

 **Note:** When launching an application on Diego, the Cloud Controller honors any user-specified overrides such as a custom start command or custom environment variables.

## Docker Security Concerns in a Multi-Tenant Environment

The attack surface area for a Docker-based container running on Diego remains somewhat higher than that of a buildpack application because Docker allows users to fully specify the contents of their root file systems. A buildpack application runs on a trusted root filesystem.

Garden-runC provides features that allow the platform to run Docker images more securely in a multi-tenant context. In particular, Cloud Foundry uses the `user-namespacing` feature found on modern Linux kernels to ensure that users cannot gain escalated privileges on the host even if they escalate privileges within a container.

The Cloud Controller always runs Docker containers on Diego with user namespaces enabled. This security restriction prevents certain features, such as the ability to mount FuseFS devices, from working in Docker containers. Docker applications can use fuse mounts through [volume services](#), but they cannot directly mount fuse devices from within the container.

To mitigate security concerns, Cloud Foundry recommends that you run only trusted Docker containers on the platform. By default, the Cloud Controller does not allow Docker-based applications to run on the platform.

## User Accounts and Communications

The following topics provide information about managing user accounts and user communications in Pivotal Application Service (PAS):

- [Creating and Managing Users with the cf CLI](#)
- [Creating and Managing Users with the UAA CLI \(UAAC\)](#)
- [Creating New PAS User Accounts](#)
- [Adding Existing SAML or LDAP Users to a Pivotal Cloud Foundry Deployment](#)
- [Getting Started with the Notifications Service](#)

## Creating and Managing Users with the cf CLI

Using the Cloud Foundry Command Line Interface (cf CLI), administrators, Org Managers, and Space Managers can manage users. Cloud Foundry uses role-based access control, with each role granting permissions in either an organization or an application space.

For more information, see [Organizations, Spaces, Roles, and Permissions](#).

### About Roles

To manage all users, organizations, and roles with the cf CLI, log in with your admin credentials. In Pivotal Operations Manager, refer to **PAS > Credentials** for the admin name and password.

If the feature flag `set_roles_by_username` is enabled, Org Managers can [assign org roles](#) to existing users in their org and Space Managers can [assign space roles](#) to existing users in their space. For more information about using feature flags, see the [Feature Flags](#) topic.

## Creating and Deleting Users

| FUNCTION                                                                              | COMMAND                                             | EXAMPLE                                         |
|---------------------------------------------------------------------------------------|-----------------------------------------------------|-------------------------------------------------|
| Create a new user                                                                     | <code>cf create-user USERNAME PASSWORD</code>       | <code>cf create-user Alice pa55w0rd</code>      |
| Create a new user, specifying LDAP as an external identity provider                   | <code>cf create-user USERNAME -origin ORIGIN</code> | <code>cf create-user Aayah ldap</code>          |
| Create a new user, specifying SAML or OpenID Connect as an external identity provider | <code>cf create-user USERNAME -origin ORIGIN</code> | <code>cf create-user Aiko provider-alias</code> |
| Delete a user                                                                         | <code>cf delete-user USERNAME</code>                | <code>cf delete-user Alice</code>               |

### Creating Administrator Accounts

To create a new administrator account, use the [UAA CLI](#).



**Note:** The cf CLI cannot create new administrator accounts.

## Org and App Space Roles

A user can have one or more roles. The combination of these roles defines the user's overall permissions in the org and within specific app spaces in that org.

### Org Roles

Valid [org roles](#) are OrgManager, BillingManager, and OrgAuditor.

| FUNCTION                                       | COMMAND                                                        | EXAMPLE                                                        |
|------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------|
| View the organizations belonging to an account | <code>cf orgs</code>                                           | <code>cf orgs</code>                                           |
| View all users in an organization by role      | <code>cf org-users ORGANIZATION-NAME</code>                    | <code>cf org-users my-example-org</code>                       |
| Assign an org role to a user                   | <code>cf set-org-role USERNAME ORGANIZATION-NAME ROLE</code>   | <code>cf set-org-role Alice my-example-org OrgManager</code>   |
| Remove an org role from a user                 | <code>cf unset-org-role USERNAME ORGANIZATION-NAME ROLE</code> | <code>cf unset-org-role Alice my-example-org OrgManager</code> |

If multiple accounts share a username, `set-org-role` and `unset-org-role` return an error. See [Identical Usernames in Multiple Origins](#) for details.

## App Space Roles

Each app space role applies to a specific app space.

Valid [app space roles](#) are SpaceManager, SpaceDeveloper, and SpaceAuditor.

| FUNCTION                          | COMMAND                                                        | EXAMPLE                                                                        |
|-----------------------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------|
| View the spaces in an org         | cf spaces                                                      | <code>cf spaces</code>                                                         |
| View all users in a space by role | cf space-users ORGANIZATION-NAME SPACE-NAME                    | <code>cf space-users my-example-org development</code>                         |
| Assign a space role to a user     | cf set-space-role USERNAME ORGANIZATION-NAME SPACE-NAME ROLE   | <code>cf set-space-role Alice my-example-org development SpaceAuditor</code>   |
| Remove a space role from a user   | cf unset-space-role USERNAME ORGANIZATION-NAME SPACE-NAME ROLE | <code>cf unset-space-role Alice my-example-org development SpaceAuditor</code> |

If multiple accounts share a username, `set-space-role` and `unset-space-role` return an error. See [Identical Usernames in Multiple Origins](#) for details.



## Creating and Managing Users with the UAA CLI (UAAC)

Page last updated:

Using the UAA Command Line Interface (UAAC), an administrator can create users in the User Account and Authentication (UAA) server.

**Note:** The UAAC only creates users in UAA, and does not assign roles in the Cloud Controller database (CCDB). In general, administrators create users using the Cloud Foundry Command Line Interface (cf CLI). The cf CLI both creates user records in the UAA and associates them with org and space roles in the CCDB. Before administrators can assign roles to the user, the user must log in through Apps Manager or the cf CLI for the user record to populate the CCDB. Review the [Creating and Managing Users with the cf CLI](#) topic for more information.

For additional details and information, refer to the following topics:

- [UAA Overview](#)
- [UAA Sysadmin Guide](#) [↗](#)
- [Other UAA Documentation](#) [↗](#)

**Note:** UAAC requires Ruby v2.3.1 or later. If you have an earlier version of Ruby installed, install v2.3.1 or later before using the UAAC.

For more information about which roles can perform various operations in Cloud Foundry, see the [Roles and Permissions](#) topic.

## Create an Admin User

1. Install the UAA CLI, `uaac`.

```
$ gem install cf-uaac
```

2. Use the `uaac target uaa.YOUR-DOMAIN` command to target your UAA server.

```
$ uaac target uaa.example.com
```

3. Record the `uaa:admin:client_secret` from your deployment manifest.

4. Run `uaac token client get admin -s ADMIN-CLIENT-SECRET` to authenticate and obtain an access token for the admin client from the UAA server. Replace `ADMIN-CLIENT-SECRET` with the admin secret you have retrieved in previous step. UAAC stores the token in `~/uaac.yml`.

```
$ uaac token client get admin -s MyAdminSecret
```

5. Use the `uaac contexts` command to display the users and applications authorized by the UAA server, and the permissions granted to each user and application.

```
$ uaac contexts

[1]*[admin]
 client_id: admin
 access_token: aBcdEfg0hIJKlm123.e
 token_type: bearer
 expires_in: 43200
 scope: uaa.admin.clients.secret scim.read
 jti: 91b3-abcd1233
```

6. In the output from `uaac contexts`, search in the `scope` section of the `client_id: admin` user for `scim.write`. The value `scim.write` represents sufficient permissions to create accounts.

7. If the admin user lacks permissions to create accounts, add the permissions by following these steps:

- Run `uaac client update admin --authorities "EXISTING-PERMISSIONS scim.write"` to add the necessary permissions to the admin user account on the UAA server. Replace EXISTING-PERMISSIONS with the current contents of the `scope` section from `uaac contexts`.
- Run `uaac token delete` to delete the local token.
- Run `uaac token client get admin` to obtain an updated access token from the UAA server.

```
$ uaac contexts

[1]*[admin]
 client_id: admin
 ...
 scope: uaa.admin clients.secret scim.read
 ...

$ uaac client update admin --authorities "uaac client get admin | \
awk '/:{e=0}/authorities:{e=1;if(e==1){$1=""};print}'" scim.write"

$ uaac token delete
$ uaac token client get admin
```

- Run the following command to create an admin user: `uaac user add NEW-ADMIN-USERNAME -p NEW-ADMIN-PASSWORD --emails NEW-ADMIN-EMAIL`  
Replace `NEW-ADMIN-USERNAME`, `NEW-ADMIN-PASSWORD`, and `NEW-ADMIN-EMAIL` with appropriate information.

```
$ uaac user add Adam -p newAdminSecretPassword --emails newadmin@example.com
```

- Run `uaac member add GROUP NEW-ADMIN-USERNAME` to add the new admin to the groups `cloud_controller.admin`, `uaa.admin`, `scim.read`, and `scim.write`.

```
$ uaac member add cloud_controller.admin Adam
$ uaac member add uaa.admin Adam
$ uaac member add scim.read Adam
$ uaac member add scim.write Adam
```

## Create an Admin Read-Only User

The admin read-only account can view but not modify almost all Cloud Controller API resources. The admin read-only account cannot view process `stats` or `logs`.

If you want to create an admin read-only user account, then perform the following steps:

- Obtain the credentials of an admin client created using UAAC as above, or refer to the `uaa: scim` section of your deployment manifest for the user name and password of an admin user.
- Run `uaac token client get admin -s ADMIN-CLIENT-SECRET` to authenticate and obtain an access token for the admin client from the UAA server. Replace `ADMIN-CLIENT-SECRET` with your admin secret. UAAC stores the token in `~/uaac.yml`.

```
$ uaac token client get admin -s MyAdminSecret
```

- Run the following command to create an admin read-only user: `uaac user add NEW-USERNAME -p NEW-PASSWORD --emails NEW-EMAIL`  
Replace `NEW-USERNAME`, `NEW-PASSWORD`, and `NEW-EMAIL` with appropriate information.

```
$ uaac user add Bob -p SecretPassword --emails bob@example.com
```

- Run `uaac member add GROUP NEW-USERNAME` to add the new admin read-only account to the groups `cloud_controller.admin_read_only` and `scim.read`.

```
$ uaac member add cloud_controller.admin_read_only Bob
$ uaac member add scim.read Bob
```

## Create a Global Auditor

The global auditor account has read-only access to almost all Cloud Controller API resources but cannot access secret data such as environment variables. The global auditor account cannot view process `stats` or `logs`.

Perform the following steps to create a global auditor account.

- Obtain the credentials of an admin client created using UAAC as above, or refer to the `uaa: scim` section of your deployment manifest for the user name and password of an admin user.
- Run `uaac token client get admin -s ADMIN-CLIENT-SECRET` to authenticate and obtain an access token for the admin client from the UAA server. Replace `ADMIN-CLIENT-SECRET` with your admin secret. UAAC stores the token in `~/uaac.yml`.

```
$ uaac token client get admin -s MyAdminSecret
```

- Run `uaac user add NEW-USERNAME -p NEW-PASSWORD --emails NEW-EMAIL` to create a global auditor user. Replace `NEW-USERNAME`, `NEW-PASSWORD`, and `NEW-EMAIL` with appropriate information.

```
$ uaac user add Alice -p SecretPassword --emails alice@example.com
```

- Ensure that the `cloud_controller.global_auditor` group exists.

```
$ uaac group add cloud_controller.global_auditor
```

- Run `uaac member add GROUP NEW-USERNAME` to add the new global auditor account to the `cloud_controller.global_auditor` group.

```
$ uaac member add cloud_controller.global_auditor Alice
```

## Grant Admin Permissions to an External Group (SAML or LDAP)


To grant all users under an external group admin permissions, do the following:

- Obtain the credentials of an admin client created using UAAC as above, or refer to the `uaa: scim` section of your deployment manifest for the user name and password of an admin user.
- Run `uaac token client get admin -s ADMIN-CLIENT-SECRET` to authenticate and obtain an access token for the admin client from the UAA server. Replace `ADMIN-CLIENT-SECRET` with your admin secret. UAAC stores the token in `~/uaac.yml`.

```
$ uaac token client get admin -s MyAdminSecret
```

- Follow the procedure that corresponds to your use case:

- [Grant Admin Permissions for LDAP](#)
- [Grant Admin Permissions for SAML](#)

 **Note:** The UAA will not grant scopes for users in external groups until the next time the user logs in. This means that users granted scopes from external group mappings must log out from PCF and log back in before their new scope takes effect.

### Grant Admin Permissions for LDAP

Run the commands below to grant all users under the mapped LDAP Group admin permissions. Replace `GROUP-DISTINGUISHED-NAME` with an appropriate group name.

- `uaac group map --name scim.read "GROUP-DISTINGUISHED-NAME"`
- `uaac group map --name scim.write "GROUP-DISTINGUISHED-NAME"`
- `uaac group map --name cloud_controller.admin "GROUP-DISTINGUISHED-NAME"`

### Grant Admin Permissions for SAML

- Retrieve the name of your SAML provider by navigating to the PAS tile on the Ops Manager Installation Dashboard, clicking **Authentication and Enterprise SSO**, and recording the value under **Provider Name**. For more information about configuring PCF for a SAML identity provider, see the [Configuring Authentication and Enterprise SSO for PAS](#) topic.
- Run the commands below to grant all users under the mapped SAML group admin permissions. Replace `GROUP-NAME` with the group name, and `SAML-PROVIDER-NAME` with the name of your SAML provider.

- `uaac group map --name scim.read "GROUP-NAME" --origin SAML-PROVIDER-NAME`
- `uaac group map --name scim.write "GROUP-NAME" --origin SAML-PROVIDER-NAME`
- `uaac group map --name cloud_controller.admin "GROUP-NAME" --origin SAML-PROVIDER-NAME`

## Create Users

1. Obtain the credentials of an admin client created using UAAC as above, or refer to the `uaa: scim` section of your deployment manifest for the user name and password of an admin user.
2. Run `cf login -u NEW-ADMIN-USERNAME -p NEW-ADMIN-PASSWORD` to log in.

```
$ cf login -u Adam -p newAdminSecretPassword
```

3. Run `cf create-user NEW-USER-NAME NEW-USER-PASSWORD` to create a new user.

```
$ cf create-user Charlie aNewPassword
```

## Change Passwords

1. Obtain the credentials of an admin client created using UAAC as above, or refer to the `uaa: scim` section of your deployment manifest for the user name and password of an admin user.
2. Run `uaac token client get admin -s ADMIN-CLIENT-SECRET` to authenticate and obtain an access token for the admin client from the UAA server. Replace `ADMIN-CLIENT-SECRET` with your admin secret. UAAC stores the token in `~/uaac.yml`.

```
$ uaac token client get admin -s MyAdminSecret
```

3. Run `uaac contexts` to display the users and applications authorized by the UAA server, and the permissions granted to each user and application.

```
$ uaac contexts

[1]*[admin]
 client_id: admin
 access_token: aBcdEfG0hIJKlm123.e
 token_type: bearer
 expires_in: 43200
 scope: uaa.admin.clients.secret.password.read
 jti: 91b3-abcd1233
```

4. In the output from `uaac contexts`, search in the `scope` section of the `client_id: admin` user for `password.write`. The value `password.write` represents sufficient permissions to change passwords.
5. If the admin user lacks permissions to change passwords, add the permissions by following these steps:
  - o Run `uaac client update admin --scope "EXISTING-PERMISSIONS password.write"` to add the necessary permissions to the admin user account on the UAA server. Replace EXISTING-PERMISSIONS with the current contents of the `scope` section from `uaac contexts`.
  - o Run `uaac token delete` to delete the local token.
  - o Run `uaac token client get admin` to obtain an updated access token from the UAA server.

```
$ uaac contexts

[1]*[admin]
 client_id: admin
 ...
 scope: uaa.admin.clients.secret.password.read
 ...

$ uaac client update admin --scope ""uaac client get admin | \
awk '/:{e=0}/authorities:/{e=1;if(e==1){$1="";print}}' password.write"

$ uaac token delete
$ uaac token client get admin
```

6. Run `uaac password set USER-NAME -p TEMP-PASSWORD` to change an existing user password to a temporary password.

```
$ uaac password set Charlie -p ThisIsATempPassword
```

7. Provide the `TEMP-PASSWORD` to the user. Have the user use `cf target api.YOUR-DOMAIN`, `cf login -u USER-NAME -p TEMP-PASSWORD`, and `cf passwd` to change the temporary password. See the [Configuring UAA Password Policy](#) topic to configure the password policy.

```
$ cf target api.example.com
$ cf login -u Charlie -p ThisIsATempPassword
$ cf passwd

Current Password>ThisIsATempPassword

New Password>*****

Verify Password>*****
Changing password...
```

## Retrieve User Email Addresses

Some Cloud Foundry components, like Cloud Controller, only use GUIDs for user identification. You can use the UAA to retrieve the emails of your Cloud Foundry instance users either as a list or, for a specific user, with that user's GUID.

Follow the steps below to retrieve user email addresses:

1. Run `uaac target uaa.YOUR-DOMAIN` to target your UAA server.

```
$ uaac target uaa.example.com
```

2. Record the `uaa:admin:client_secret` from your deployment manifest.
3. Run `uaac token client get admin -s ADMIN-CLIENT-SECRET` to authenticate and obtain an access token for the admin client from the UAA server. Replace `ADMIN-CLIENT-SECRET` with your admin secret. UAAC stores the token in `~/.uaac.yml`.

```
$ uaac token client get admin -s MyAdminSecret
```

4. Run `uaac contexts` to display the users and applications authorized by the UAA server, and the permissions granted to each user and application.

```
$ uaac contexts

[1]*[admin]
 client_id: admin
 access_token: aBcdEfg0hIJKlm123.e
 token_type: bearer
 expires_in: 43200
 scope: uaa.admin clients.secret
 jti: 91b3-abcd1233
```

5. In the output from `uaac contexts`, search in the `scope` section of the `client_id: admin` user for `scim.read`. The value `scim.read` represents sufficient permissions to query the UAA server for user information.
6. If the admin user lacks permissions to query the UAA server for user information, add the permissions by following these steps:
  - Run `uaac client update admin --authorities "EXISTING-PERMISSIONS scim.write"` to add the necessary permissions to the admin user account on the UAA server. Replace EXISTING-PERMISSIONS with the current contents of the `scope` section from `uaac contexts`.
  - Run `uaac token delete` to delete the local token.
  - Run `uaac token client get admin` to obtain an updated access token from the UAA server.

```
$ uaac contexts

[1]*[admin]
 client_id: admin
 ...
 scope: uaa.admin clients.secret
 ...

$ uaac client update admin --authorities "uaa.admin clients.secret scim.read"

$ uaac token delete
$ uaac token client get admin
```

7. Run `uaac users` to list your Cloud Foundry instance users. By default, the `uaac users` command returns information about each user account including GUID, name, permission groups, activity status, and metadata. Use the `--attributes emails` or `-a emails` flag to limit the output of `uaac users` to email

addresses.

```
$ uaac users --attributes emails

resources:
 emails:
value: user1@example.com
 emails:
value: user2@example.com
 emails:
value: user3@example.com
```

8. Run `uaac users "id eq GUID" --attributes emails` with the GUID of a specific user to retrieve that user's email address.

```
$ uaac users "id eq 'aabbcc11-22a5-87-8056-beaf84'" --attributes emails

resources:
 emails:
value: user1@example.com
```

## Getting Started with the Notifications Service

Page last updated:

This topic describes how to use the Notifications Service, including how to create a client, obtain a token, register notifications, create a custom template, and send notifications to your users.

### Prerequisites

- Install [Pivotal Application Service](#).
- You must have `admin` permissions on your Cloud Foundry instance. You also must configure [Application Security Groups \(ASGs\)](#).
- Install the [Cloud Foundry Command Line Interface \(cf CLI\)](#) and [User Account and Authorization Server \(UAAC\)](#) command line tools.

### Create a Client and Get a Token

To interact with the Notifications Service, you must create [UAA](#) scopes:

1. Use `uaac target uaa.YOUR-DOMAIN` to target your UAA server.

```
$ uaac target uaa.example.com
```

2. Record the **Admin Client Credentials** from the **UAA** row in the PAS **Credentials** tab.

3. Use `uaac token client get admin -s ADMIN-CLIENT-SECRET` to authenticate and obtain an access token for the admin client from the UAA server. UAAC stores the token in `~/uaac.yml`.

```
$ uaac token client get admin -s MyAdminPassword
```


4. Create a `notifications-admin` client with the required scopes.

```
$ uaac client add notifications-admin --authorized_grant_types client_credentials --authorities \
notifications.manage,notifications.write,notification_templates.write,notification_templates.read,critical_notifications.write
```

- `notifications.write`: send a notification. For example, you can send notifications to a user, space, or everyone in the system.
- `notifications.manage`: update notifications and assign templates for that notification.
- (Optional) `notification_templates.write`: create a custom template for a notification.
- (Optional) `notification_templates.read`: check which templates are saved in the database.

5. Log in using your newly created client:

```
$ uaac token client get notifications-admin
```

 **Note:** Stay logged in to this client to follow the examples in this topic.

### Register Notifications


 **Note:** To register notifications, you must have the `notifications.manage` scope on the client. To set critical notifications, you must have the `critical_notifications.write` scope.

You must register a notification before sending it. Using the token `notifications-admin` from the previous step, the following example registers two notifications with the following properties:

```
$ uaac curl https://notifications.user.example.com/notifications -X PUT --data '{ "source_name": "Cloud Ops Team",
"notifications": {
 "system-going-down": { "critical": true, "description": "Cloud going down" },
 "system-up": { "critical": true, "description": "Cloud back up" }
}
}'
```

- `source_name` has “Cloud Ops Team” set as the description.
- `system-going-down` and `system-up` are the notifications set.
- `system-going-down` and `system-up` are made `critical`, so no users can unsubscribe from that notification.

## Create a Custom Template

 **Note:** To view a list of templates, you must have the `notifications_templates.read` scope. To create a custom template, you must have the `notification_templates.write` scope.

A template is made up of a name, a subject, a text representation of the template you are sending for mail clients that do not support HTML, and an HTML version of the template.

The system provides a default template for all notifications, but you can create a custom template using the following curl command.

```
$ uaac curl https://notifications.user.example.com/templates -X POST --data \
'{"name":"site-maintenance","subject":"Maintenance: {{.Subject}}","text":"The site has gone down for maintenance. More information to follow {{.Text}}","html":"
The site has gone down for maintenance. More information to follow {{.HTML}}"}'
```

Variables that take the form `{{.}}` interpolate data provided in the send step before a notification is sent. Data that you can insert into a template during the send step include `{{.Text}}`, `{{.HTML}}`, and `{{.Subject}}`.

This curl command returns a unique template ID that can be used in subsequent calls to refer to your custom template. The result looks similar to this:

```
{"template-id": "E3710280-954B-4147-B7E2-AF5BF62772B5"}
```

Check all of your saved templates by running a curl command:

```
$ uaac curl https://notifications.user.example.com/templates -X GET
```

## Associate a Custom Template with a Notification

In this example, the `system-going-down` notification belonging to the `notifications-admin` client is associated with the template ID `E3710280-954B-4147-B7E2-AF5BF62772B5`. This is the template ID of the template we created in the previous section.

Associating a template with a notification requires the `notifications.manage` scope.

```
$ uaac curl https://notifications.user.example.com/clients/notifications-admin/notifications/system-going-down/template \
-X PUT --data '{"template": "E3710280-954B-4147-B7E2-AF5BF62772B5"}'
```

Any notification that does not have a custom template applied, such as `system-up`, defaults to a system-provided template.

## Send a Notification

 **Note:** To send a critical notification, you must have the `critical_notifications.write` scope. To send a non-critical notification, you must have the `notifications_write` scope.

You can send a notification to the following recipients:

- A user



- A space
- An organization
- All users in the system
- A UAA-scope
- An email address

For details, see the [Notifications V1 Documentation](#) in GitHub.

The following example sends the `system-going-down` notification described above to all users in the system.

```
$ uaac curl https://notifications.user.example.com/everyone -X POST --data \
'{"kind_id":"system-going-down","text":"The system is going down while we upgrade our storage","html":" THE SYSTEM IS DOWN

The system is going down while we upgrade our storage

","subject":"Upgrade to Storage","reply_to":"no-reply@example.com"}'
```

## Routing

The following topics provide information about managing routes and domains in Pivotal Application Service (PAS):

- [Enabling IPv6 for Hosted Applications](#)
- [Supporting WebSockets](#)
- [Configuring Load Balancer Healthchecks for Cloud Foundry](#)
- [Securing Traffic into Cloud Foundry](#)
- [Enabling TCP Routing](#)

## Enabling IPv6 for Hosted Applications

Page last updated:

The procedure described below allows apps deployed to Pivotal Application Service to be reached using IPv6 addresses.

**Note:** Amazon Web Services (AWS) EC2 instances currently do not support IPv6.

Pivotal Application Service system components use a separate DNS subdomain from hosted applications. These components currently support only IPv4 DNS resolved addresses. This means that although an IPv6 address can be used for application domains, the system domain must resolve to an IPv4 address.

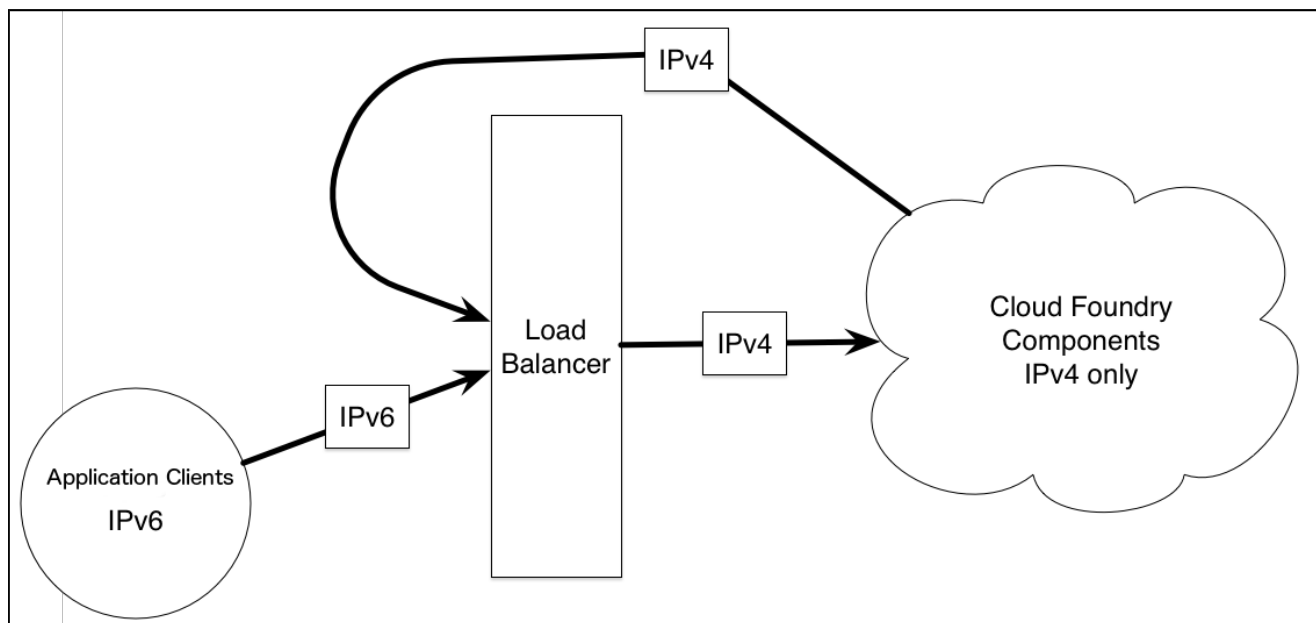
Complete the following steps to enable support for IPv6 application domains:

1. Set up an external load balancer for your Pivotal Application Service deployment. See [Using Your Own Load Balancer](#).
2. Configure DNS to resolve application domains to an IPv6 address on your external load balancer.

**Note:** Your IPv4 interface for the system domain and IPv6 interface for application domain can be configured on the same or different load balancers.

3. Configure the external load balancer to route requests for an IPv6 address to an IPv4 address as follows:
  - If you are using the HAProxy load balancer for SSL termination, route to its IPv4 address.
  - Otherwise, route directly to the IPv4 addresses of the Gorouters.

The following diagram illustrates how a single load balancer can support traffic on both IPv4 and IPv6 addresses for a Pivotal Application Service installation.



See [Routes and Domains](#) for more information about domains in Pivotal Application Service.

## Supporting WebSockets

Page last updated:

This topic explains how Cloud Foundry (CF) uses WebSockets, why developers use WebSockets in their applications, and how operators can configure their load balancer to support WebSockets.

Operators who use a load balancer to distribute incoming traffic across CF [router](#) instances must configure their load balancer for WebSockets. Otherwise, the [Loggregator](#) system cannot stream application logs to developers, or application event data and component metrics to third-party aggregation services. Additionally, developers cannot use WebSockets in their applications.

## Understand WebSockets

The WebSocket protocol provides full-duplex communication over a single TCP connection. Applications can use WebSockets to perform real-time data exchange between a client and a server more efficiently than HTTP.

CF uses WebSockets for the following metrics and logging purposes:

1. To stream all application event data and component metrics from the [Doppler](#) server instances to the [Traffic Controller](#)
2. To stream application logs from the Traffic Controller to developers using the Cloud Foundry Command Line Interface (cf CLI) or [Apps Manager](#)
3. To stream all application event data and component metrics from the Traffic Controller over the [Firehose](#) endpoint to external applications or services

For more information about these Loggregator components, see the [Overview of the Loggregator System](#) topic.

## Configure Your Load Balancer for WebSockets

To form a WebSocket connection, the client sends an HTTP request that contains an `Upgrade` header and other headers required to complete the WebSocket handshake. You must configure your load balancer to not upgrade the HTTP request, but rather to pass the `Upgrade` header through to the CF router. The procedures required to configure your load balancer depends on your IaaS and load balancer. The following list includes several possible approaches:

- Some load balancers can recognize the `Upgrade` header and pass these requests through to the CF router without returning the WebSocket handshake response. This may or may not be default behavior, and may require additional configuration.
- Some load balancers do not support passing WebSocket handshake requests containing the `Upgrade` header to the CF router. For instance, the Amazon Web Services (AWS) Elastic Load Balancer (ELB) does not support this behavior. In this scenario, you must configure your load balancer to forward TCP traffic to your CF router to support WebSockets. If your load balancer does not support TCP pass-through of WebSocket requests on the same port as other HTTP requests, you can do one of the following:
  - Configure your load balancer to listen on a non-standard port (the built-in CF load balancer listens on 8443 by default for this purpose), and forward requests for this port in TCP mode. Application clients must make WebSockets upgrade requests to this port. If you choose this strategy, you must follow the steps below in the [Set Your Loggregator Port](#) section of this topic
  - If a non-standard port is not acceptable, add a load balancer that will handle WebSocket traffic (or another IP on an existing load balancer) and configure it to listen on standard ports 80 and 443 in TCP mode. Configure DNS with a new hostname, such as `ws.cf.example.com`, to be used for WebSockets. This hostname should resolve to the new load balancer interface.



**Note:** Regardless of your IaaS and configuration, you must configure your load balancer to send the X-Forwarded-For and X-Forwarded-Proto headers for non-WebSocket HTTP requests on ports 80 and 443. See the [Securing Traffic into Cloud Foundry](#) topic for more information.

## Set Your Loggregator Port

By default, PCF assigns port 443 for TCP/WebSocket communications. If you have configured your load balancer to use a port other than 443 for TCP/WebSocket traffic, you must edit the **Loggregator Port** field in the **Networking** pane of the PAS tile.

HTTP Headers to Log

HAProxy Request Max Buffer Size \*

16384

HAProxy Protected Domains

HAProxy Trusted CIDRs

Loggregator Port

Default is 443. Enter a new value to override the default, for instance if port 443 on your load balancer is used for other traffic.

## Configuring Load Balancer Healthchecks for Cloud Foundry Routers

Page last updated:

This topic describes how to configure load balancer healthchecks for Cloud Foundry (CF) routers to ensure that the load balancer only forwards requests to healthy router instances. You can also configure a healthcheck for your HAProxy if your deployment uses the HAProxy component.

In environments that require high availability, operators must configure their own redundant load balancer to forward traffic directly to the CF routers. In environments that do not require high availability, operators can skip the load balancer and configure DNS to resolve the CF domains directly to a single instance of a router.

### Add Healthcheck Endpoints for Routers

Configure your load balancer to use the following HTTP healthcheck endpoints. Add the IP addresses of all router instances along with their corresponding port and path.

- HTTP Router (Gorouter): `http://GOROUTER_IP:8080/health`
- TCP Router: `http://TCP_ROUTER_IP:80/health`

The configuration above assumes the default healthcheck ports for the CF routers. To modify these ports, see the sections below.

### Add a Healthcheck Endpoint for HAProxy

If you have deployed one or more instances of HAProxy between your infrastructure load balancer and Gorouters, configure your infrastructure load balancer to use the following HTTP healthcheck endpoint: `http://HAPROXY_IP:8080/health`.

The HAProxy is an optional component that provides some features that Gorouter does not and can be helpful for demonstrating horizontal scalability of the CF routers in environments where an infrastructure load balancer is not available.

### Set the Healthy and Unhealthy Threshold Properties for the Gorouter

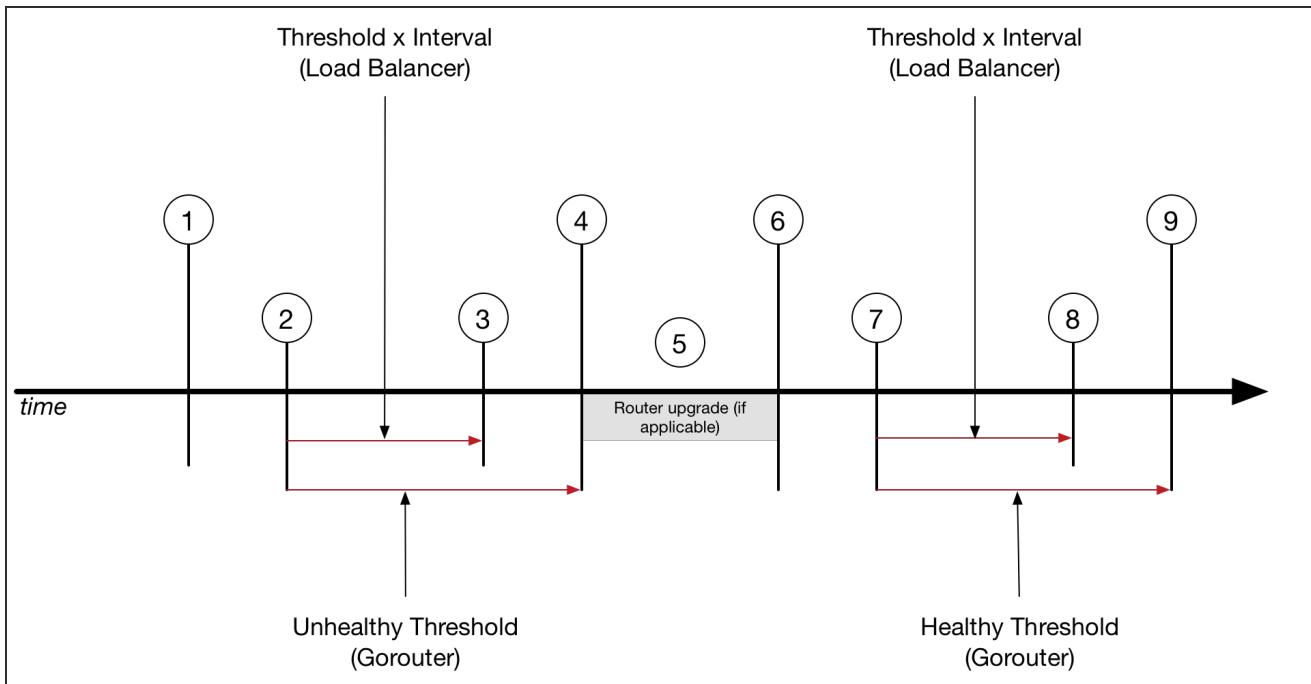
To maintain high availability during upgrades to the HTTP router, each router is upgraded on a rolling basis. During upgrade of a highly available environment with multiple routers, each router is shutdown, upgraded, and restarted before the next router is upgraded. This ensures that any pending HTTP request passed to the HTTP router are handled correctly.

Pivotal Application Service (PAS) uses the following properties:

- **Unhealthy Threshold:** Specifies the amount of time, in seconds, that the Router continues to accept connections before shutting down. During this period, the healthcheck reports `unhealthy` to cause load balancers to fail over to other routers. You should set this value greater than or equal to the maximum amount of time it could take your load balancer to consider a router instance unhealthy, given contiguous failed healthchecks.
- **Healthy Threshold:** Specifies the amount of time, in seconds, to wait until declaring the router instance started. This allows an external load balancer time to register the instance as `healthy`.

You can configure these properties from the **Settings > Network** tab.

The image and table below describe the behavior of the load balancer health checks when a router shuts down and is restarted.



| Step | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | A shutdown request is sent to the router.                                                                                                                                                                                                                                                                                                                                                        |
| 2    | The router receives shutdown request, which causes the following: <ul style="list-style-type: none"> <li>The router begins sending Service Unavailable responses to the load balancer health checks.</li> <li>The load balancer continues sending HTTP request to the router</li> </ul>                                                                                                          |
| 3    | The load balancer considers the router to be in an unhealthy state, which causes the load balancer to stop sending HTTP requests to the router.<br>The time between step 2 and 3 is defined by the values of the health check interval and threshold configured on the load balancer.                                                                                                            |
| 4    | The router shuts down.<br>The interval between step 2 and 4 is defined by the Unhealthy Threshold property of the Gorouter. In general, the value of this property should be longer than the value of the interval and threshold values (interval x threshold) of the load balancer. This additional interval ensures that any remaining HTTP requests are handled before the router shuts down. |
| 5    | If the router shutdown is initiated by an upgrade, the Gorouter software is upgraded.                                                                                                                                                                                                                                                                                                            |
| 6    | The router restarts. The router will return Service Unavailable responses for load balancer health checks for 20 seconds; during this time the routing table is preloaded.                                                                                                                                                                                                                       |
| 7    | The routers begins returning Service Available responses to the load balancer health check.                                                                                                                                                                                                                                                                                                      |
| 8    | The load balancer considers the router to be in a healthy state. The time between step 7 and 8 is specified by the health check interval and threshold configured for your load balancer (health check threshold x health check interval).                                                                                                                                                       |
| 9    | Shutdown and upgrade of the other router begins.                                                                                                                                                                                                                                                                                                                                                 |

## Securing Traffic into Cloud Foundry

Page last updated:

This topic describes the options for securing HTTP traffic into your Pivotal Application Service deployment with TLS certificates. You can configure the location where your deployment terminates TLS depending on your needs and certificate restrictions.

### Protocol Support

The Gorouter supports HTTP/HTTPS requests only. For more information about features supported by the Gorouter, see the [HTTP Routing](#) topic.


You can force HTTPS-only connections by enabling HSTS on HAProxy. For more information, see [Secure Apps Domain with HAProxy](#).

To secure non-HTTP traffic over TCP Routing, terminate TLS at your load balancer or at the application. See [TCP Routing](#) for details.

### TLS Termination Options for HTTP Routing

There are several options for terminating TLS for HTTP traffic. You can terminate TLS at the Gorouter, your load balancer, or at both.

The following table summarizes TLS termination options and which option to choose for your deployment.


 **Note:** To ensure traffic is sent to the platform securely, Pivotal recommends as a minimum that you terminate TLS at the Gorouter. You can optionally terminate TLS at the Load Balancer.

| If the following applies to you:                                                                                                                                                                                                                                                                                           | Then configure TLS termination at:             | Related topic and configuration procedure                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>You want the optimum balance of performance and security, and</li> <li>You want to make minimum changes to your load balancer, or</li> <li>You are deploying CF to AWS. For information about AWS limitations, see <a href="#">TLS Cipher Suite Support by AWS ELBs</a>.</li> </ul> | Gorouter only                                  | <a href="#">Terminating TLS at the Gorouter Only</a>              |
| <ul style="list-style-type: none"> <li>You require TLS termination at a load balancer, or</li> <li>You want the highest level of security, and</li> <li>You do not mind a slightly less performant deployment.</li> </ul>                                                                                                  | Load Balancer and Gorouter                     | <a href="#">Terminating TLS at the Load Balancer and Gorouter</a> |
| <ul style="list-style-type: none"> <li>You require TLS termination at a load balancer, and</li> <li>You prefer unencrypted traffic between the Load Balancer and the Gorouter.</li> </ul>                                                                                                                                  | Load Balancer only                             | <a href="#">Terminating TLS at the Load Balancer Only</a>         |
| <b>Optionally, if you are deploying HAProxy, and</b>                                                                                                                                                                                                                                                                       | <b>Then in addition, terminate SSL/TLS at:</b> | <b>Related topic and configuration procedure</b>                  |
| <ul style="list-style-type: none"> <li>You would like to secure traffic to the HAProxy.</li> </ul>                                                                                                                                                                                                                         | HAProxy                                        | <a href="#">Terminating SSL/TLS at HAProxy</a>                    |

### Certificate Requirements

The following requirements apply to the certificates you use to secure traffic into PAS

- You must obtain at least one TLS certificate for your environment.
  - In a production environment, use a signed TLS certificate (trusted) from a known certificate authority (CA).
  - In a development or testing environment, you can use a trusted CA certificate or a self-signed certificate. You can generate a self-signed certificate with `openssl` or a similar tool.

 Alternately, you can use the PAS Ops Manager interface to [generate a certificate](#) for you. Certificates generated in PAS are signed by the Ops Manager Certificate Authority. They are not technically self-signed, but they are sometimes referred to as “Self-Signed Certificates” in the Ops Manager UI and throughout this documentation.



- Certificates used in CF must be encoded in the PEM format.
- The Gorouter supports mutual TLS, and validates a client provided certificate chain against its CA certificates if one is provided in the TLS handshake, but does not require it. Depending on whether you choose to terminate at both the Load Balancer and the Gorouter, or at the Gorouter alone, the client certificate may be that of the load balancer or of the originating client.
- The certificate on the Gorouter must be associated with the correct hostname so that HTTPS can validate the request.
- If wildcard certificates are not supported for some or all of your domains, then configure termination requests at the [load balancer only](#). In this type of deployment, the load balancer passes unencrypted traffic to the Gorouter. As a result, you avoid having to reissue and reinstall certificates on the Gorouter for every app or UAA security zone.
- Extended Validation (EV) certificates support multiple hostnames, like SAN, but do not support wildcards. As the Gorouter has not been tested with EV certificates, if EV certificates are required, then terminate TLS at the [load balancer only](#).
- Given the dynamic and multi-tenant nature of PAS, use of wildcard domains is highly recommended to avoid the need for adding an additional certificate for each application.

## Multiple Certificates

In order to support custom domains on CF, an operator has to configure the Gorouter with a certificate that represents the domain. It is recommended that operators add a new certificate instead of reissuing a single certificate when adding TLS support for an additional domain. Using multiple certificates provides a security benefit in that it prevents clients from discovering all the custom domains of applications running on a CF platform.

The Gorouter supports SNI and can be configured with multiple certificates, each which may optionally include wildcard and alternative names. The Gorouter uses SNI to determine the correct certificate to present in a TLS handshake. It requires clients to support the SNI protocol by sending a server name outside the encrypted request payload. For clients that do not support SNI, the Gorouter presents a default certificate. The default is the first certificate keypair in the Gorouter's configuration.

The Gorouter decides which certificate to provide in the TLS handshake as follows:

- If a client provides an SNI header with a ServerName that matches to a configured certificate keypair, the Gorouter returns the matching certificate.
- If a client provides an SNI header with a ServerName that does not match a configured certificate keypair, the Gorouter returns the default certificate.

The first certificate keypair listed is used as the default.

The Gorouter supports both RSA and ECDSA certificates in PEM encoding. In the case that a certificate chain is required, the order should be as follows: primary certificate, intermediate certificate, then root certificate.

## How to Configure Multiple Certificate Keypairs

To configure multiple HTTPS certificate keypairs for PAS, add each keypair along with a meaningful name in the applicable **Certificates and Private Keys for HAProxy and Router** fields of the **Networking** configuration screen in PAS. For more information, see the Deploying PAS topic for your platform. For example, see [Deploying PAS on GCP](#) if you are using GCP.

In PCF, multiple certificates configured for the Gorouter are also configured for HAProxy.

## TLS Cipher Suite Support

Some CF components like the Gorouter support additional TLS cipher suites to accommodate older clients. As a security best practice, only configure the TLS cipher suites that you need for your deployment.

### Default Gorouter Cipher Suites

By default, the Gorouter supports the following TLS cipher suites, both of which require TLS v1.2:

| RFC                                   | OpenSSL                     |
|---------------------------------------|-----------------------------|
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDHE-RSA-AES128-GCM-SHA256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDHE-RSA-AES256-GCM-SHA384 |

You can override the default cipher suites in the **TLS Cipher Suites for Router** and **Minimum version of TLS** fields in the **Networking** tab of the PAS tile. See the following procedures for either [Gorouter Only](#) or [Load Balancer and Gorouter](#) for more information about using custom SSL ciphers.

## TLS Cipher Suite Support by AWS Load Balancers

AWS Classic Load Balancers (formerly referred to as ELBs) support configuration of cipher suites for front-end connections with clients only. When configuring Classic Load Balancers to forward requests to Gorouters over TLS, operators may encounter a “Cipher Suite Mismatch” error. This is because the cipher suites supported by Classic Load Balancers for TLS handshakes with backends (Gorouters in this case) are hardcoded, undocumented, and do not support the Gorouter default cipher suites.

Operators have two options:

- Configure Classic Load Balancer listeners in TCP mode so that TCP connections from clients are passed through the Classic Load Balancer to Gorouters on port 443. Then Gorouters are the first point of TLS termination.
- If you require TLS termination at an AWS load balancer in addition to terminating at the Gorouter, use [AWS Application Load Balancers \(ALBs\)](#) [↗](#) that support the Gorouter default cipher suites.

## TLS v1.2

The following cipher suites are optionally supported for TLS v1.2 only:

| RFC                                     | OpenSSL                       |
|-----------------------------------------|-------------------------------|
| TLS_RSA_WITH_AES_128_GCM_SHA256         | AES128-GCM-SHA256             |
| TLS_RSA_WITH_AES_256_GCM_SHA384         | AES256-GCM-SHA384             |
| TLS_ECDHE_ECDSA_WITH_RC4_128_SHA        | ECDHE-ECDSA-RC4-SHA           |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA    | ECDHE-ECDSA-AES128-SHA        |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA    | ECDHE-ECDSA-AES256-SHA        |
| TLS_ECDHE_RSA_WITH_RC4_128_SHA          | ECDHE-RSA-RC4-SHA             |
| TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA     | ECDHE-RSA-DES-CBC3-SHA        |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA      | ECDHE-RSA-AES128-SHA          |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA      | ECDHE-RSA-AES256-SHA          |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256   | ECDHE-RSA-AES128-GCM-SHA256   |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | ECDHE-ECDSA-AES128-GCM-SHA256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   | ECDHE-RSA-AES256-GCM-SHA384   |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | ECDHE-ECDSA-AES256-GCM-SHA384 |
| TLS_RSA_WITH_AES_128_CBC_SHA256         | AES128-SHA256                 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 | ECDHE-ECDSA-AES128-SHA256     |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256   | ECDHE-RSA-AES128-SHA256       |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305    | ECDHE-RSA-CHACHA20-POLY1305   |
| TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305  | ECDHE-ECDSA-CHACHA20-POLY1305 |

## TLS v1.0 and v1.1

The following cipher suites are optionally supported for TLS v1.0 and TLS v1.1 only:

| RFC                           | OpenSSL      |
|-------------------------------|--------------|
| TLS_RSA_WITH_RC4_128_SHA      | RC4-SHA      |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | DES-CBC3-SHA |
| TLS_RSA_WITH_AES_128_CBC_SHA  | AES128-SHA   |
| TLS_RSA_WITH_AES_256_CBC_SHA  | AES256-SHA   |

You can override the default cipher suites in the **TLS Cipher Suites for Router** and **Minimum version of TLS** fields in the **Networking** tab of the PAS tile. See the following procedures for either [Gorouter Only](#) or [Load Balancer and Gorouter](#) for more information about using custom SSL ciphers.

See [Golang Constants](#) [↗](#) and [OpenSSL Cipher Suites](#) [↗](#) for more information about supported ciphers.

**Note:** ECDSA ciphers require a certificate and key for DSA, as opposed to RSA.

## Mutual Authentication with Clients

Gorouter supports validation of client certificates in TLS handshakes with clients, also known as mutual authentication. Operators can choose whether Gorouter requests client certificates and when requesting certificates, whether or not to require them.

By default, Gorouter requests but does not require client certificates in TLS handshakes.

To configure Gorouter behavior for handling client certificates, select one of the options in the **Router behavior for Client Certificates** field of the **Networking** configuration screen in PAS.

- **Router does not request client certificates.** The Gorouter does not request client certificates in TLS handshakes so clients will not provide them and validation of client certificates does not occur. This option is incompatible with the XFCC configuration options **TLS terminated for the first time at HAProxy** and **TLS terminated for the first time at the Router** in PAS because these options require mutual authentication.
- **Router requests but does not require client certificates.** The Gorouter requests client certificates in TLS handshakes. The handshake will fail if the client certificate is not signed by a CA configured for the router. This is the default configuration.
- **Router requires client certificates.** The Gorouter requests and requires client certificates in TLS handshakes. The handshake will fail if a client cert is not provided or if the client certificate is not signed by a CA configured for the router.

The behavior controlled by this property is global; it applies to all requests received by Gorouters so configured.

If Gorouter is the first point of TLS termination (your load balancer does not terminate TLS, and passes the request through to Gorouter over TCP), consider the following:

- Only option **Router does not request client certificates** should be used with PAS, as the Gorouters are in that product receive requests for the system domain. Many clients of CF platform APIs do not present client certificates in TLS handshakes, so the first point of TLS termination for requests to the system domain must not request them.
- All options may be used for routers deployed with the Isolation Segment tile, as these only receive requests for app domains.
- Options **Router requests but does not require client certificates** and **Router requires client certificates** will trigger browsers to prompt users to select a certificate if the browser is not already configured with a certificate signed by one of the CAs configured for the router.

If Gorouter is not the first point of TLS termination, this property can be used to secure communications between the Load Balancer and Gorouter. The router must be configured with the CA used to sign the client certification the load balancer will present.

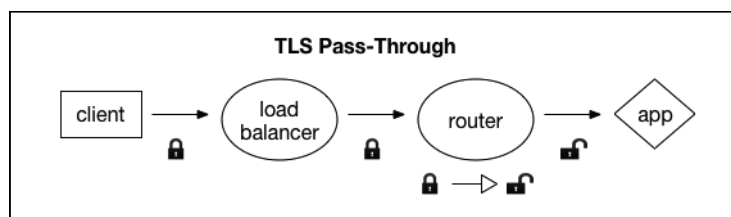
**Warning:** Requests to the platform will fail upon upgrade if your load balancer is configured to present a client certificate in the TLS handshake with Gorouter but Gorouter has not been configured with the certificate authority used to sign it. To mitigate this issue, select **Router does not request client certificates** for **Router behavior for Client Certificate Validation** in the **Networking** pane or configure the router with the appropriate CA.

## Terminating TLS at the Gorouter Only

In this configuration, the load balancer does not terminate TLS for CF domains at all. Instead, it passes through the underlying TCP connection to the Gorouter.

This option is the recommended and more performant option, establishing and terminating a single TLS connection.

The following diagram illustrates communication between the client, load balancer, Gorouter, and app.



Traffic between the load balancer and the Gorouter is encrypted only if the client request is encrypted.

## About HTTP Header Forwarding


If you terminate TLS at the Gorouter only, your load balancer does not send HTTP headers.

The Gorouter appends the `X-Forwarded-For` and `X-Forwarded-Proto` headers to requests forwarded to applications and platform system components.

`X-Forwarded-For` is set to the IP address of the source. Depending on the behavior of your load balancer, this may be the IP address of your load balancer. For Gorouter to deliver the IP address of the client to applications, configure your load balancer to forward the IP address of the client or configure your load balancer to send the client IP address using the PROXY protocol.

`X-Forwarded-Proto` provides the scheme of the HTTP request from the client. The scheme is HTTP if the client made a request on port 80 (unencrypted) or HTTPS if the client made a request on port 443 (encrypted). Gorouter sanitizes the `X-Forwarded-Proto` header based on the settings of the `router.sanitize_forwarded_proto` and `router.force_forwarded_proto_https` manifest properties as follows:

- `router.sanitize_forwarded_proto: true` and `router.force_forwarded_proto_https: true` :  
Gorouter sets the value of `X-Forwarded-Proto` header to `HTTPS` in requests forwarded to backends.
- `router.sanitize_forwarded_proto: true` and `router.force_forwarded_proto_https: false` :  
Gorouter strips the `X-Forwarded-Proto` header when present in requests from front-end clients. When the request is received on port 80 (unencrypted), Gorouter sets the value of this header to `HTTP` in requests forwarded to backends, When the request is received on port 443 (encrypted), Gorouter sets the value of this header to `HTTPS`.
- `router.sanitize_forwarded_proto: false` and `router.force_forwarded_proto_https: true` :  
Gorouter passes through the header as received from the load balancer, without modification.
- `router.sanitize_forwarded_proto: false` and `router.force_forwarded_proto_https: false` :  
Gorouter passes through the header as received from the load balancer, without modification.

 **Note:** If Gorouter is the first point of TLS, we recommend setting `router.sanitize_forwarded_proto: true` and `router.force_forwarded_proto_https: false` to secure against header spoofing.

For more information about HTTP headers in Cloud Foundry, see the [HTTP Headers](#) section of *HTTP Routing*. For information about configuring the forwarding of client certificates, see the [Forward Client Certificate to Applications](#) section of *HTTP Routing*.

## Procedure: Gorouter Only

Perform the following steps to configure SSL termination on the Gorouter in Pivotal Cloud Foundry (PCF):

1. Configure your load balancer to pass through TCP requests from the client to the Gorouter.
2. Navigate to the Ops Manager Installation Dashboard.
3. Click the Pivotal Application Service (PAS) tile in the Installation Dashboard.
4. Click **Networking**.
5. For PCF deployments on OpenStack or vSphere, choose IP addresses for the Gorouters from the subnet configured for Ops Manager and enter them in the **Router IPs** field. Then configure your load balancer to forward requests for the above domains to these IP addresses. For more information, see the PAS networking configuration topic for [OpenStack](#) or [vSphere](#).
6. In the **Certificates and Private Keys for HAProxy and Routerfield**, click the **Add** button to define at least one certificate keypair for HAProxy and Router. For each certificate keypair that you add, assign a name, enter the PEM-encoded certificate chain and PEM-encoded private key. You can either upload your own certificate or generate an RSA certificate in PAS. For options and instructions on creating a certificate for your wildcard domains, see [Creating a Wildcard Certificate for PCF Deployments](#).
7. In the **Minimum version of TLS supported by HAProxy and Router**, select the minimum version of TLS to use in Gorouter communications. The Gorouter uses TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Cipher Suites](#).
8. Under **HAProxy forwards requests to Router over TLS**, select **Disable**.
9. If you want to use a specific set of TLS ciphers for the Gorouter, configure **TLS Cipher Suites for Router**. Enter an ordered, colon-separated list of TLS cipher suites in the OpenSSL format. For example, if you have selected support for an earlier version of TLS, you can enter cipher suites supported by this version. For a list of TLS ciphers supported by the Gorouter, see [Cipher Suites](#). Otherwise, leave the default values in this field.
10. (Optional) If you are not using SSL encryption or if you are using self-signed certificates, you can select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.



Use this checkbox only for development and testing environments. Do not select it for production environments.

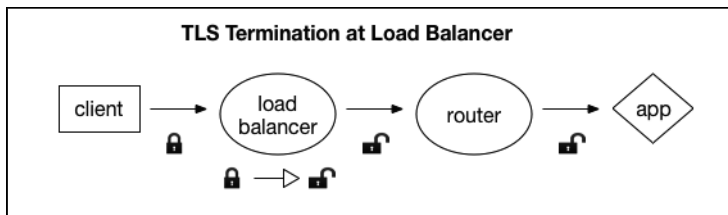
11. (Optional) If you do not want the Gorouter to accept any non-encrypted HTTP traffic, select the **Disable HTTP on HAProxy and Router** checkbox.
12. In the **Configure the CF Router support for the X-Forwarded-Client-Cert** headerfield, select the third option, **Strip the XFCC header when present and set it to the client certificate**.
13. Click **Save**.
14. In the PAS tile, click **Resource Config**.
15. In the **Instances** drop down for the **HAProxy** job, select **0** instances.
16. Click **Save**.

## Terminating TLS at the Load Balancer Only

In this configuration, your load balancer terminates TLS, and passes unencrypted traffic to the Gorouter, which routes it to your app. Traffic between the load balancer and the Gorouter is not encrypted.

This option is recommended if you cannot use SAN certificates and if you do not require traffic to be encrypted between the load balancer and the Gorouter.

The following diagram illustrates communication between the client, load balancer, Gorouter, and app.



## About HTTP Header Forwarding

If you terminate TLS at your load balancer, then you must also configure the load balancer to append the **X-Forwarded-For** and **X-Forwarded-Proto** HTTP headers to the HTTP traffic it passes to the Gorouter.

For more information about HTTP headers in CF, see [HTTP Headers](#). If you are configuring the forwarding of client certificates, see [Forward Client Certificate to Applications](#).

## Procedure: Load Balancer Only

Perform the following steps to configure SSL termination on the load balancer only in Pivotal Cloud Foundry (PCF):

1. Create an A record in your DNS that points to your load balancer IP address. The A record associates the **System Domain** and **Apps Domain** that you configure in the **Domains** section of the Pivotal Application Service (PAS) tile with the IP address of your load balancer.

For example, with `cf.example.com` as the main subdomain for your Cloud Foundry deployment and a load balancer IP address `198.51.100.1`, you must create an A record in your DNS that serves `example.com` and points `*.cf` to `198.51.100.1`.

| Name | Type | Data         | Domain      |
|------|------|--------------|-------------|
| *.cf | A    | 198.51.100.1 | example.com |

2. Navigate to the Ops Manager Installation Dashboard.
3. Click the PAS tile in the Installation Dashboard.
4. Click **Networking**.
5. For PCF deployments on OpenStack or vSphere, choose IP addresses for the Gorouters from the subnet configured for Ops Manager and enter them

in the **Router IPs** field. Then configure your load balancer to forward requests for the above domains to these IP addresses. For more information, see the PAS networking configuration topic for [OpenStack](#) or [vSphere](#).

6. In the **Certificates and Private Keys for HAProxy and Router** field, click the **Add** button to define one certificate keypair for HAProxy and Router. Since you have opted for unencrypted traffic behind the load balancer, then you can generate an RSA certificate in PAS.
7. In the **Minimum version of TLS supported by HAProxy and Router**, select the minimum version of TLS to use in HAProxy communications. HAProxy use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the HAProxy, see [Cipher Suites](#).
8. Under **HAProxy forwards requests to Router over TLS**, select **Disable**.
9. If you want to use a specific set of TLS ciphers for HAProxy, configure **TLS Cipher Suites for HAProxy**. Enter an ordered, colon-separated list of TLS cipher suites in the OpenSSL format. For example, if you have selected support for an earlier version of TLS, you can enter cipher suites supported by this version. Otherwise, leave the default values in this field.
10. (Optional) If you are not using SSL encryption or if you are using self-signed certificates, you can select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

💡 Use this checkbox only for development and testing environments. Do not select it for production environments.

11. (Optional) If you do not want HAProxy or the Gorouter to accept any non-encrypted HTTP traffic, select the **Disable HTTP on HAProxy and Router** checkbox.
12. In the **Configure the CF Router support for the X-Forwarded-Client-Cert** header field, select **Always forward the XFCC header in the request, regardless of the whether the client connection is mTLS**.
13. Click **Save**.
14. After you complete the configuration in PCF, add your certificate or certificates to your load balancer, and configure its listening port. The procedures vary depending on your IaaS.
15. Configure your load balancer to append the `X-Forwarded-For` and `X-Forwarded-Proto` headers to client requests.

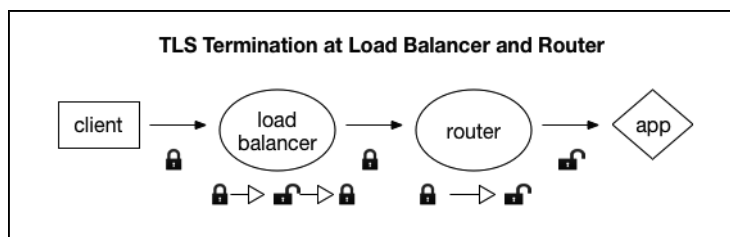
If the load balancer cannot be configured to provide the `X-Forwarded-For` header, the Gorouter will append it in requests forwarded to applications and system components, set to the IP address of the load balancer.

💡 **Note:** If the load balancer accepts unencrypted requests, it **must** provide the `X-Forwarded-Proto` header. Conversely, if the load balancer cannot be configured to send the `X-Forwarded-Proto` header, it should not accept unencrypted requests. Otherwise, applications and platform system components that require encrypted client requests will accept unencrypted requests when they should not accept them.

## Terminating TLS at the Load Balancer and Gorouter

In this configuration two TLS connections are established: one from the client to the load balancer, and another from the load balancer to the Gorouter. This configuration secures all traffic between the load balancer and the Gorouter.

The following diagram illustrates communication between the client, load balancer, Gorouter, and app.



This option is less performant, but allows for termination at a load balancer, as well as secure traffic between the load balancer and the Gorouter.

## Certificate Guidelines

In this deployment scenario, the following guidelines apply:

- Certificates for the PAS domains must be stored on the load balancer, as well as on the Gorouter.
- Generate certificates for your load balancer and the Gorouter with different keys. If the key for the certificate on the Gorouter is compromised, then the certificate on the load balancer is not at risk, and vice versa.
- If you choose to host only one certificate on the Gorouter and many on your load balancer, configure your load balancer with the CA and hostname with which to validate the certificate hosted by the Gorouter.

## About Hostname Verification

Hostname verification between the load balancer and the Gorouter is unnecessary when the load balancer is already configured with the Gorouter's IP address to correctly route the request.

If the load balancer uses DNS resolution to route requests to the Gorouters, then you should enable hostname verification.

## About HTTP Header Forwarding

If you terminate TLS at your load balancer, then you must configure the load balancer to append the `X-Forwarded-For` and `X-Forwarded-Proto` HTTP headers to requests it sends to the Gorouter.

If you terminate TLS at your load balancer but it does not support HTTP, such that it cannot append HTTP headers, a workaround exists. We recommend you use this workaround **only if your load balancer does not accept unencrypted requests**. Configure your load balancer to send the client IP address using the PROXY protocol, and enable PROXY in the Gorouter. As the `X-Forwarded-Proto` header will not be present, configure the Gorouter to force-set this header to 'HTTPS'.

For more information about HTTP headers in CF, see [HTTP Headers](#). If you are configuring the forwarding of client certificates, see [Forward Client Certificate to Applications](#).

## Procedure: Load Balancer and Gorouter

Perform the following steps to configure SSL termination on the Gorouter and load balancer in Pivotal Cloud Foundry (PCF):

1. Create an A record in your DNS that points to your load balancer IP address. The A record associates the **System Domain** and **Apps Domain** that you configure in the **Domains** section of the Pivotal Application Service (PAS) tile with the IP address of your load balancer.

For example, with `cf.example.com` as the main subdomain for your Cloud Foundry (CF) deployment and a load balancer IP address `198.51.100.1`, you must create an A record in your DNS that serves `example.com` and points `*.cf` to `198.51.100.1`.

| Name | Type | Data         | Domain      |
|------|------|--------------|-------------|
| *.cf | A    | 198.51.100.1 | example.com |

2. Navigate to the Ops Manager Installation Dashboard.
3. Click the PAS tile in the Installation Dashboard.
4. Click **Networking**.
5. For PCF deployments on OpenStack or vSphere, choose IP addresses for the Gorouters from the subnet configured for Ops Manager and enter them in the **Router IPs** field. Then configure your load balancer to forward requests for the above domains to these IP addresses. For more information, see the PAS networking configuration topic for [OpenStack](#) or [vSphere](#).
6. In the **Certificates and Private Keys for HAProxy and Routerfield**, click the **Add** button to define at least one certificate keypair for HAProxy and Router. For each certificate keypair that you add, assign a name, enter the PEM-encoded certificate chain and PEM-encoded private key. You can either upload your own certificate or generate an RSA certificate in PAS. For options and instructions on creating a certificate for your wildcard domains, see [Creating a Wildcard Certificate for PCF Deployments](#).
7. In the **Minimum version of TLS supported by HAProxy and Router**, select the minimum version of TLS to use in HAProxy and Gorouter communications. The Gorouter use TLS v1.2 by default. If you need to accommodate clients that use an older version of TLS, select a lower minimum version. For a list of TLS ciphers supported by the Gorouter, see [Cipher Suites](#).
8. If you are using **HAProxy**, complete the following steps:
  - a. Under **HAProxy forwards requests to Router over TLS**, select **Enable**.
  - b. In the **Certificate Authority for HAProxy Backend** field, specify the Certificate Authority (CA) that signed the certificate you configured in the

## Certificate and Private Key for HAProxy and Router field.


 If you used the **Generate RSA Certificate** link to generate a self-signed certificate, then the CA to specify is the Ops Manager CA, which you can locate at the `/api/v0/certificate_authorities` endpoint in the Ops Manager API.

- c. If you want to use a specific set of TLS ciphers for HAProxy, configure **TLS Cipher Suites for HAProxy**. Enter an ordered, colon-separated list of TLS cipher suites in the OpenSSL format. For example, if you have selected support for an earlier version of TLS, you can enter cipher suites supported by this version. Otherwise, leave the default values in this field.
  - d. In the **Configure the CF Router support for the X-Forwarded-Client-Cert header** field, select **Always forward the XFCC header in the request, regardless of the whether the client connection is mTLS**.
  - e. Proceed to step 11.
9. If you want to use a specific set of TLS ciphers for the Gorouter, configure **TLS Cipher Suites for Router**. Enter an ordered, colon-separated list of TLS cipher suites in the OpenSSL format. For example, if you have selected support for an earlier version of TLS, you can enter cipher suites supported by this version. For a list of TLS ciphers supported by the Gorouter, see [Cipher Suites](#). Otherwise, leave the default values in this field.
10. If you are not using HAProxy, complete the following steps:
- a. Under **HAProxy forwards requests to Router over TLS**, select **Disable**.
  - b. In the **Configure the CF Router support for the X-Forwarded-Client-Cert header** field, select any of the available options depending on your client application needs. For more information about XFCC header forwarding, see [Forward Client Certificate to Applications](#).
  - c. In the PAS tile, click **Resource Config**.
  - d. In the **Instances** drop down for the **HAProxy** job, select `0` instances.
  - e. Click **Save**.
11. (Optional) If you are not using SSL encryption or if you are using self-signed certificates, you can select **Disable SSL certificate verification for this environment**. Selecting this checkbox also disables SSL verification for route services.

 Use this checkbox only for development and testing environments. Do not select it for production environments.

12. (Optional) If you do not want HAProxy or the Gorouter to accept any non-encrypted HTTP traffic, select the **Disable HTTP on HAProxy and Router** checkbox.
13. Click **Save**.
14. After you complete the configuration in PCF, add your certificate or certificates to your load balancer, and configure its listening port. The procedures vary depending on your IaaS.
15. Configure your load balancer to append the `X-Forwarded-For` and `X-Forwarded-Proto` headers to client requests.

If you cannot configure the load balancer to provide the `X-Forwarded-For` header, the Gorouter appends it in requests forwarded to applications and system components, set to the IP address of the load balancer.

 **Note:** If the load balancer accepts unencrypted requests, it **must** provide the `X-Forwarded-Proto` header. Conversely, if the load balancer cannot be configured to send the `X-Forwarded-Proto` header, it should not accept unencrypted requests. Otherwise, applications and platform system components that require encrypted client requests will accept unencrypted requests when they should not accept them.



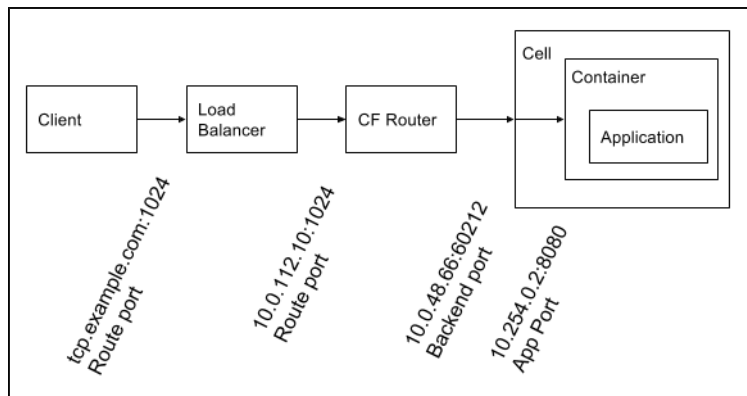
## Enabling TCP Routing

Page last updated:

This topic describes enabling TCP Routing for your Cloud Foundry (CF) deployment. This feature enables developers to run applications that serve requests on non-HTTP TCP protocols. You can use TCP Routing to comply with regulatory requirements that require your organization to terminate the TLS as close to your apps as possible so that packets are not decrypted before reaching the application level.

### Route Ports

The diagram below shows the layers of network address translation that occur in Cloud Foundry in support of TCP Routing. The descriptions step through an example work flow that covers route ports, backend ports, and app ports.



- A developer creates a TCP route for their application based on a TCP domain and a route port, and maps this route to one or more applications. See the [Creating Routes](#) topic for more information.
- Clients make requests to the route. DNS resolves the domain name to the load balancer.
- The load balancer listens on the port and forwards requests for the domain to the TCP routers. The load balancer must listen on a range of ports to support multiple TCP route creation. Additionally, Cloud Foundry must be configured with this range, so that the platform knows what ports can be reserved when developers create TCP routes.
- The TCP router can be dynamically configured to listen on the port when the route is mapped to an application. The domain the request was originally sent to is no longer relevant to the routing of the request to the application. The TCP router keeps a dynamically updated record of the backends for each route port. The backends represent instances of an application mapped to the route. The TCP Router chooses a backend using a round-robin load balancing algorithm for each new TCP connection from a client. As the TCP Router is protocol agnostic, it does not recognize individual requests, only TCP connections. All client requests transit the same connection to the selected backend until the client or backend closes the connection. Each subsequent connection triggers the selection of a backend.
- Because containers each have their own private network, the TCP router does not have direct access to application containers. When a container is created for an application instance, a port on the Cell VM is randomly chosen and iptables are configured to forward requests for this port to the internal interface on the container. The TCP router then receives a mapping of the route port to the Cell IP and port.
- The Diego Cell only routes requests to port `8080`, the App Port, on the container internal interface. The App Port is the port on which applications must listen.

### Pre-Deployment Steps

Before enabling TCP Routing, you must complete the following steps to set up networking requirements.

1. Choose a domain name from which your developers will create TCP routes for their applications. For example, create a domain which is similar to your app domain but prefixed by the TCP subdomain: `tcp.APPS-DOMAIN.com`
2. Configure DNS to resolve this domain name to the IP address of a highly-available load balancer that will forward traffic for the domain to the TCP routers. For more information, view the [Domains](#) topic. If you are operating an environment that does not require high-availability, configure DNS to resolve the TCP domain name you have chosen directly to a single instance of the TCP Router.
3. (Optional) Choose IP addresses for the TCP routers and configure your load balancer to forward requests for the domain you chose in the step above to these addresses. Skip this step if you have configured DNS to resolve the TCP domain name to an instance of the TCP Router. Review the Enable TCP Routing steps in the *Deploying PAS* topic for your IaaS to configure your IP addresses for your PCF deployment: [AWS](#), [OpenStack](#), or [vSphere](#).

4. (Optional) Decide on the number of TCP routes you want to support. For each TCP route, you must reserve a port. Configure your load balancer to forward the range of ports to the TCP routers. Skip this step if you have configured DNS to resolve the TCP domain name to an instance of the TCP Router.
5. Review the “Enable TCP Routing” steps in the *Deploying Pivotal Application Service* topic for your IaaS to configure your ports for your PCF deployment: [AWS](#), [OpenStack](#), or [vSphere](#).

## Post-Deployment Steps

In the following steps you use the [Cloud Foundry Command Line Interface](#) (cf CLI) to add the TCP shared domain and configure organization quotas to grant developers the ability to create TCP routes. This requires an admin user account.

### Configure CF with Your TCP Domain

After deployment, you must configure Cloud Foundry with the domain that you configured in the Pre-Deployment step above so that developers can create TCP routes from it.

1. Run `cf router-groups`. You should see `default-tcp` as a response.
2. Run `cf create-shared-domain` to create a shared domain and associate it with the router group.

```
$ cf create-shared-domain tcp.APPS-DOMAIN.com --router-group default-tcp
```

3. Run `cf domains`. Verify that next to your TCP domain, `TCP` appears under `type`.

### Configure a Quota for TCP Routes

Since TCP route ports are a limited resource in some environments, quotas are configured to allow creation of zero TCP routes by default. After you deploy Cloud Foundry, you can increase the maximum number of TCP routes for all organizations or for particular organizations and spaces. Because you reserve a route port for each TCP route, the quota for this resource is managed with the cf CLI command option `--reserved-route-ports`. See the [Creating and Modifying Quota Plans](#) topic for more information.

If you have a default quota that applies to all organizations, you can update it to configure the number of route ports that can be reserved by each organization.

```
$ cf update-quota QUOTA --reserved-route-ports X
```

To create a new organization quota that can be allocated to particular organizations, provide the following required quota attributes in addition to the number of reserved route ports:

```
$ cf create-quota QUOTA --reserved-route-ports X
```

You can also create a quota that governs the number of route ports that can be created in a particular space.

```
$ cf create-space-quota QUOTA --reserved-route-ports X
```

## Create a TCP Route

For instructions about creating a TCP Route, see the [Create a TCP Route with a Port](#) topic.

## Router Groups

In [Post-Deployment Steps](#), we describe that in order to create a domain from which to create TCP routes, it must be associated with the TCP Router Group. A router group is a cluster of identically configured routers. Router Groups were introduced as mechanism to support reservation of the same port for multiple TCP routes, thus increasing the capacity for TCP routes. However, only one router group is currently supported. In the [Pre-Deployment Steps](#),

we describe how an admin user can configure the port range available for TCP routes in preparation for deployment.

## Modify your TCP ports

After deployment, you can modify the range of ports available for TCP routes using `cf curl` commands, as demonstrated with the commands below. These commands require an admin user with the `routing.router_groups.read` and `routing.router_groups.write` scopes.

1. In a terminal window, run `cf curl /routing/v1/router_groups` to view the `reservable_ports` :

```
$ cf curl /routing/v1/router_groups
[
 {
 "guid": "9d1c1da9-ed63-45e8-45ee-256f8579455c",
 "name": "default-tcp",
 "type": "tcp",
 "reservable_ports": "60000-60098"
 }
]
```

2. Modify the `reservable_ports` :

```
$ cf curl /routing/v1/router_groups/f7392031-a488-4890-8835-c4a038a3bded -X PUT -d '{"reservable_ports":"1024-1199"}'
```

## Isolation Segments

The following topics provide information about managing isolation segments in Pivotal Application Service (PAS):

- [Managing Isolation Segments](#)
- [Routing for Isolation Segments](#)

## Managing Isolation Segments

This topic describes how operators can isolate deployment workloads into dedicated resource pools called isolation segments.

### Requirements

You must have the [v.6.26.0](#) version or later of the [Cloud Foundry Command Line Interface \(cf CLI\)](#) installed to manage isolation segments.

Target the API endpoint of your deployment with `cf api` and log in with `cf login` before performing the procedures in this topic. For more information, see the [Identifying the API Endpoint for your PAS Instance](#) topic.

### Overview


To enable isolation segments, an operator must install the PCF Isolation Segment tile by performing the procedures in the [Installing PCF Isolation Segment](#) topic. Installing the tile creates a single isolation segment.

After an admin creates a new isolation segment, the admin can then create and manage relationships between the orgs and spaces of a Cloud Foundry deployment and the new isolation segment.

## Create an Isolation Segment

Before you create an isolation segment in PCF, you must install the PCF Isolation Segment tile by performing the procedures in the [Installing PCF Isolation Segment](#) topic.

To register an isolation segment with Cloud Controller, use the cf CLI.

 **Note:** The isolation segment name used in the cf CLI command must match the value specified in the **Segment Name** field of the PCF Isolation Segment tile. If the names do not match, PCF fails to place apps in the isolation segment when apps are started or restarted in the space assigned to the isolation segment.

The following command creates an isolation segment named `my_segment`:

```
$ cf create-isolation-segment my_segment
```

If successful, the command returns an `OK` message:

```
Creating isolation segment my_segment as admin...
OK
```

## Retrieve Isolation Segment Information

The `cf isolation-segments`, `cf org`, and `cf space` commands retrieve information about isolation segments. The isolation segments you can see depends on your role, as follows:

- **Admins** see all isolation segments in the system.
- **Other users** only see the isolation segments that their orgs are entitled to.

### List Isolation Segments

The following request returns a list of the isolation segments that are available to you:

```
$ cf isolation-segments
```

For example, the command returns results similar to the following:

```
Getting isolation segments as admin...
OK

name orgs
my_segment org1, org2
```

## Display Isolation Segments Enabled for an Org

An admin can entitle an org to multiple isolation segments.

Run `cf org ORG-NAME` command to view the isolation segments that are available to an org. Replace `ORG-NAME` with the name of your org.

For example:

```
$ cf org my-org
```

The command returns results similar to the following:

```
Getting info for org my-org as user@example.com...

name: my-org
domains: example.com, apps.example.com
quota: paid
spaces: development, production, sample-apps, staging
isolation segments: my_segment, my_other_segment
```

## Show the Isolation Segment Assigned to a Space

Only one isolation segment can be assigned to a space.

Run `cf space SPACE-NAME` to view the isolation segment assigned to a space. Replace `SPACE-NAME` with the name of the space.


For example:

```
$ cf space staging
```

The command returns results similar to the following:

```
name: staging
org: my-org
apps:
services:
isolation segment: my_segment
space quota:
security groups: dns, p-mysql, p.mysql, pcf-redis, public_networks, rabbitmq, ssh-logging
```

## Delete an Isolation Segment

 **Note:** An isolation segment with deployed apps cannot be deleted.

Only admins can delete isolation segments.

Run `cf delete-isolation-segment SEGMENT-NAME` to delete an isolation segment. Replace `SEGMENT-NAME` with the name of the isolation segment. If successful, the command returns an `OK` message.

For example:

```
$ cf delete-isolation-segment my_segment
Deleting isolation segment my_segment as admin...
OK
```

## Manage Isolation Segment Relationships

The commands listed in the sections below manage the relationships between isolation segments, orgs, and spaces.

### Enable an Org to Use Isolation Segments


Only admins can enable orgs to use isolation segments. Run `cf enable-org-isolation ORG-NAME SEGMENT-NAME` to enable the use of an isolation segment. Replace `ORG-NAME` with the name of your org, and `SEGMENT-NAME` with the name of the isolation segment.

For example:

```
$ cf enable-org-isolation org2 my_segment
```

If an org is entitled to use only one isolation segment, that isolation segment does not automatically become the default isolation segment for the org. You must explicitly [set the default isolation segment](#) of an org.

### Disable an Org from Using Isolation Segments

 **Note:** You cannot disable an org from using an isolation segment if a space within that org is assigned to the isolation segment. Additionally, you cannot disable an org from using an isolation segment if the isolation segment is configured as the default for that org.

Run `cf disable-org-isolation ORG-NAME SEGMENT-NAME` to disable an org from using an isolation segment. Replace `ORG-NAME` with the name of your org, and `SEGMENT-NAME` with the name of the isolation segment.

For example:

```
$ cf disable-org-isolation org1 my_segment
```

If successful, the command returns an `OK` message:

```
Removing entitlement to isolation segment my_segment from org org1 as admin...
OK
```

### Set the Default Isolation Segment for an Org

*This section requires [cf CLI v6.29.0](#) or later.*

Only admins and org managers can set the default isolation segment for an org.

When an org has a default isolation segment, apps in its spaces belong to the default isolation segment unless you assign them to another isolation segment. You must restart running applications to move them into the default isolation segment.

Run `cf set-org-default-isolation-segment ORG-NAME SEGMENT-NAME` to set the default isolation segment for an org. Replace `ORG-NAME` with the name of your org, and `SEGMENT-NAME` with the name of the isolation segment.

For example:

```
$ cf set-org-default-isolation-segment org1 my_segment
Setting isolation segment my_segment to default on org org1 as admin...
OK
```

To display the default isolation segment for an org, use the `cf org` command.

## Assign an Isolation Segment to a Space

Admins and org managers can assign an isolation segment to a space. Apps in that space start in the specified isolation segment.

To assign an isolation segment to a space, you must first enable the space's org to use the isolation segment. See [Enable an Org to Use Isolation Segments](#)

Run `cf set-space-isolation-segment SPACE-NAME SEGMENT-NAME` to assign an isolation segment to a space. Replace `SPACE-NAME` with the name of the space, and `SEGMENT-NAME` with the name of the isolation segment.

For example:

```
$ cf set-space-isolation-segment space1 my_segment
```

## Reset the Isolation Segment Assignment for a Space

Admins can reset the isolation segment assigned to a space to use the org's default isolation segment.

Run `cf reset-space-isolation-segment SPACE-NAME` to assign the default isolation segment for an org to a space. Replace `SPACE-NAME` with the name of the space.

For example:

```
$ cf reset-space-isolation-segment space1
```



## Routing for Isolation Segments

Page last updated:

This topic describes how operators can configure and manage routing for isolation segments. Operators can deploy an additional set of routers for each isolation segment to handle requests for applications within the segment. This topic includes the following sections:

- [Overview](#)
- [Step 1: Create Networks](#)
- [Step 2: Configure Networks for Routers](#)
- [Step 3: Configure Additional Routers](#)
- [Step 4: Add Routers to Load Balancers](#)
- [Step 5: Configure DNS and Load Balancers](#)
- [Step 6: Configure Firewall Rules](#)
- [Additional GCP Information](#)
- [Sharding Routers for Isolation Segments](#)
- [Metrics for Routers Associated with Isolation](#)

For more information about how isolation segments work, see the [Isolation Segments](#) section of the *Cloud Foundry Security* topic. For more information about creating isolation segments, see the [Installing PCF Isolation Segment](#) topic.

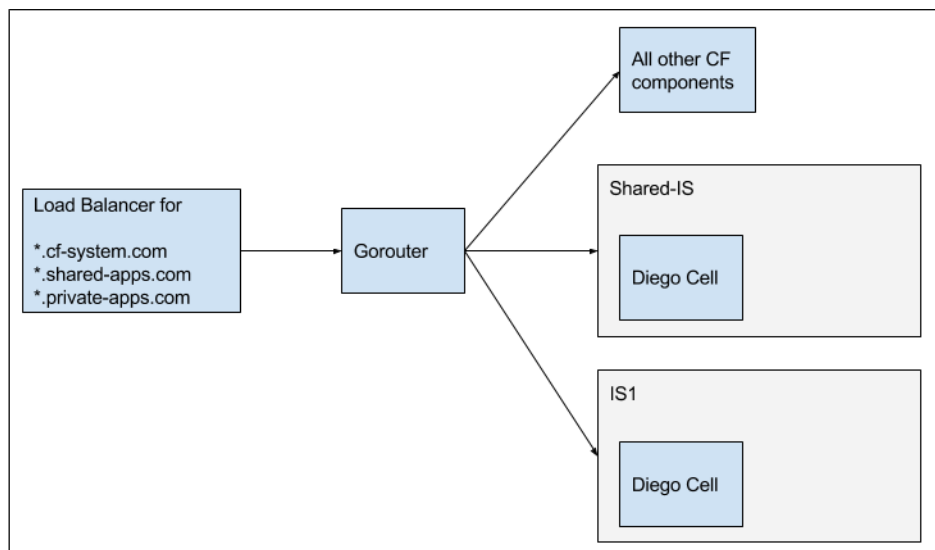
**Note:** The instructions in this topic assume you are using Google Cloud Platform (GCP). The procedures may differ on other IaaSes, but the concepts should be transferable.

## Overview

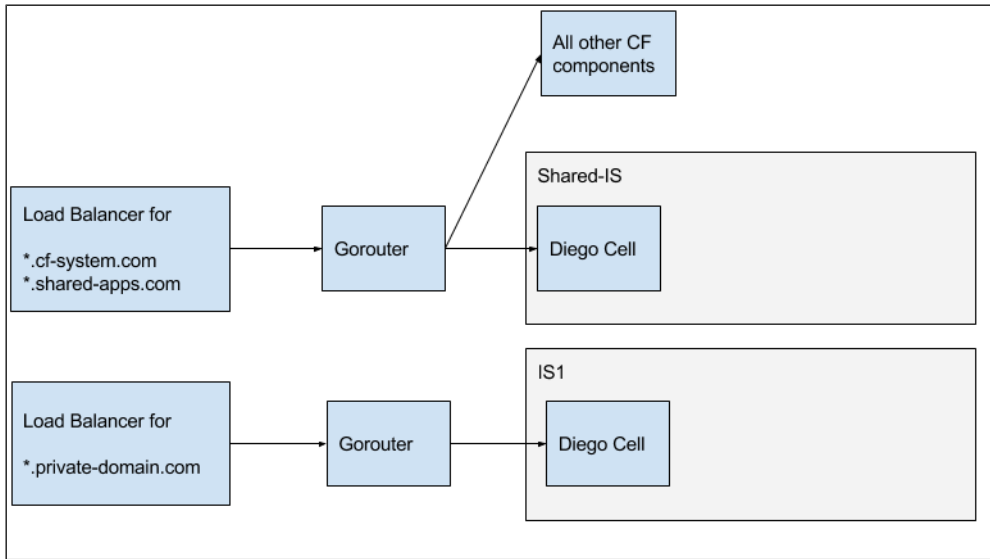
Isolation segments isolate the compute resources for one group of applications from another. However, these applications still share the same network resources. Requests for applications on all isolation segments, as well as for system components, transit the same load balancers and Cloud Foundry routers.

A shared Isolation Segment is the default isolation segment assigned to every org and space. This can be overwritten by assigning an explicit default for an organization. For more information about creating isolation segments, see the [Installing PCF Isolation Segment](#) topic.

The illustration below shows isolation segments sharing the same network resources.



Operators who want to prevent all isolation segments and system components from using the same network resources can deploy an additional set of routers for each isolation segment:



Use cases include:

- Requests for applications in an isolation segment must not share networking resources with requests for other applications.
- The Cloud Foundry management plane should only be accessible from a private network. As multiple IaaS load balancers cannot typically share the same pool of backends, such as Cloud Foundry routers, each load balancer requires an additional deployment of routers.

## Step 1: Create Networks

### Create a network or subnet for each isolation segment on your infrastructure

As an example, an operator who wants one shared isolation segment and one private segment could create one network named `sample-network` with two subnets named `sample-subnet-shared`, `sample-subnet-is1`.

The following diagram describes the network topology:

```
IaaS network: sample-network
|
|___ IaaS subnet: sample-subnet-shared
|
|___ IaaS subnet: sample-subnet-is1
```

Subnets do not generally span IaaS availability zones, so the same operator with two availability zones will need four subnets

```
IaaS network: sample-network
|
|___ IaaS subnet: sample-subnet-shared-az1
|
|___ IaaS subnet: sample-subnet-shared-az2
|
|___ IaaS subnet: sample-subnet-is1-az1
|
|___ IaaS subnet: sample-subnet-is1-az2
```

For more information about networks and subnets in GCP, see the [Using Networks and Firewalls](#) topic in the GCP documentation.

## Step 2: Configure Networks for Routers

To configure the subnets with Bosh, use [Bosh Cloud Config](#) subnets. Each subnet in the IaaS should correspond to a Bosh subnet that is labeled with the correct isolation segment

Navigate to the **Assign AZs and Networks** section of the PCF Isolation Segment tile to assign your isolation segment to the network you created in Step 1.

See the [Installing PCF Isolation Segment](#) topic for more information.

## Step 3: Configure Additional Routers

Navigate to the **Resource Config** section of the PCF Isolation Segment tile and use the dropdown menu to set your **Router** instances to a number greater than zero. See the [Installing PCF Isolation Segment](#) topic for more information.

## Step 4: Add Routers to Load Balancer

If your IaaS supports it, navigate to the **Resource Config** section of the PCF Isolation Segment tile and enter the name of your load balancer under **Load Balancers**. See the documentation specific to your IaaS in [Installing Pivotal Cloud Foundry](#) for more information. If your IaaS does not support this configuration, you must create static IP addresses and assign them to your load balancer out of band.

## Step 5: Configure DNS and Load Balancers

Create a separate domain name for each router instance group, and configure DNS to resolve these domain names to a load balancer that routes requests to the matching routers.

 **Note:** You must configure your load balancers to forward requests for a given domain to one router instance group only.

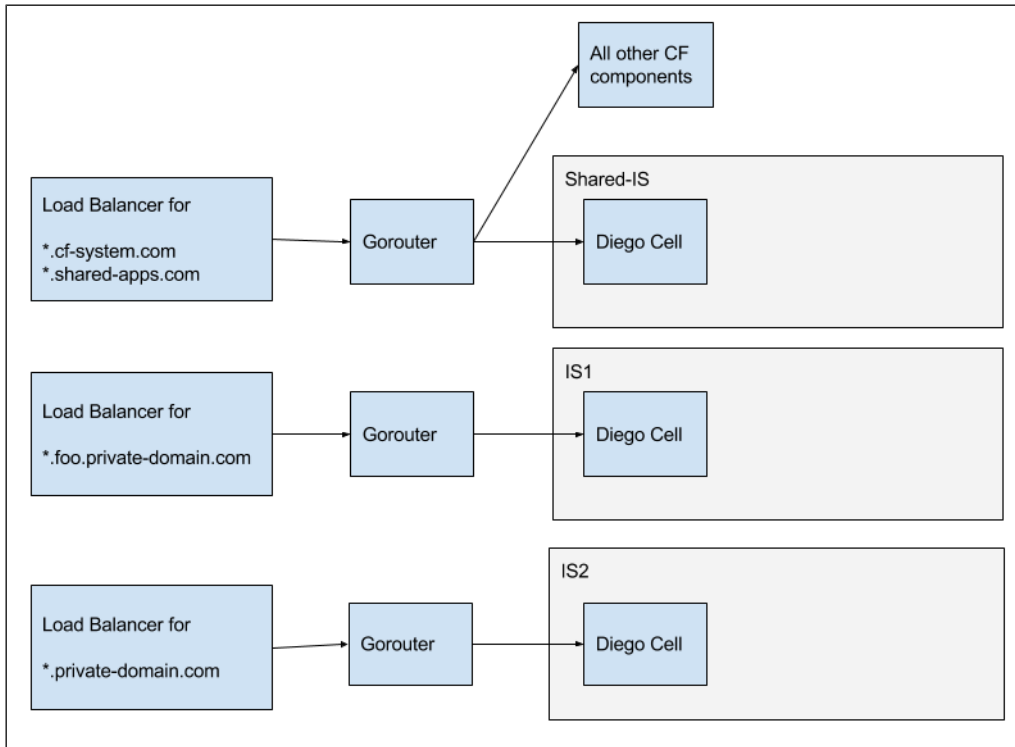
As router instance groups may be responsible for separate isolation segments, and an application may be deployed to only one isolation segment, requests should only reach a router that has access to the applications for that domain name. Load balancing requests for a domain across more than one router instance group can result in request failures unless all the router instance groups have access to the isolation segments where applications for that domain are deployed.

### Shared Domain Name

It is a common requirement for applications on separate isolation segments to be accessible at domain names that share a domain, such as `private-domain.com`. To achieve this configuration while also obeying the guideline for forwarding requests for a domain to only one router instance group, create a new Cloud Foundry domain for a needed subdomain, such as `*.foo.private-domain.com`.

The diagrams illustrate a topology with separate load balancers, but you could also use one load balancer with multiple interfaces. In this configuration:

- Requests for system domain `*.cf-system.com` and the shared domain `*.shared-apps.com` are forwarded to the routers for the shared isolation segment.
- Requests for private domain `*.foo.private-domain.com` are forwarded to the routers for IS1. Requests for private domain `*.private-domain.com` are forwarded to the routers for IS2.



## Step 6: Configure Firewall Rules

Configure firewall rules to allow for necessary ingress and egress traffic for private and shared isolation segments. Assuming a default deny-all rule, properly configuring firewall rules prevents a request with a spoofed Host header from being forwarded by a router to an application in a different isolation segment.

To configure firewall rules for isolation segment traffic, do the following:

1. Configure the firewall rules in the table below:

**Note:** Firewall rules are specific to each IaaS, so the exact definition of `Source` and `Destination` depends on the IaaS. For example, on GCP, a `Source` is a subnet and a `Destination` is a tag. On AWS, both `Source` and `Destination` are security groups.

| Rule Name                    | Source                    | Allowed Protocols/Ports           | Destination               | Reason                                                                            |
|------------------------------|---------------------------|-----------------------------------|---------------------------|-----------------------------------------------------------------------------------|
| <code>shared-to-bosh</code>  | Shared isolation segment  | <code>tcp</code>                  | BOSH Director             | BOSH Agent on VMs in the shared isolation segment to reach BOSH Director          |
| <code>bosh-to-shared</code>  | BOSH Director             | <code>tcp</code>                  | Shared isolation segment  | BOSH director to control VMs in the shared isolation segment                      |
| <code>shared-internal</code> | Shared isolation segment  | <code>tcp</code>                  | Shared isolation segment  | VMs within the shared isolation segment to reach one another                      |
| <code>shared-to-is1</code>   | Shared isolation segment  | <code>tcp:1801,8853</code>        | Private isolation segment | Diego BBS in shared isolation segment to reach Cells in private isolation segment |
| <code>is1-to-bosh</code>     | Private isolation segment | <code>tcp:4222,25250,25777</code> | BOSH Director             | BOSH agent on VMs in private isolation segment to reach BOSH Director             |
| <code>is1-internal</code>    | Private isolation segment | <code>tcp</code>                  | Private isolation segment | VMs within private isolation segment to reach one another                         |
|                              |                           |                                   |                           |                                                                                   |

|                            |                           |                                                                                                                                                                                                                                                                              |                          |                                                                                                                                                                                                        |
|----------------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>isl-to-shared</code> | Private isolation segment | <code>tcp:3000,3457,4003<br/>4103,4222,4443,8080<br/>8082,8083,8443,8844<br/>8853,8889,8891<br/>9022,9023,9090,9091</code><br>See <a href="#">Port Reference Table</a> for information about the processes that use these ports and their corresponding manifest properties. | Shared isolation segment | Diego Cells in private isolation segment to reach BBS, Auctioneer, and CredHub in shared isolation segment. Loggregator Agent to reach Traffic Controller. Routers to reach NATS, UAA, and Routing API |
|----------------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

2. (Optional) Configure the firewall rules in the table below:

| Rule Name                      | Source                                     | Allowed Protocols/Ports | Destination               | Reason                                                                                                                                                           |
|--------------------------------|--------------------------------------------|-------------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>jumpbox-to-isl</code>    | Jumpbox VM                                 | <code>tcp:22</code>     | Private isolation segment | Jumpbox VMs to reach private isolation segment through SSH or BOSH SSH.                                                                                          |
| <code>isl-to-jumpbox</code>    | Private isolation segment                  | <code>tcp</code>        | Jumpbox VM                | Private isolation segment to reach jumpbox VM. Opens reverse SSH or BOSH SSH tunnel from jumpbox VM to private isolation segment.                                |
| <code>diego-cell-egress</code> | Diego cell VM on private isolation segment | <code>tcp</code>        | Internet                  | If Diego Cells must download buildpacks to stage applications, allow egress traffic from all Diego Cell VMs on private isolation segments to reach the Internet. |

For more information about ports used by agents to communicate with BOSH, see [bosh-deployment](#) in GitHub.

For more information about networks and firewall rules for GCP, see [Using Subnetworks](#) in the GCP documentation.

## Port Reference Table

See the following table to understand which protocols and ports map to which processes and manifest properties for the `isl-to-shared` rule above.

| Protocol         | Port              | Process                 | Manifest Property                                                  |
|------------------|-------------------|-------------------------|--------------------------------------------------------------------|
| <code>tcp</code> | <code>3000</code> | Routing API             | <code>routing_api.port</code>                                      |
| <code>tcp</code> | <code>3457</code> | Doppler                 | <code>metron_endpoint.dropsonde_port</code>                        |
| <code>tcp</code> | <code>4003</code> | VXLAN Policy Agent      | <code>cf_networking.policy_server.internal_listen_port</code>      |
| <code>tcp</code> | <code>4103</code> | Silk Controller         | <code>cf_networking.silk_controller.listen_port</code>             |
| <code>tcp</code> | <code>4222</code> | NATS                    | <code>router.nats.port</code>                                      |
| <code>tcp</code> | <code>8080</code> | Diego file server       | <code>diego.file_server.listen_addr</code>                         |
| <code>tcp</code> | <code>8082</code> | Doppler gRPC            | <code>loggregator.doppler.grpc_port</code>                         |
| <code>tcp</code> | <code>8300</code> | Consul**                |                                                                    |
| <code>tcp</code> | <code>8301</code> | Consul**                |                                                                    |
| <code>tcp</code> | <code>8302</code> | Consul**                |                                                                    |
| <code>tcp</code> | <code>8443</code> | UAA                     | <code>uaa.ssl.port</code>                                          |
| <code>tcp</code> | <code>8844</code> | CredHub                 | <code>credhub.port</code>                                          |
| <code>tcp</code> | <code>8853</code> | BOSH DNS health         | <code>health.server.port</code> from <code>bosh-dns-release</code> |
| <code>tcp</code> | <code>8889</code> | Diego BBS               | <code>diego.rep.bbs.api_location</code>                            |
| <code>tcp</code> | <code>8891</code> | Diego Database (Locket) | <code>diego.locket.listen_addr</code>                              |
| <code>tcp</code> | <code>9022</code> | CC stager               | <code>capi.stager.cc.external_port</code>                          |

|     |      |             |                           |
|-----|------|-------------|---------------------------|
| tcp | 9023 | CC TPS      | capi.tps.cc.external_port |
| tcp | 9090 | CC uploader | http_port                 |
| tcp | 9091 | CC uploader | https_port                |
| udp | 8301 | Consul**    |                           |
| udp | 8302 | Consul**    |                           |
| udp | 8600 | Consul**    |                           |

\*\* [Consul documentation: Ports Used](#)

## Additional GCP Information


For more information, see the following:

- “Backend Services” in the GCP [documentation](#)
- BOSH Google Compute Engine CPI GitHub [repository](#)

## Sharding Routers for Isolation Segments

You can configure router sharding for isolation segments depending on your use case:

| Use Case                                       | Description                                                                                                                                                                                                                                                                            | How to Configure                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Securing apps that run in an isolation segment | To provide security guarantees in addition to the firewall rules described above, you can configure sharding of the Gorouter’s routing table, resulting in a router dedicated for an isolation segment having knowledge only of routes for applications in the same isolation segment. | <ol style="list-style-type: none"> <li>1. In the <b>Networking</b> configuration pane of the Pivotal Application Service (PAS) tile, select the checkbox labeled <b>Routers reject requests for Isolation Segments</b>.</li> <li>2. Set the <b>Router Sharding Mode</b> in the isolation segment tile to <b>Isolation Segment Only</b>.</li> </ol> |
| Deploying additional routers for PAS           | The flexibility of the configuration also supports deployment of a router that excludes all isolation segments.                                                                                                                                                                        | <ol style="list-style-type: none"> <li>1. In the <b>Networking</b> configuration pane of the PAS tile, select the checkbox labeled <b>Routers reject requests for Isolation Segments</b>.</li> <li>2. Set the <b>Router Sharding Mode</b> in the isolation segment tile to <b>No isolation Segment</b>.</li> </ol>                                 |

 **Note:** For compute isolation only, you can leave the **Routers reject requests for isolation segments** checkbox unselected in the PAS **Networking** pane. This is the default setting, which does not require any additional routers for the Isolation Segment tile.

## Metrics for Routers Associated with Isolation Segments

For metrics emitted by the Gorouter, metrics can be distinguished by the name of the job. For example, the following line is a metric emitted or `uptime`:

```
origin:"gorouter" eventType:ValueMetric timestamp:1491338040750977602 deployment:"superman.cf-app.com" job:"router_is1" index:"9a4b639c-8f0e-4b2b-b332-4161ee4646e6" ip:"10.0.16.23" valueMetric:<
```

## Monitoring PAS

This guide describes how Pivotal Cloud Foundry (PCF) operators can monitor their Pivotal Application Service (PAS) deployments. For information about monitoring Pivotal Container Service (PKS) deployments, see [Logging and Monitoring PKS](#).

For more information about logging and metrics in PCF, see [Overview of Logging and Metrics](#).

## Overview

This guide includes the following topics:

- [Key Performance Indicators](#): A list of Key Performance Indicators (KPIs) that operators may want to monitor with their PAS deployment to help ensure it is in a good operational state.
- [Key Capacity Scaling Indicators](#): A list of capacity scaling indicators that operators may want to monitor to determine when they need to scale their PAS deployments.
- [Selecting and Configuring a Monitoring System](#): Guidance for setting up PAS with monitoring platforms to continuously monitor component metrics and trigger health alerts.

## KPI Changes from PAS v2.1 to v2.2

This table highlights new and changed KPIs in PAS v2.2.

|                 |                                                                                                                                        |                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <i>Modified</i> | KPI: <code>Scalable Syslog Drain Bindings Count</code><br><br>The recommended scaling threshold for this metric was modified downward. | <a href="#">Link</a> |
| <i>Modified</i> | KPI: <code>Cloud Controller and Diego in Sync</code><br><br>The recommended alerting threshold for this metric was modified.           | <a href="#">Link</a> |

## Monitor PCF Services

For information about KPIs and metrics for PCF services, see the following topics:


- MySQL for PCF: [Monitoring MySQL for PCF](#).
- Pivotal Cloud Cache: See [Monitoring Pivotal Cloud Cache](#).
- Redis for PCF: [Monitoring Redis for PCF](#).
- RabbitMQ for PCF (pre-provisioned): See [Monitoring and KPIs for Pre-Provisioned RabbitMQ for PCF](#).
- RabbitMQ for PCF (on-demand): See [Monitoring and KPIs for On-Demand RabbitMQ for PCF](#).

## Key Performance Indicators

This topic describes Key Performance Indicators (KPIs) that operators may want to monitor with their Pivotal Application Service (PAS) deployment to help ensure it is in a good operational state.

The following PAS v2.2 KPIs are provided for operators to give general guidance on monitoring a PCF deployment using platform component and system (BOSH) metrics. Although many metrics are emitted from the platform, the following PAS v2.2 KPIs are high-signal-value metrics that can indicate emerging platform issues.

This alerting and response guidance has been shown to apply to most deployments. Pivotal recommends that operators continue to fine-tune the alert measures to their deployment by observing historical trends. Pivotal also recommends that operators expand beyond this guidance and create new, deployment-specific monitoring metrics, thresholds, and alerts based on learning from their deployments.

 **Note:** Thresholds noted as “dynamic” in the tables below indicate that while a metric is highly important to watch, the relative numbers to set threshold warnings at are specific to a given PAS deployment and its use cases. These dynamic thresholds should be occasionally revisited because the PCF foundation and its usage continue to evolve. See [Determine Warning and Critical Thresholds](#) for more information.

## Diego Auctioneer Metrics

### Auctioneer App Instance (AI) Placement Failures

| auctioneer.AuctioneerLRPAuctionsFailed |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                            | <p>The number of Long Running Process (LRP) instances that the auctioneer failed to place on Diego cells. This metric is cumulative over the lifetime of the auctioneer job.</p> <p><b>Use:</b> This metric can indicate that PAS is out of container space or that there is a lack of resources within your environment. This indicator also increases when the LRP is requesting an isolation segment, volume drivers, or a stack that is unavailable, either not deployed or lacking sufficient resources to accept the work.</p> <p>This metric is emitted on event, and therefore gaps in receipt of this metric can be normal during periods of no app instances being scheduled.</p> <p>This error is most common due to capacity issues, for example, if cells do not have enough resources, or if cells are going back and forth between a healthy and unhealthy state.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Counter (Integer)<br/> <b>Frequency:</b> During each auction</p> |
| Recommended measurement                | Per minute delta averaged over a 5-minute window                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Recommended alert thresholds           | <p><b>Yellow warning:</b> <math>\geq 0.5</math></p> <p><b>Red critical:</b> <math>\geq 1</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Recommended response                   | <ol style="list-style-type: none"> <li>1. To best determine the root cause, examine the Auctioneer logs. Depending on the specific error and resource constraint, you may also find a failure reason in the Cloud Controller (CC) API.</li> <li>2. Investigate the health of your Diego cells to determine if they are the resource type causing the problem.</li> <li>3. Consider scaling additional cells using Ops Manager.</li> <li>4. If scaling cells does not solve the problem, pull Diego brain logs and BBS node logs and contact Pivotal Support telling them that LRP auctions are failing.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                 |

### Auctioneer Time to Fetch Cell State

| auctioneer.AuctioneerFetchStateDuration |
|-----------------------------------------|
|-----------------------------------------|



| auctioneer.AuctioneerFetchStatesDuration |                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                              | <p>Time in ns that the auctioneer took to fetch state from all the Diego cells when running its auction.</p> <p><b>Use:</b> Indicates how the cells themselves are performing. Alerting on this metric helps alert that app staging requests to Diego may be failing.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge, integer in ns<br/> <b>Frequency:</b> During event, during each auction</p> |
| Recommended measurement                  | Maximum over the last 5 minutes divided by 1,000,000,000                                                                                                                                                                                                                                                                                                                                                 |
| Recommended alert thresholds             | <p><b>Yellow warning:</b> <math>\geq 2</math> s</p> <p><b>Red critical:</b> <math>\geq 5</math> s</p>                                                                                                                                                                                                                                                                                                    |
| Recommended response                     | <ol style="list-style-type: none"> <li>1. Check the health of the cells by reviewing the logs and looking for errors.</li> <li>2. Review IaaS console metrics.</li> <li>3. Pull Diego brain logs and cell logs and contact Pivotal Support telling them that fetching cell states is taking too long.</li> </ol>                                                                                         |

## Auctioneer App Instance Starts

| auctioneer.AuctioneerLRPAuctionsStarted |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                             | <p>The number of LRP instances that the auctioneer successfully placed on Diego cells. This metric is cumulative over the lifetime of the auctioneer job.</p> <p><b>Use:</b> Provides a sense of running system activity levels in your environment. Can also give you a sense of how many app instances have been started over time. The recommended measurement, below, can help indicate a significant amount of container churn. However, for capacity planning purposes, it is more helpful to observe deltas over a long time window.</p> <p>This metric is emitted on event, and therefore gaps in receipt of this metric can be normal during periods of no app instances being scheduled.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Counter (Integer)<br/> <b>Frequency:</b> During event, during each auction</p> |
| Recommended measurement                 | Per minute delta averaged over a 5-minute window                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Recommended alert thresholds            | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recommended response                    | <p>When observing a significant amount of container churn, do the following:</p> <ol style="list-style-type: none"> <li>1. Look to eliminate explainable causes of temporary churn, such as a deployment or increased developer activity.</li> <li>2. If container churn appears to continue over an extended period, pull logs from the Diego Brain and BBS node before contacting Pivotal support.</li> </ol> <p>When observing extended periods of high or low activity trends, scale up or down CF components as needed.</p>                                                                                                                                                                                                                                                                                                   |

## Auctioneer Task Placement Failures

| auctioneer.AuctioneerTaskAuctionsFailed |                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | <p>The number of Tasks that the auctioneer failed to place on Diego cells. This metric is cumulative over the lifetime of the auctioneer job.</p> <p><b>Use:</b> Failing Task auctions indicate a lack of resources within your environment and that you likely need to scale.</p> |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                  | <p>This indicator also increases when the Task is requesting an isolation segment, volume drivers, or a stack that is unavailable, either not deployed or lacking sufficient resources to accept the work.</p> <p>This metric is emitted on event, and therefore gaps in receipt of this metric can be normal during periods of no tasks being scheduled.</p> <p>This error is most common due to capacity issues, for example, if cells do not have enough resources, or if cells are going back and forth between a healthy and unhealthy state.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Counter (Float)<br/> <b>Frequency:</b> During event, during each auction</p> |
| <b>Recommended measurement</b>      | Per minute delta averaged over a 5-minute window                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Recommended alert thresholds</b> | <p><b>Yellow warning:</b> <math>\geq 0.5</math><br/> <b>Red critical:</b> <math>\geq 1</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Recommended response</b>         | <ol style="list-style-type: none"> <li>1. In order to best determine the root cause, examine the Auctioneer logs. Depending on the specific error or resource constraint, you may also find a failure reason in the CC API.</li> <li>2. Investigate the health of Diego cells.</li> <li>3. Consider scaling additional cells using Ops Manager.</li> <li>4. If scaling cells does not solve the problem, pull Diego brain logs and BBS logs for troubleshooting and contact Pivotal Support for additional troubleshooting. Inform Pivotal Support that Task auctions are failing.</li> </ol>                                                                                    |

## Diego BBS Metrics

### BBS Time to Run LRP Convergence

| bbs.ConvergenceLRPDURATION          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                  | <p>Time in ns that the BBS took to run its LRP convergence pass.</p> <p><b>Use:</b> If the convergence run begins taking too long, apps or Tasks may be crashing without restarting. This symptom can also indicate loss of connectivity to the BBS database.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Integer in ns)<br/> <b>Frequency:</b> During event, every 30 seconds when LRP convergence runs, emission should be near-constant on a running deployment</p>                                                                                   |
| <b>Recommended measurement</b>      | Maximum over the last 15 minutes divided by 1,000,000,000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Recommended alert thresholds</b> | <p><b>Yellow warning:</b> <math>\geq 10</math> s<br/> <b>Red critical:</b> <math>\geq 20</math> s</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Recommended response</b>         | <ol style="list-style-type: none"> <li>1. Check BBS logs for errors.</li> <li>2. Try vertically scaling the BBS VM resources up. For example, add more CPUs or memory depending on its <code>system.cpu</code> / <code>system.memory</code> metrics.</li> <li>3. Consider vertically scaling the PAS backing database, if <code>system.cpu</code> and <code>system.memory</code> metrics for the database instances are high.</li> <li>4. If that does not solve the issue, pull the BBS logs and contact Pivotal Support for additional troubleshooting.</li> </ol> |

### BBS Time to Handle Requests

| bbs.RequestLatency           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>The maximum observed latency time over the past 60 seconds that the BBS took to handle requests across all its API endpoints.</p> <p>Diego is now aggregating this metric to emit the max value observed over 60 seconds.</p> <p><b>Use:</b> If this metric rises, the PAS API is slowing. Response to certain cf CLI commands is slow if request latency is high.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Integer in ns)<br/> <b>Frequency:</b> 60 s</p>                                                                                                                                                                                                                       |
| Recommended measurement      | Average over the last 15 minutes divided by 1,000,000,000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recommended alert thresholds | <p><b>Yellow warning:</b> <math>\geq 5</math> s</p> <p><b>Red critical:</b> <math>\geq 10</math> s</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Check CPU and memory statistics in Ops Manager.</li> <li>2. Check BBS logs for faults and errors that can indicate issues with BBS.</li> <li>3. Try scaling the BBS VM resources up. For example, add more CPUs/memory depending on its <code>system.cpu</code> / <code>system.memory</code> metrics.</li> <li>4. Consider vertically scaling the PAS backing database, if <code>system.cpu</code> and <code>system.memory</code> metrics for the database instances are high.</li> <li>5. If the above steps do not solve the issue, collect a sample of the cell logs from the BBS VMs and contact Pivotal Support to troubleshoot further.</li> </ol> |

## Cloud Controller and Diego in Sync

| bbs.Domain.cf-apps           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Indicates if the <code>cf-apps</code> Domain is up-to-date, meaning that CF App requests from Cloud Controller are synchronized to <code>bbs.LRPsDesired</code> (Diego-desired AIs) for execution.</p> <ul style="list-style-type: none"> <li>• <code>1</code> means <code>cf-apps</code> Domain is up-to-date</li> <li>• No data received means <code>cf-apps</code> Domain is not up-to-date</li> </ul> <p><b>Use:</b> If the <code>cf-apps</code> Domain does not stay up-to-date, changes requested in the Cloud Controller are not guaranteed to propagate throughout the system. If the Cloud Controller and Diego are out of sync, then apps running could vary from those desired.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float)<br/> <b>Frequency:</b> 30 s</p> |
| Recommended measurement      | Value over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Recommended alert thresholds | <p><b>Yellow warning:</b> <i>N/A</i><br/> <b>Red critical:</b> <math>\neq 1</math></p> <p>The recommended threshold value represents a state where an up-to-date metric <code>1</code> has not been received for the entire 5-minute window.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Check the BBS and Clock Global (Cloud Controller clock) logs.</li> <li>2. If the problem continues, pull the BBS logs and contact Pivotal Support to say that the <code>cf-apps</code> domain is not being kept fresh.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## More App Instances Than Expected

| bbs.LRPsExtra                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Total number of LRP instances that are no longer desired but still have a BBS record. When Diego wants to add more apps, the BBS sends a request to the auctioneer to spin up additional LRPs. LRPsExtra is the total number of LRP instances that are no longer desired but still have a BBS record.</p> <p><b>Use:</b> If Diego has more LRPs running than expected, there may be problems with the BBS.</p> <p>Deleting an app with many instances can temporarily spike this metric. However, a sustained spike in <code>bbs.LRPsExtra</code> is unusual and should be investigated.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float)<br/> <b>Frequency:</b> 30 s</p> |
| Recommended measurement      | Average over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Recommended alert thresholds | <p><b>Yellow warning:</b> <math>\geq 5</math></p> <p><b>Red critical:</b> <math>\geq 10</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Review the BBS logs for proper operation or errors, looking for detailed error messages.</li> <li>2. If the condition persists, pull the BBS logs and contact Pivotal Support.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Fewer App Instances Than Expected

| bbs.LRPsMissing              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Total number of LRP instances that are desired but have no record in the BBS. When Diego wants to add more apps, the BBS sends a request to the auctioneer to spin up additional LRPs. LRPsMissing is the total number of LRP instances that are desired but have no BBS record.</p> <p><b>Use:</b> If Diego has less LRP running than expected, there may be problems with the BBS.</p> <p>An app push with many instances can temporarily spike this metric. However, a sustained spike in <code>bbs.LRPsMissing</code> is unusual and should be investigated.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float)<br/> <b>Frequency:</b> 30 s</p> |
| Recommended measurement      | Average over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Recommended alert thresholds | <p><b>Yellow warning:</b> <math>\geq 5</math></p> <p><b>Red critical:</b> <math>\geq 10</math></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Review the BBS logs for proper operation or errors, looking for detailed error messages.</li> <li>2. If the condition persists, pull the BBS logs and contact Pivotal Support.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Crashed App Instances

| bbs.CrashedActualLRPs |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description           | <p>Total number of LRP instances that have crashed.</p> <p><b>Use:</b> Indicates how many instances in the deployment are in a crashed state. An increase in <code>bbs.CrashedActualLRPs</code> can indicate several problems, from a bad app with many instances associated, to a platform issue that is resulting in app crashes. Use this metric to help create a baseline for your deployment. After you have a baseline, you can create a deployment-specific alert to notify of a spike in crashes above the</p> |

|                                     |                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <p>trend line. Tune alert values to your deployment.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float)<br/> <b>Frequency:</b> 30 s</p>                                                                                                                                                                                                            |
| <b>Recommended measurement</b>      | Average over the last 5 minutes                                                                                                                                                                                                                                                                                                                                |
| <b>Recommended alert thresholds</b> | <p><b>Yellow warning:</b> Dynamic<br/> <b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                        |
| <b>Recommended response</b>         | <ol style="list-style-type: none"> <li>1. Look at the BBS logs for apps that are crashing and at the cell logs to see if the problem is with the apps themselves, rather than a platform issue.</li> <li>2. Before contacting Pivotal Support, pull the BBS logs and, if particular apps are the problem, pull the logs from their Diego cells too.</li> </ol> |

## Running App Instances, Rate of Change

| 1hr average of <code>bbs.LRPsRunning</code> – prior 1hr average of <code>bbs.LRPsRunning</code> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                                                                              | <p>Rate of change in app instances being started or stopped on the platform. It is derived from <code>bbs.LRPsRunning</code> and represents the total number of LRP instances that are running on Diego cells.</p> <p><b>Use:</b> Delta reflects upward or downward trend for app instances started or stopped. Helps to provide a picture of the overall growth trend of the environment for capacity planning. You may want to alert on delta values outside of the expected range.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float)<br/> <b>Frequency:</b> During event, emission should be constant on a running deployment</p> |
| <b>Recommended measurement</b>                                                                  | derived=(1-hour average of <code>bbs.LRPsRunning</code> – prior 1-hour average of <code>bbs.LRPsRunning</code> )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Recommended alert thresholds</b>                                                             | <p><b>Yellow warning:</b> Dynamic<br/> <b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Recommended response</b>                                                                     | Scale components as necessary.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Diego Cell Metrics

### Remaining Memory Available — Cell Memory Chunks Available

| <code>rep.CapacityRemainingMemory</code> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                       | <p>Remaining amount of memory in MiB available for this Diego cell to allocate to containers.</p> <p><b>Use:</b> Indicates the available cell memory. Insufficient cell memory can prevent pushing and scaling apps.</p> <p>The strongest operational value of this metric is to understand a deployment's average app size and monitor/alert on ensuring that at least some cells have large enough capacity to accept standard app size pushes. For example, if pushing a 4 GB app, Diego would have trouble placing that app if there is no one cell with sufficient capacity of 4 GB or greater.</p> <p>As an example, Pivotal Cloud Ops uses a standard of 4 GB, and computes and monitors for the number of cells with at least 4 GB free. When the number of cells with at least 4 GB falls below a defined threshold, this is a scaling indicator alert to increase capacity. This <i>free chunk</i> count threshold should be tuned to the deployment size and the standard size of apps being pushed to the deployment.</p> <p><b>Origin:</b> Firehose</p> |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <b>Type:</b> Gauge (Integer in MiB)<br><b>Frequency:</b> 60 s<br><b>For alerting:</b> <ol style="list-style-type: none"> <li>Determine the size of a standard app in your deployment. This is the suggested value to calculate <i>free chunks</i> of Remaining Memory by.</li> <li>Create a script/tool that can iterate through each Diego Cell and do the following: <ol style="list-style-type: none"> <li>Pull the <code>rep.CapacityRemainingMemory</code> metric for each cell.</li> <li>Divide the values received by 1000 to get the value in Gigabytes (if desired threshold is GB-based).</li> <li>Compare recorded values to your minimum capacity threshold, and count the number of cells that have equal or greater than the desired amount of <i>free chunks</i> space.</li> </ol> </li> <li>Determine a desired scaling threshold based on the minimum amount of <i>free chunks</i> that are acceptable in this deployment given historical trends.</li> <li>Set an alert to indicate the need to scale cell memory capacity when the value falls below the desired threshold number.</li> </ol> <b>For visualization purposes:</b><br>Looking at this metric ( <code>rep.CapacityRemainingMemory</code> ) as a minimum value per cell has more informational value than alerting value. It can be an interesting heatmap visualization, showing average variance and density over time. |
| Recommended measurement      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recommended alert thresholds | <b>Yellow warning:</b> Dynamic<br><b>Red critical:</b> Dynamic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Recommended response         | <ol style="list-style-type: none"> <li>Assign more resources to the cells or assign more cells.</li> <li>Scale additional Diego cells using Ops Manager.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Alternative Metric           | If you are using <a href="#">PCF Healthwatch</a> , Pivotal recommends the metric <a href="#">healthwatch.Diego.AvailableFreeChunks</a> for this purpose.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Remaining Memory Available — Overall Remaining Memory Available

| <code>rep.CapacityRemainingMemory</code><br>(Alternative Use) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                   | <p>Remaining amount of memory in MiB available for this Diego cell to allocate to containers.</p> <p><b>Use:</b> Can indicate low memory capacity overall in the platform. Low memory can prevent app scaling and new deployments. The overall sum of capacity can indicate that you need to scale the platform. Observing capacity consumption trends over time helps with capacity planning.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Integer in MiB)<br/> <b>Frequency:</b> 60 s</p> |
| Recommended measurement                                       | Minimum over the last 5 minutes divided by 1024 (across all instances)                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended alert thresholds                                  | <b>Yellow warning:</b> $\leq 64$ GB<br><b>Red critical:</b> $\leq 32$ GB                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Recommended response                                          | <ol style="list-style-type: none"> <li>Assign more resources to the cells or assign more cells.</li> <li>Scale additional Diego cells via Ops Manager.</li> </ol>                                                                                                                                                                                                                                                                                                                                      |
| Alternative Metric                                            | If you are using <a href="#">PCF Healthwatch</a> , Pivotal recommends the metric <a href="#">healthwatch.Diego.AvailableFreeChunks</a> for this purpose.                                                                                                                                                                                                                                                                                                                                               |

## Remaining Disk Available

|  |
|--|
|  |
|--|


| rep.CapacityRemainingDisk    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Remaining amount of disk in MiB available for this Diego cell to allocate to containers.</p> <p><b>Use:</b> Low disk capacity can prevent app scaling and new deployments. Because Diego staging Tasks can fail without at least 6 GB free, the recommended red threshold is based on the minimum disk capacity across the deployment falling below 6 GB in the previous 5 minutes.</p> <p>It can also be meaningful to assess how many chunks of free disk space are above a given threshold, similar to <code>rep.CapacityRemainingMemory</code>.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Integer in MiB)<br/> <b>Frequency:</b> 60 s</p> |
| Recommended measurement      | Minimum over the last 5 minutes divided by 1024 (across all instances)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Recommended alert thresholds | <p><b>Yellow warning:</b> <math>\leq 12</math> GB</p> <p><b>Red critical:</b> <math>\leq 6</math> GB</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Assign more resources to the cells or assign more cells.</li> <li>2. Scale additional cells using Ops Manager.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Alternative Metric           | If you are using <a href="#">PCF Healthwatch</a> , Pivotal recommends the metric <a href="#">healthwatch.Diego.AvailableFreeChunks</a> for this purpose.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Cell Rep Time to Sync

| rep.RepBulkSyncDuration      |                                                                                                                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Time in ns that the Diego Cell Rep took to sync the ActualLRPs that it claimed with its actual garden containers.</p> <p><b>Use:</b> Sync times that are too high can indicate issues with the BBS.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float in ns)<br/> <b>Frequency:</b> 30 s</p> |
| Recommended measurement      | Maximum over the last 15 minutes divided by 1,000,000,000                                                                                                                                                                                                                                                   |
| Recommended alert thresholds | <p><b>Yellow warning:</b> <math>\geq 5</math> s</p> <p><b>Red critical:</b> <math>\geq 10</math> s</p>                                                                                                                                                                                                      |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Investigate BBS logs for faults and errors.</li> <li>2. If a particular cell or cells appear problematic, pull logs for the cells and the BBS logs before contacting Pivotal Support.</li> </ol>                                                                  |

## Unhealthy Cells

| rep.UnhealthyCell |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description       | <p>The Diego cell periodically checks its health against the garden backend. For Diego cells, <code>0</code> means healthy, and <code>1</code> means unhealthy.</p> <p><b>Use:</b> Set an alert for further investigation if multiple unhealthy Diego cells are detected in the given time window. If one cell is impacted, it does not participate in auctions, but end-user impact is usually low. If multiple cells are impacted, this can indicate a larger problem with Diego, and should be considered a more critical investigation need.</p> <p>Suggested alert threshold based on multiple unhealthy cells in the given time window.</p> |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <p>Although end-user impact is usually low if only one cell is impacted, this should still be investigated. Particularly in a lower capacity environment, this situation could result in negative end-user impact if left unresolved.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float, 0-1)<br/> <b>Frequency:</b> 30 s</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Recommended measurement      | Maximum over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Recommended alert thresholds | <p><b>Yellow warning:</b> = 1<br/> <b>Red critical:</b> &gt; 1</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Recommended response         | <ol style="list-style-type: none"> <li>Investigate Diego cell servers for faults and errors.</li> <li>If a particular cell or cells appear problematic: <ol style="list-style-type: none"> <li>Determine a time interval during which the metrics from the cell changed from healthy to unhealthy.</li> <li>Pull the logs that the cell generated over that interval. The Cell ID is the same as the BOSH instance ID.</li> <li>Pull the BBS logs over that same time interval.</li> <li>Contact Pivotal Support.</li> </ol> </li> <li>As a last resort, if you cannot wait for Pivotal Support, it sometimes helps to recreate the cell by running <code>bosh recreate</code>. See the <a href="#">BOSH documentation</a> for <code>bosh recreate</code> command syntax.</li> </ol> <div>  <b>warning:</b> Recreating a cell destroys its logs. To enable a root cause analysis of the cell's problem, save out its logs before running <code>bosh recreate</code>. </div> |

## Diego Locket Metrics

### Active Locks

| locket.ActiveLocks           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Total count of how many locks the system components are holding.</p> <p><b>Use:</b> If the ActiveLocks count is not equal to the expected value, there is likely a problem with Diego.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge<br/> <b>Frequency:</b> 60 s</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Recommended measurement      | Maximum over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Recommended alert thresholds | <p><b>Yellow warning:</b> N/A<br/> <b>Red critical:</b> ≠ 4</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Recommended response         | <ol style="list-style-type: none"> <li>Run <code>monit status</code> to inspect for failing processes.</li> <li>If there are no failing processes, then review the logs for the components using the Locket service: BBS, Auctioneer, TPS Watcher, and Routing API. Look for indications that only one of each component is active at a time.</li> <li>Focus triage on the BBS first: <ul style="list-style-type: none"> <li>A healthy BBS shows obvious activity around starting or claiming LRPs.</li> <li>An unhealthy BBS leads to the Auctioneer showing minimal or no activity. The BBS sends work to the Auctioneer.</li> <li>Reference the BBS-level Locket metric <a href="#">Locks Held by BBS</a>. A value of 0 indicates Locket issues at the BBS level.</li> </ul> </li> <li>If the BBS appears healthy, then check the Auctioneer to ensure it is processing auction payloads. <ul style="list-style-type: none"> <li>Recent logs for Auctioneer should show all but one of its instances are currently waiting on locks, and the active Auctioneer should show a record of when it last attempted to execute work. This attempt should correspond to app development activity, such as <code>cf push</code>.</li> </ul> </li> </ol> |



- Reference the Auctioneer-level Locket metric [Locks Held by Auctioneer](#). A value of 0 indicates Locket issues at the Auctioneer level.
- 5. The TPS Watcher is primarily active when app instances crash. Therefore, if the TPS Watcher is suspected, review the most recent logs.
- 6. If you are unable to resolve on-going excessive active locks, pull logs from the Diego BBS and Auctioneer VMs, which includes the Locket service component logs, and contact Pivotal Support.

## Locks Held by BBS

| bbs.LockHeld                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Whether a BBS instance holds the expected BBS lock (in Locket). 1 means the active BBS server holds the lock, and 0 means the lock was lost.</p> <p><b>Use:</b> This metric is complimentary to <a href="#">Active Locks</a>, and it offers a BBS-level version of the Locket metrics. Although it is emitted per BBS instance, only 1 active lock is held by BBS. Therefore, the expected value is 1. The metric may occasionally be 0 when the BBS instances are performing a leader transition, but a prolonged value of 0 indicates an issue with BBS.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge<br/> <b>Frequency:</b> Periodically</p> |
| Recommended measurement      | Maximum over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Recommended alert thresholds | <p><b>Yellow warning:</b> N/A</p> <p><b>Red critical:</b> ≠ 1</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Recommended response         | <ol style="list-style-type: none"> <li>Run <code>monit status</code> on the Diego database VM to check for failing processes.</li> <li>If there are no failing processes, then review the logs for BBS. <ul style="list-style-type: none"> <li>A healthy BBS shows obvious activity around starting or claiming LRPs.</li> <li>An unhealthy BBS leads to the Auctioneer showing minimal or no activity. The BBS sends work to the Auctioneer.</li> </ul> </li> <li>If you are unable to resolve the issue, pull logs from the Diego BBS, which include the Locket service component logs, and contact Pivotal Support.</li> </ol>                            |

## Locks Held by Auctioneer

| auctioneer.LockHeld          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Whether an Auctioneer instance holds the expected Auctioneer lock (in Locket). 1 means the active Auctioneer holds the lock, and 0 means the lock was lost.</p> <p><b>Use:</b> This metric is complimentary to <a href="#">Active Locks</a>, and it offers an Auctioneer-level version of the Locket metrics. Although it is emitted per Auctioneer instance, only 1 active lock is held by Auctioneer. Therefore, the expected value is 1. The metric may occasionally be 0 when the Auctioneer instances are performing a leader transition, but a prolonged value of 0 indicates an issue with Auctioneer.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge<br/> <b>Frequency:</b> Periodically</p> |
| Recommended measurement      | Maximum over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended alert thresholds | <p><b>Yellow warning:</b> N/A</p> <p><b>Red critical:</b> ≠ 1</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                              | <ol style="list-style-type: none"> <li>Run <code>monit status</code> on the Diego Database VM to check for failing processes.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recommended response | <ol style="list-style-type: none"> <li>If there are no failing processes, then review the logs for Auctioneer. <ul style="list-style-type: none"> <li>Recent logs for Auctioneer should show all but one of its instances are currently waiting on locks, and the active Auctioneer should show a record of when it last attempted to execute work. This attempt should correspond to app development activity, such as <code>cf push</code>.</li> </ul> </li> <li>If you are unable to resolve the issue, pull logs from the Diego BBS and Auctioneer VMs, which includes the Locket service component logs, and contact Pivotal Support.</li> </ol> |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Active Presences

| loket.ActivePresences        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Total count of active presences. Presences are defined as the registration records that the cells maintain to advertise themselves to the platform.</p> <p><b>Use:</b> If the Active Presences count is far from the expected, there might be a problem with Diego.</p> <p>The number of active presences varies according to the number of cells deployed. Therefore, during purposeful scale adjustments to PAS, this alerting threshold should be adjusted.</p> <p>Establish an initial threshold by observing the historical trends for the deployment over a brief period of time, Increase the threshold as more cells are deployed. During a rolling deploy, this metric shows variance during the BOSH lifecycle when cells are evacuated and restarted. Tolerable variance is within the bounds of the BOSH max inflight range for the instance group.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge<br/> <b>Frequency:</b> 60 s</p> |
| Recommended measurement      | Maximum over the last 15 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recommended alert thresholds | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended response         | <ol style="list-style-type: none"> <li>Ensure that the variance is not the result of an active rolling deploy. Also ensure that the alert threshold is appropriate to the number of cells in the current deployment.</li> <li>Run <code>monit status</code> to inspect for failing processes.</li> <li>If there are no failing processes, then review the logs for the components using the Locket service itself on Diego BBS instances.</li> <li>If you are unable to resolve the problem, pull the logs from the Diego BBS, which include the Locket service component logs, and contact Pivotal Support.</li> </ol>                                                                                                                                                                                                                                                                                                                                   |

## Diego Route Emitter Metrics


### Route Emitter Time to Sync

| route_emitter.RouteEmitterSyncDuration |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                            | <p>Time in ns that the active Route Emitter took to perform its synchronization pass.</p> <p><b>Use:</b> Increases in this metric indicate that the Route Emitter may have trouble maintaining an accurate routing table to broadcast to the Gorouters. Tune alerting values to your deployment based on historical data and adjust based on observations over time. The suggested starting point is <math>\geq 5</math> for the yellow threshold and <math>\geq 10</math> for the critical threshold. Pivotal has observed on its Pivotal Web Services deployment that above 10 s, the BBS may be failing.</p> |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <b>Origin:</b> Firehose<br><b>Type:</b> Gauge (Float in ns)<br><b>Frequency:</b> 60 s                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Recommended measurement</b>      | Maximum, per job, over the last 15 minutes divided by 1,000,000,000                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Recommended alert thresholds</b> | <b>Yellow warning:</b> Dynamic<br><b>Red critical:</b> Dynamic                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Recommended response</b>         | <p>If all or many jobs showing as impacted, there is likely an issue with Diego.</p> <ol style="list-style-type: none"> <li>1. Investigate the Route Emitter and Diego BBS logs for errors.</li> <li>2. Verify that app routes are functional by making a request to an app, pushing an app and pinging it, or if applicable, checking that your smoke tests have passed.</li> </ol> <p>If one or a few jobs showing as impacted, there is likely a connectivity issue and the impacted job should be investigated further.</p> |

## PAS MySQL KPIs

When PAS uses an internal MySQL database, as configured in the PAS tile **Settings** tab > **Databases** pane, the database cluster generates KPIs as described below.

 **Note:** This section assumes you are using the [Internal Databases - MySQL - MariaDB Galera Cluster](#) option as your system database.

### MySQL Server Availability

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <code>/mysql/available</code>                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>                  | <p>The MySQL Server is currently responding to requests, which indicates that the server is running.</p> <p><b>Use:</b> This metric is especially useful in single-node mode, where cluster metrics are not relevant. If the server does not emit heartbeats, it is offline.</p> <p><b>Origin:</b> Firehose<br/> <b>Envelope Type:</b> Gauge<br/> <b>Unit:</b> boolean<br/> <b>Frequency:</b> 30 s (default)</p> |
| <b>Recommended measurement</b>      | Average over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Recommended alert thresholds</b> | <b>Yellow warning:</b> N/A<br><b>Red critical:</b> < 1                                                                                                                                                                                                                                                                                                                                                           |
| <b>Recommended response</b>         | Run <code>mysql-diag</code> and check the MySQL Server logs for errors.                                                                                                                                                                                                                                                                                                                                          |

### Galera Cluster Node Readiness

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <code>/mysql/galera/wsrep_ready</code>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>             | <p>Shows whether each cluster node can accept queries. Returns only 0 or 1. When this metric is 0, almost all queries to that node fail with the error:</p> <pre>ERROR 1047 (08501) Unknown Command</pre> <p><b>Use:</b> Discover when nodes of a cluster have been unable to communicate and, thus, unable to accept transactions.</p> <p><b>Origin:</b> Firehose<br/> <b>Envelope Type:</b> Gauge<br/> <b>Unit:</b> boolean<br/> <b>Frequency:</b> 30 s (default)</p> |
| <b>Recommended measurement</b> | Average of values of each cluster node, over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                         |

|                              |                                                                                                                                                                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recommended alert thresholds | <b>Yellow warning:</b> $\leq 1.0$<br><b>Red critical:</b> 0 (cluster is down)                                                                                                                                                                                                                                 |
| Recommended response         | - Run <code>mysql-diag</code> and check the MySQL Server logs for errors.<br>- Make sure there has been no infrastructure event that affects intra-cluster communication.<br>- Ensure that <code>wsrep_ready</code> has not been set to off by using the query:<br><pre>SHOW STATUS LIKE 'wsrep_ready';</pre> |

## Galera Cluster Size

|                              |                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <code>/mysql/galera/wsrep_cluster_size</code>                                                                                                                                                                                                                                                                                                                                       |
| Description                  | <p>The number of cluster nodes with which each node is communicating normally.</p> <p><b>Use:</b> When running in a multi-node configuration, this metric indicates if each member of the cluster is communicating normally with all other nodes.</p> <p><b>Origin:</b> Firehose<br/> <b>Envelope Type:</b> Gauge<br/> <b>Unit:</b> count<br/> <b>Frequency:</b> 30 s (default)</p> |
| Recommended measurement      | (Average of the values of each node / cluster size), over the last 5 minutes                                                                                                                                                                                                                                                                                                        |
| Recommended alert thresholds | <b>Yellow warning:</b> $< 3.0$ (availability compromised)<br><b>Red critical:</b> $< 1.0$ (cluster unavailable)                                                                                                                                                                                                                                                                     |
| Recommended response         | Run <code>mysql-diag</code> and check the MySQL Server logs for errors.                                                                                                                                                                                                                                                                                                             |

## Galera Cluster Status

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <code>/mysql/galera/wsrep_cluster_status</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Description                  | <p>Shows the primary status of the cluster component that the node is in.</p> <p>Values are:</p> <ul style="list-style-type: none"> <li>- Primary = 1</li> <li>- Non-primary = 0</li> <li>- Disconnected = -1</li> </ul> <p>See: <a href="https://mariadb.com/kb/en/mariadb/galera-cluster-status-variables/">https://mariadb.com/kb/en/mariadb/galera-cluster-status-variables/</a></p> <p><b>Use:</b> Any value other than “Primary” indicates that the node is part of a nonoperational component. This occurs in cases of multiple membership changes that result in a loss of quorum.</p> <p><b>Origin:</b> Firehose<br/> <b>Envelope Type:</b> Gauge<br/> <b>Unit:</b> integer (see above)<br/> <b>Frequency:</b> 30 s (default)</p> |
| Recommended measurement      | Sum of each of the nodes, over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recommended alert thresholds | <b>Yellow warning:</b> $< 3$<br><b>Red critical:</b> $< 1$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended response         | - Check node status to ensure that they are all in working order and able to receive write-sets.<br>- Run <code>mysql-diag</code> and check the MySQL Server logs for errors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Connections per Second

|             |                                                                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <code>/mysql/net/connections</code>                                                                                                                                                                                           |
| Description | <p>Connections per second made to the server.</p> <p><b>Use:</b> If the number of connections drastically changes or if apps are unable to connect, there might be a network or app issue.</p> <p><b>Origin:</b> Firehose</p> |

|                                     | <code>/mysql/performance/connections</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <b>Unit:</b> count<br><b>Frequency:</b> 30 s (default)                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Recommended measurement</b>      | (Average of all nodes / max connections), over last 1 minute                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Recommended alert thresholds</b> | <b>Yellow warning:</b> > 80%<br><b>Red critical:</b> > 90%                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Recommended response</b>         | <ul style="list-style-type: none"> <li>- Run <code>mysql-diag</code> and check the MySQL Server logs for errors.</li> <li>- When approaching 100% of max connections, Apps may be experiencing times when they cannot connect to the database. The connections per second for the cluster vary based on application instances and app utilization. If this threshold is met or exceeded for an extended period of time, monitor app usage to ensure everything is behaving as expected.</li> </ul> |

## CPU Utilization Percent

|                                     | <code>/mysql/performance/cpu_utilization_percent</code>                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                  | <p>CPU time being consumed by the MySQL service.</p> <p><b>Use:</b> A node that experiences context switching or high CPU usage will become unresponsive. This also affects the ability of the node to report metrics.</p> <p><b>Origin:</b> Doppler/Firehose<br/> <b>Envelope Type:</b> Gauge<br/> <b>Unit:</b> percent<br/> <b>Frequency:</b> 30 s (default)</p> |
| <b>Recommended measurement</b>      | Average over last 10 minutes                                                                                                                                                                                                                                                                                                                                       |
| <b>Recommended alert thresholds</b> | <b>Yellow warning:</b> > 80%<br><b>Red critical:</b> > 90%                                                                                                                                                                                                                                                                                                         |
| <b>Recommended response</b>         | <ul style="list-style-type: none"> <li>- Run <code>mysql-diag</code> and check the MySQL Server logs for errors.</li> <li>- Determine what is using so much CPU. If it is from normal processes, update the service instance to use a plan with larger CPU capacity.</li> </ul>                                                                                    |

## Queries Delta

|                                     | <code>/mysql/performance/queries_delta</code>                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                  | <p>The number of statements executed by the server over the last 30 seconds.</p> <p><b>Use:</b> The server should always be processing some queries. If the server does not process any queries, the server is non-functional.</p> <p><b>Origin:</b> Doppler/Firehose<br/> <b>Envelope Type:</b> Gauge<br/> <b>Unit:</b> count<br/> <b>Frequency:</b> 30 s</p> |
| <b>Recommended measurement</b>      | Average over last 2 minutes                                                                                                                                                                                                                                                                                                                                    |
| <b>Recommended alert thresholds</b> | <b>Red critical:</b> 0                                                                                                                                                                                                                                                                                                                                         |
| <b>Recommended response</b>         | <ul style="list-style-type: none"> <li>- Run <code>mysql-diag</code> and check the MySQL Server logs for errors.</li> <li>- Investigate the MySQL server logs, such as the audit log, to understand why query rate changed and determine appropriate action.</li> </ul>                                                                                        |

## Gorouter Metrics

## Router File Descriptors

| gorouter.file_descriptors    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>The number of file descriptors currently used by the Gorouter job.</p> <p><b>Use:</b> Indicates an impending issue with the Gorouter. Without proper mitigation, it is possible for an unresponsive app to eventually exhaust available Gorouter file descriptors and cause route starvation for other apps running on PAS. Under heavy load, this unmitigated situation can also result in the Gorouter losing its connection to NATS and all routes being pruned.</p> <p>While a drop in <code>gorouter.total_routes</code> or an increase in <code>gorouter.ms_since_last_registry_update</code> helps to surface that the issue may already be occurring, alerting on <code>gorouter.file_descriptors</code> indicates that such an issue is impending.</p> <p>The Gorouter limits the number of file descriptors to 100,000 per job. Once the limit is met, the Gorouter is unable to establish any new connections.</p> <p>To reduce the risk of DDoS attacks, Pivotal recommends doing one or both of the following:</p> <ul style="list-style-type: none"> <li>• Within PAS, set <b>Max Connections Per Backend</b> to define how many requests can be routed to any particular app instance. This prevents a single app from using all Gorouter connections. The value specified should be determined by the operator based on the use cases for that foundation. For example, Pivotal sets the number of connections to 500 for Pivotal Web Services.</li> <li>• Add rate limiting at the load balancer level.</li> </ul> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge<br/> <b>Frequency:</b> 5 s</p> |
| Recommended measurement      | Maximum, per Gorouter job, over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Recommended alert thresholds | <p><b>Yellow warning:</b> 50,000 per job</p> <p><b>Red critical:</b> 60,000 per job</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Identify which app(s) are requesting excessive connections and resolve the impacting issues with these apps.</li> <li>2. If the above recommended mitigation steps have not already been taken, do so.</li> <li>3. Consider adding more Gorouter VM resources to increase the number of available file descriptors.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Router Exhausted Connections

| gorouter.backend_exhausted_conns |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                      | <p>The lifetime number of requests that have been rejected by the Gorouter VM due to the <code>Max Connections Per Backend</code> limit being reached across all tried backends. The limit controls the number of concurrent TCP connections to any particular app instance and is configured within PAS.</p> <p><b>Use:</b> Indicates that PAS is mitigating risk to other applications by self-protecting the platform against one or more unresponsive applications. Increases in this metric indicate the need to investigate and resolve issues with potentially unresponsive applications. A rapid rate of change upward is concerning and should be assessed further.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Counter (Integer)<br/> <b>Frequency:</b> 5 s</p> |
| Recommended measurement          | Maximum delta per minute, per Gorouter job, over a 5-minute window                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Recommended alert thresholds     | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                  | <ol style="list-style-type: none"> <li>1. If <code>gorouter.backend_exhausted_conns</code> spikes, first look to the Router Throughput metric</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recommended response | <code>gorouter.total_requests</code> to determine if this measure is high or low in relation to normal bounds for this deployment.                                                                                                                                                                                                                                                                                             |
|                      | 2. If Router Throughput appears within normal bounds, it is likely that <code>gorouter.backend_exhausted_conns</code> is spiking due to an unresponsive application, possibly due to application code issues or underlying application dependency issues. To help determine the problematic application, look in access logs for repeated calls to one application. Then proceed to troubleshoot this application accordingly. |
|                      | 3. If Router Throughput also shows unusual spikes, the cause of the increase in <code>gorouter.backend_exhausted_conns</code> spikes is likely external to the platform. Unusual increases in load may be due to expected business events driving additional traffic to applications. Unexpected increases in load may indicate a DDoS attack risk.                                                                            |

## Router Throughput

| gorouter.total_requests      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>The lifetime number of requests completed by the Gorouter VM, emitted per Gorouter instance</p> <p><b>Use:</b> The aggregation of these values across all Gorouters provide insight into the overall traffic flow of a deployment. Unusually high spikes, if not known to be associated with an expected increase in demand, could indicate a DDoS risk. For performance and capacity management, consider this metric a measure of router throughput per job, converting it to requests-per-second, by looking at the delta value of <code>gorouter.total_requests</code> and deriving back to 1s, or <code>gorouter.total_requests.delta)/5</code>, per Gorouter instance. This helps you see trends in the throughput rate that indicate a need to scale the Gorouter instances. Use the trends you observe to tune the threshold alerts for this metric.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Counter (Integer)<br/> <b>Frequency:</b> 5 s</p> |
| Recommended measurement      | Average over the last 5 minutes of the derived per second calculation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Recommended alert thresholds | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Recommended response         | <p>For optimizing the Gorouter, consider the requests-per-second derived metric in the context of router latency and Gorouter VM CPU utilization. From performance and load testing of the Gorouter, Pivotal has observed that at approximately 2500 requests per second, latency can begin to increase.</p> <p>To increase throughput and maintain low latency, scale the Gorouters either horizontally or vertically and watch that the <code>system.cpu.user</code> metric for the Gorouter stays in the suggested range of 60-70% CPU Utilization.</p>                                                                                                                                                                                                                                                                                                                                                                                                        |

## Router Handling Latency

| gorouter.latency |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description      | <p>The time in milliseconds that the Gorouter takes to handle requests to backend endpoints, which include both applications routable platform system APIs like Cloud Controller and UAA. This is the average round trip response time, which includes router handling.</p> <p><b>Use:</b> Indicates how Gorouter jobs in PAS are impacting overall responsiveness. Latencies above 100 ms can indicate problems with the network, misbehaving backends, or the need to scale the Gorouter itself due to ongoing traffic congestion. An alert value on this metric should be tuned to the specifics of the deployment and its underlying network considerations; a suggested starting point is 100 ms.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float in ms)<br/> <b>Frequency:</b> Emitted per Gorouter request, emission should be constant on a running deployment</p> |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recommended measurement</b>      | Average over the last 30 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Recommended alert thresholds</b> | Yellow warning: Dynamic<br>Red critical: Dynamic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Recommended response</b>         | <p>Extended periods of high latency can point to several factors. The Gorouter latency measure includes network and backend latency impacts as well.</p> <ol style="list-style-type: none"> <li>1. First inspect logs for network issues and indications of misbehaving backends.</li> <li>2. If it appears that the Gorouter needs to scale due to ongoing traffic congestion, do not scale on the latency metric alone. You should also look at the CPU utilization of the Gorouter VMs and keep it within a maximum 60-70% range.</li> <li>3. Resolve high utilization by scaling the Gorouter.</li> </ol> |

## Time Since Last Route Register Received

| gorouter.ms_since_last_registry_update |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                     | <p>Time in milliseconds since the last route register was received, emitted per Gorouter instance</p> <p><b>Use:</b> Indicates if routes are not being registered to apps correctly.</p> <p><b>Origin:</b> Firehose<br/><b>Type:</b> Gauge (Float in ms)<br/><b>Frequency:</b> 30 s</p>                                                                                                                                                                                                   |
| <b>Recommended measurement</b>         | Maximum over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Recommended alert thresholds</b>    | <p>Yellow warning: N/A<br/>Red critical: &gt; 30,000</p> <p>This threshold is suitable for normal platform usage. It alerts if it has been at least 30 seconds since the Gorouter last received a message from an app.</p>                                                                                                                                                                                                                                                                |
| <b>Recommended response</b>            | <ol style="list-style-type: none"> <li>1. Search the Gorouter and Route Emitter logs for connection issues to NATS.</li> <li>2. Check the BOSH logs to see if the NATS, Gorouter, or Route Emitter VMs are failing.</li> <li>3. Look more broadly at the health of all VMs, particularly Diego-related VMs.</li> <li>4. If problems persist, pull the Gorouter and Route Emitter logs and contact Pivotal Support to say there are consistently long delays in route registry.</li> </ol> |

## Router Error: 502 Bad Gateway

| gorouter.bad_gateways               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                  | <p>The lifetime number of bad gateways, or 502 responses, from the Gorouter itself, emitted per Gorouter instance. The Gorouter emits a 502 bad gateway error when it has a route in the routing table and, in attempting to make a connection to the backend, finds that the backend does not exist.</p> <p><b>Use:</b> Indicates that route tables might be stale. Stale routing tables suggest an issue in the route register management plane, which indicates that something has likely changed with the locations of the containers. Always investigate unexpected increases in this metric.</p> <p><b>Origin:</b> Firehose<br/><b>Type:</b> Count (Integer, Lifetime)<br/><b>Frequency:</b> 5 s</p> |
| <b>Recommended measurement</b>      | Maximum delta per minute over a 5-minute window                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Recommended alert thresholds</b> | Yellow warning: Dynamic<br>Red critical: Dynamic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recommended response | <ol style="list-style-type: none"> <li>1. Check the Gorouter and Route Emitter logs to see if they are experiencing issues when connecting to NATS.</li> <li>2. Check the BOSH logs to see if the NATS, Gorouter, or Route Emitter VMs are failing.</li> <li>3. Look broadly at the health of all VMs, particularly Diego-related VMs.</li> <li>4. If problems persist, pull Gorouter and Route Emitter logs and contact Pivotal Support to say there has been an unusual increase in Gorouter bad gateway responses.</li> </ol> |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Router Error: Server Error

| gorouter.responses.5xx       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>The lifetime number of requests completed by the Gorouter VM for HTTP status family 5xx, server errors, emitted per Gorouter instance.</p> <p><b>Use:</b> A repeatedly crashing app is often the cause of a big increase in 5xx responses. However, response issues from apps can also cause an increase in 5xx responses. Always investigate an unexpected increase in this metric.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Counter (Integer)<br/> <b>Frequency:</b> 5 s</p> |
| Recommended measurement      | Maximum delta per minute over a 5-minute window                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Recommended alert thresholds | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Look for out-of-memory errors and other app-level errors.</li> <li>2. As a temporary measure, ensure that the troublesome app is scaled to more than one instance.</li> </ol>                                                                                                                                                                                                                                                                   |

## Number of Gorouter Routes Registered

| gorouter.total_routes        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>The current total number of routes registered with the Gorouter, emitted per Gorouter instance</p> <p><b>Use:</b> The aggregation of these values across all Gorouters indicates uptake and gives a picture of the overall growth of the environment for capacity planning.</p> <p>Pivotal also recommends alerting on this metric if the number of routes falls outside of the normal range for your deployment. Dramatic decreases in this metric volume may indicate a problem with the route registration process, such as an app outage, or that something in the route register management plane has failed.</p> <p>If visualizing these metrics on a dashboard, <code>gorouter.total_routes</code> can be helpful for visualizing dramatic drops. However, for alerting purposes, the <code>gorouter.ms_since_last_registry_update</code> metric is more valuable for quicker identification of Gorouter issues. Alerting thresholds for <code>gorouter.total_routes</code> should focus on dramatic increases or decreases out of expected range.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float)<br/> <b>Frequency:</b> 30 s</p> |
| Recommended measurement      | 5-minute average of the per second delta                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Recommended alert thresholds | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                              | <ol style="list-style-type: none"> <li>1. For capacity needs, scale up or down the Gorouter VMs as necessary.</li> <li>2. For significant drops in current total routes, see the <code>gorouter.ms_since_last_registry_update</code> metric value for additional context.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recommended response | <ol style="list-style-type: none"> <li>3. Check the Gorouter and Route Emitter logs to see if they are experiencing issues when connecting to NATS.</li> <li>4. Check the BOSH logs to see if the NATS, Gorouter, or Route Emitter VMs are failing.</li> <li>5. Look broadly at the health of all VMs, particularly Diego-related VMs.</li> <li>6. If problems persist, pull the Gorouter and Route Emitter logs and contact Pivotal Support.</li> </ol> |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Number of Route Registration Messages Sent and Received

| gorouter.registry_message.route-emitter<br>route_emitter.HTTPRouteNATSMessagesEmitted |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                                           | <p>This KPI is based on the following metrics:</p> <ul style="list-style-type: none"> <li><code>route_emitter.HTTPRouteNATSMessagesEmitted</code> reports the lifetime number of route registration messages sent by the Route Emitter component. The metric is emitted for each Route Emitter.</li> <li><code>gorouter.registry_message.route-emitter</code> reports the lifetime number of route registration messages received by the Gorouter. The metric is emitted for each Gorouter instance.</li> </ul> <p>Dynamic configuration that enables the Gorouter to route HTTP requests to apps is published by the Route Emitter component colocated on each Diego cell to the NATS clustered message bus. All router instances subscribed to this message bus receive the same configuration. (Router instances within an isolation segment receive configuration only for cells in the same isolation segment.)</p> <p>As Gorouters prune app instances from the route when a TTL expires, each Route Emitter periodically publishes the routing configuration for the app instances on the same cell.</p> <p>Therefore, the aggregate number of route registration messages published by all the Route Emitters should be equal to the number of messages received by each Gorouter instance.</p> <p><b>Use:</b> A difference in the rate of change of these metrics is an indication of an issue in the control plane responsible for updating the routers with changes to the routing table.</p> <p>Pivotal recommends alerting when the number of messages received per second for a given router instance falls below the sum of messages emitted per second across all Route Emitters.</p> <p>If visualizing these metrics on a dashboard, look for increases in the difference between the rate of messages received and sent. If the number of messages received by a Gorouter instance drops below the sum of messages sent by the Route Emitters, this is an indication of a problem in the control plane.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Counter<br/> <b>Frequency:</b> With each event</p> |
| Recommended measurement                                                               | Difference of 5-minute average of the per second deltas for <code>gorouter.registry_message.route-emitter</code> and sum of <code>route_emitter.HTTPRouteNATSMessagesEmitted</code> for all Route Emitters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Recommended alert thresholds                                                          | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Recommended response                                                                  | <ol style="list-style-type: none"> <li>1. Check the Gorouter and Route Emitter logs to see if they are experiencing issues when connecting to NATS.</li> <li>2. Check the BOSH logs to see if the NATS, Gorouter, or Route Emitter VMs are failing.</li> <li>3. Look broadly at the health of all VMs, particularly Diego-related VMs.</li> <li>4. If problems persist, pull the Gorouter and Route Emitter logs and contact Pivotal Support.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## UAA Metrics

## UAA Throughput

| uaa.requests.global.completed.count |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                         | <p>The lifetime number of requests completed by the UAA VM, emitted per UAA instance. This number includes health checks.</p> <p><b>Use:</b> For capacity planning purposes, the aggregation of these values across all UAA instances can provide insight into the overall load that UAA is processing. It is recommended to alert on unexpected spikes per UAA instance. Unusually high spikes, if they are not associated with an expected increase in demand, could indicate a DDoS risk and should be investigated.</p> <p>For performance and capacity management, look at the UAA Throughput metric as either a requests-completed-per-second or requests-completed-per-minute rate to determine the throughput per UAA instance. This helps you see trends in the throughput rate that may indicate a need to scale UAA instances. Use the trends you observe to tune the threshold alerts for this metric.</p> <p>From performance and load testing of UAA, Pivotal has observed that while UAA endpoints can have different throughput behavior, once throughput reaches its peak value per VM, it stays constant and latency increases.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Integer), emitted value increments over the lifetime of the VM like a counter<br/> <b>Frequency:</b> 5 s</p> |
| Recommended measurement             | Average over the last 5 minutes of the derived requests-per-second or requests-per-minute rate, per instance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Recommended alert thresholds        | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Recommended response                | <p>For optimizing UAA, consider this metric in the context of <a href="#">UAA Request Latency</a> and <a href="#">UAA VM CPU Utilization</a>. To increase throughput and maintain low latency, scale the UAA VMs horizontally by editing the number of your UAA VM instances in the <b>Resource Config</b> pane of the PAS tile and ensure that the <code>system.cpu.user</code> metric for UAA is not sustained in the suggested range of 80-90% maximum CPU utilization.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## UAA Request Latency

| gorouter.latency.uaa         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Time in milliseconds that UAA took to process a request that the Gorouter sent to UAA endpoints.</p> <p><b>Use:</b> Indicates how responsive UAA has been to requests sent from the Gorouter. Some operations may take longer to process, such as creating bulk users and groups. It is important to correlate latency observed with the endpoint and evaluate this data in the context of overall historical latency from that endpoint. Unusual spikes in latency could indicate the need to scale UAA VMs.</p> <p>This metric is emitted only for the routers serving the UAA system component and is not emitted per isolation segment even if you are using isolated routers.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float in ms)<br/> <b>Frequency:</b> Emitted per Gorouter request to UAA</p> |
| Recommended measurement      | Maximum, per job, over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended alert thresholds | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended response         | <p>Latency depends on the endpoint and operation being used. It is important to correlate the latency with the endpoint and evaluate this data in the context of the historical latency from that endpoint.</p> <ol style="list-style-type: none"> <li>1. Inspect which endpoints requests are hitting. Use historical data to determine if the latency is unusual for that endpoint. A list of UAA endpoints is available in the <a href="#">UAA API documentation</a>.</li> <li>2. If it appears that UAA needs to be scaled due to ongoing traffic congestion, do not scale based on the latency metric alone. You should also ensure that the <code>system.cpu.user</code> metric for UAA stays in the suggested range of 80-90% maximum CPU utilization.</li> </ol>                                                  |

3. Resolve high utilization by scaling UAA VMs horizontally. To scale UAA, navigate to the **Resource Config** pane of the PAS tile and edit the number of your **UAA** VM instances.

## UAA Requests In Flight

| uaa.server.inflight.count    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>The number of requests UAA is currently processing (in-flight requests), emitted per UAA instance.</p> <p><b>Use:</b> Indicates how many concurrent requests are currently in flight for the UAA instance. Unusually high spikes, if they are not associated with an expected increase in demand, could indicate a DDoS risk.</p> <p>From performance and load testing of the UAA component, Pivotal has observed that the number of concurrent requests impacts throughput and latency. The UAA Requests In Flight metric helps you see trends in the request rate that may indicate the need to scale UAA instances. Use the trends you observe to tune the threshold alerts for this metric.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Integer)<br/> <b>Frequency:</b> 5 s</p> |
| Recommended measurement      | Maximum, per job, over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recommended alert thresholds | <p><b>Yellow warning:</b> Dynamic</p> <p><b>Red critical:</b> Dynamic</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Recommended response         | <p>To increase throughput and maintain low latency when the number of in-flight requests is high, scale UAA VMs horizontally by editing the <b>UAA</b> VM field in the <b>Resource Config</b> pane of the PAS tile. Ensure that the <code>system.cpu.user</code> metric for UAA is not sustained in the suggested range of 80-90% maximum CPU utilization.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## System (BOSH) Metrics

### VM Health

| system.healthy               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p><code>1</code> means the system is healthy, and <code>0</code> means the system is not healthy.</p> <p><b>Use:</b> This is the most important BOSH metric to monitor. It indicates if the VM emitting the metric is healthy. Review this metric for all VMs to estimate the overall health of the system.</p> <p>Multiple unhealthy VMs signals problems with the underlying IAAS layer.</p> <p><b>Origin:</b> Firehose<br/> <b>Type:</b> Gauge (Float, 0-1)<br/> <b>Frequency:</b> 60 s</p> |
| Recommended measurement      | Average over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Recommended alert thresholds | <p><b>Yellow warning:</b> N/A</p> <p><b>Red critical:</b> &lt; 1</p>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Recommended response         | Investigate CF logs for the unhealthy component(s).                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### VM Memory Used

| system.mem.percent |                                                     |
|--------------------|-----------------------------------------------------|
|                    | System Memory — Percentage of memory used on the VM |

|                              |                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Use: Set an alert and investigate if the free RAM is low over an extended period.</p> <p>Origin: Firehose<br/>Type: Gauge (%)<br/>Frequency: 60 s</p> |
| Recommended measurement      | Average over the last 10 minutes                                                                                                                         |
| Recommended alert thresholds | <p>Yellow warning: <math>\geq 80\%</math></p> <p>Red critical: <math>\geq 90\%</math></p>                                                                |
| Recommended response         | The response depends on the job the metric is associated with. If appropriate, scale affected jobs out and monitor for improvement.                      |

## VM Disk Used

| system.disk.system.percent   |                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>System disk — Percentage of the system disk used on the VM</p> <p>Use: Set an alert to indicate when the system disk is almost full.</p> <p>Origin: Firehose<br/>Type: Gauge (%)<br/>Frequency: 60 s</p> |
| Recommended measurement      | Average over the last 30 minutes                                                                                                                                                                            |
| Recommended alert thresholds | <p>Yellow warning: <math>\geq 80\%</math></p> <p>Red critical: <math>\geq 90\%</math></p>                                                                                                                   |
| Recommended response         | <p>Investigate what is filling the jobs system partition.</p> <p>This partition should not typically fill because BOSH deploys jobs to use ephemeral and persistent disks.</p>                              |

## VM Ephemeral Disk Used

| system.disk.ephemeral.percent |                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                   | <p>Ephemeral disk — Percentage of the ephemeral disk used on the VM</p> <p>Use: Set an alert and investigate if the ephemeral disk usage is too high for a job over an extended period.</p> <p>Origin: Firehose<br/>Type: Gauge (%)<br/>Frequency: 60 s</p> |
| Recommended measurement       | Average over the last 30 minutes                                                                                                                                                                                                                            |
| Recommended alert thresholds  | <p>Yellow warning: <math>\geq 80\%</math></p> <p>Red critical: <math>\geq 90\%</math></p>                                                                                                                                                                   |
| Recommended response          | <ol style="list-style-type: none"> <li>Run <code>bosh vms --details</code> to view jobs on affected deployments.</li> <li>Determine cause of the data consumption, and, if appropriate, increase disk space or scale out the affected jobs.</li> </ol>      |

## VM Persistent Disk Used

| system.disk.persistent.percent |                                                                |
|--------------------------------|----------------------------------------------------------------|
|                                | Persistent disk — Percentage of persistent disk used on the VM |

|                              |                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>Use: Set an alert and investigate further if the persistent disk usage for a job is too high over an extended period.</p> <p>Origin: Firehose<br/>Type: Gauge (%)<br/>Frequency: 60 s</p>                                                             |
| Recommended measurement      | Average over the last 30 minutes                                                                                                                                                                                                                         |
| Recommended alert thresholds | <p>Yellow warning: <math>\geq 80\%</math><br/>Red critical: <math>\geq 90\%</math></p>                                                                                                                                                                   |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Run <code>bosh vms --details</code> to view jobs on affected deployments.</li> <li>2. Determine cause of the data consumption, and, if appropriate, increase disk space or scale out affected jobs.</li> </ol> |

## VM CPU Utilization

| system.cpu.user              |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | <p>CPU utilization — The percentage of CPU spent in user processes</p> <p>Use: Set an alert and investigate further if the CPU utilization is too high for a job.</p> <p>For monitoring Gorouter performance, CPU utilization of the Gorouter VM is the recommended key capacity scaling indicator. For more information, see <a href="#">Gorouter Latency and Throughput</a>.</p> <p>Origin: Firehose<br/>Type: Gauge (%)<br/>Frequency: 60 s</p> |
| Recommended measurement      | Average over the last 5 minutes                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Recommended alert thresholds | <p>Yellow warning: <math>\geq 85\%</math><br/>Red critical: <math>\geq 95\%</math></p>                                                                                                                                                                                                                                                                                                                                                             |
| Recommended response         | <ol style="list-style-type: none"> <li>1. Investigate the cause of the spike.</li> <li>2. If the cause is a normal workload increase, then scale up the affected jobs.</li> </ol>                                                                                                                                                                                                                                                                  |

## Key Capacity Scaling Indicators

This topic describes key capacity scaling indicators that operators monitor to determine when they need to scale their Pivotal Application Service (PAS) deployments.


Pivotal provides these indicators to operators as general guidance for capacity scaling. Each indicator is based on platform metrics from different components. This guidance is applicable to most PAS v2.2 deployments. Pivotal recommends that operators fine-tune the suggested alert thresholds by observing historical trends for their deployments.

## Diego Cell Capacity Scaling Indicators

There are three key capacity scaling indicators recommended for Diego cell:

- [Diego Cell Memory Capacity](#) is a measure of the percentage of remaining memory capacity
- [Diego Cell Disk Capacity](#) is a measure of the percentage of remaining disk capacity
- [Diego Cell Container Capacity](#) is a measure of the percentage of remaining container capacity

### Diego Cell Memory Capacity

| rep.CapacityRemainingMemory / rep.CapacityTotalMemory |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                                    | <p>Percentage of remaining memory capacity for a given cell. Monitor this derived metric across all cells in a deployment.</p> <p>The metric <code>rep.CapacityRemainingMemory</code> indicates the remaining amount in MiB of memory available for this cell to allocate to containers.</p> <p>The metric <code>rep.CapacityTotalMemory</code> indicates the total amount in MiB of memory available for this cell to allocate to containers.</p> |
| <b>Purpose</b>                                        | <p>A best practice deployment of Cloud Foundry includes three availability zones (AZs). For these types of deployments, Pivotal recommends that you have enough capacity to suffer failure of an entire AZ.</p> <p>The <i>Recommended threshold</i> assumes a three-AZ configuration. Adjust the threshold percentage if you have more or fewer AZs.</p>                                                                                           |
| <b>Recommended thresholds</b>                         | < avg(35%)                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>How to scale</b>                                   | Scale up your Diego Cells                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Additional details</b>                             | <p><b>Origin:</b> Firehose</p> <p><b>Type:</b> Gauge (%)</p> <p><b>Frequency:</b> Emitted every 60 s</p> <p><b>Applies to:</b> cf:diego_cells</p>                                                                                                                                                                                                                                                                                                  |
| <b>Alternative Metric</b>                             | PCF Healthwatch expresses this indicator with the metric <a href="#">healthwatch.Diego.TotalPercentageAvailableMemoryCapacity.5M</a>  .                                                                                                                                                                                                                       |

### Diego Cell Disk Capacity

| rep.CapacityRemainingDisk / rep.CapacityTotalDisk |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                                | <p>Percentage of remaining disk capacity for a given cell. Monitor this derived metric across all cells in a deployment.</p> <p>The metric <code>rep.CapacityRemainingDisk</code> indicates the remaining amount in MiB of disk available for this cell to allocate to containers.</p> <p>The metric <code>rep.CapacityTotalDisk</code> indicates the total amount in MiB of disk available for this cell to allocate to containers.</p> |
|                                                   | A best practice deployment of Cloud Foundry includes three availability zones (AZs). For these types of deployments, Pivotal recommends that you have enough capacity to suffer failure of an entire AZ.                                                                                                                                                                                                                                 |

|                        |                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purpose                | The <i>Recommended threshold</i> assumes a three-AZ configuration. Adjust the threshold percentage if you have more or fewer AZs.                      |
| Recommended thresholds | < avg(35%)                                                                                                                                             |
| How to scale           | Scale up your Diego Cells                                                                                                                              |
| Additional details     | <b>Origin:</b> Firehose<br><b>Type:</b> Gauge (%)<br><b>Frequency:</b> Emitted every 60 s<br><b>Applies to:</b> cf:diego_cells                         |
| Alternative Metric     | PCF Healthwatch expresses this indicator with the metric <a href="#">healthwatch.Diego.TotalPercentageAvailableDiskCapacity.5M</a> <a href="#">↗</a> . |

## Diego Cell Container Capacity

| rep.CapacityRemainingContainers / rep.CapacityTotalContainers |                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                   | <p>Percentage of remaining container capacity for a given cell. Monitor this derived metric across all cells in a deployment.</p> <p>The metric <code>rep.CapacityRemainingContainers</code> indicates the remaining number of containers this cell can host.</p> <p>The metric by <code>rep.CapacityTotalContainer</code> indicates the total number of containers this cell can host.</p> |
| Purpose                                                       | <p>A best practice deployment of Cloud Foundry includes three availability zones (AZs). For these types of deployments, Pivotal recommends that you have enough capacity to suffer failure of an entire AZ.</p> <p>The <i>Recommended threshold</i> assumes a three-AZ configuration. Adjust the threshold percentage if you have more or fewer AZs.</p>                                    |
| Recommended thresholds                                        | < avg(35%)                                                                                                                                                                                                                                                                                                                                                                                  |
| How to scale                                                  | Scale up your Diego Cells                                                                                                                                                                                                                                                                                                                                                                   |
| Additional details                                            | <b>Origin:</b> Firehose<br><b>Type:</b> Gauge (%)<br><b>Frequency:</b> Emitted every 60 s<br><b>Applies to:</b> cf:diego_cells                                                                                                                                                                                                                                                              |
| Alternative Metric                                            | PCF Healthwatch expresses this indicator with the metric <a href="#">healthwatch.Diego.TotalPercentageAvailableContainerCapacity.5M</a> <a href="#">↗</a> .                                                                                                                                                                                                                                 |

## Firehose Performance Scaling Indicators

There are two key capacity scaling indicators recommended for Firehose performance.

### Log Transport Loss Rate

| loggregator.doppler.dropped / loggregator.doppler.ingress |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                               | This derived value represents the loss rate occurring as messages are transported from the <a href="#">Metron Agent</a> components (log ingress point) through the <a href="#">Doppler</a> components to the firehose endpoints. Metric <code>loggregator.doppler.ingress</code> represents the number of messages entering Dopplers for transport through the firehose, and <code>loggregator.doppler.dropped</code> represents the number of messages dropped without delivery. Messages include the combined stream of logs from all apps and the metrics data from Cloud Foundry components. |
| Purpose                                                   | <p>Excessive dropped messages can indicate the Dopplers and/or Traffic Controllers are not processing messages fast enough.</p> <p>The recommended scaling indicator is to look at the total dropped as a percentage of the total throughput and scale if the derived loss rate value grows greater than <code>0.01</code>.</p>                                                                                                                                                                                                                                                                  |
| Recommended                                               | <p>Scale indicator: <math>\geq 0.01</math></p> <p>If alerting:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



|                     |                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thresholds          | Yellow warning: $\geq 0.005$<br><b>Red critical:</b> $> 0.01$                                                                                                                                                                                                                                                                                                                           |
| How to scale        | Scale up the number of Traffic Controller and Doppler instances.<br><br><b>Note:</b> At approximately 40 Doppler instances and 20 Traffic Controller instances, horizontal scaling is no longer useful for improving Loggregator Firehose performance. To improve performance, add vertical scale to the existing Doppler and Traffic Controller instances by increasing CPU resources. |
| Additional details  | <b>Origin:</b> Firehose<br><b>Type:</b> Gauge (float)<br><b>Frequency:</b> Base metrics are emitted every 5 s<br><b>Applies to:</b> cf:doppler                                                                                                                                                                                                                                          |
| Alternative Metrics | PCF Healthwatch expresses this indicator with the metrics <code>healthwatch.Firehose.LossRate.1h</code> and <code>healthwatch.Firehose.LossRate.1m</code> .                                                                                                                                                                                                                             |

## Doppler Message Rate Capacity

| loggregator.doppler.ingress (sum across instances) / current number of Doppler instances |                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                                              | This derived value represents the average rate of envelopes (messages) per Doppler instance. Deriving this into a per-Doppler envelopes-per-second, or envelopes-per-minute, rate can indicate the need to scale when Doppler instances are at their recommended maximum load. |
| Purpose                                                                                  | The recommended scaling indicator is to look at the average load on the Doppler instances, and increase the number of Doppler instances when the derived rate is 16,000 envelopes per second, or 1 million envelopes per minute.                                               |
| Recommended thresholds                                                                   | <b>Scale indicator:</b> $\geq 16,000$ envelopes per second (or 1 million envelopes per minute)                                                                                                                                                                                 |
| How to scale                                                                             | Increase the number of Doppler VMs in the <b>Resource Config</b> pane of the PAS tile.                                                                                                                                                                                         |
| Additional details                                                                       | <b>Origin:</b> Firehose<br><b>Type:</b> Gauge (float)<br><b>Frequency:</b> Emitted every 15 s<br><b>Applies to:</b> cf:doppler                                                                                                                                                 |
| Alternative Metric                                                                       | PCF Healthwatch expresses this indicator with the metric <code>healthwatch.Doppler.MessagesAverage.1m</code> .                                                                                                                                                                 |

## CF Syslog Drain Performance Scaling Indicators

There are three key capacity scaling indicators recommended for CF Syslog Drain performance.

**Note:** These CF Syslog Drain scaling indicators are only relevant if your deployment contains apps using the CF syslog drain binding feature.

### Adapter Loss Rate

| cf-syslog-drain.adapter.dropped / cf-syslog-drain.adapter.ingress |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                       | The loss rate of the Syslog Adapters, that is, the total messages dropped as a percentage of the total traffic coming through the <a href="#">Syslog Adapters</a> . Total messages include only logs for bound applications.<br><br>This loss rate is specific to the Syslog Adapters and does not impact the Firehose loss rate. For example, you can suffer lossiness in syslog while not suffering any lossiness in the Firehose. |
| Purpose                                                           | Indicates that the syslog drains are not keeping up with the number of logs that a syslog-drain-bound app is producing. This likely means that the syslog-drain consumer is failing to keep up with the incoming log volume.<br><br>The recommended scaling indicator is to look at the maximum per minute loss rate over a 5-minute window and scale if the derived loss rate value grows greater than <code>0.1</code> .           |
| Recommended thresholds                                            | <b>Scale indicator:</b> $\geq 0.1$<br>If alerting:<br>Yellow warning: $\geq 0.01$                                                                                                                                                                                                                                                                                                                                                    |

|                           |                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | <b>Red critical:</b> $\geq 0.1$                                                                                                                                                 |
| <b>How to scale</b>       | Performance test your syslog server, review the logs of the syslog consuming system for intake and other performance issues that indicate a need to scale the consuming system. |
| <b>Additional details</b> | <b>Origin:</b> Firehose<br><b>Type:</b> Counter (Integer)<br><b>Frequency:</b> Emitted every 60 s<br><b>Applies to:</b> cf:cf-syslog                                            |
| <b>Alternative Metric</b> | PCF Healthwatch expresses this indicator with the metric <a href="#">healthwatch.SyslogDrain.Adapter.LossRate.1M</a> <a href="#">↗</a> .                                        |

## Reverse Log Proxy Loss Rate

| loggregator.rlp.dropped / loggregator.rlp.ingress |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                                | <p>The loss rate of the reverse log proxies (RLP), that is, the total messages dropped as a percentage of the total traffic coming through the <a href="#">reverse log proxy</a>. Total messages include only logs for bound applications.</p> <p>This loss rate is specific to the RLP and does not impact the Firehose loss rate. For example, you can suffer lossiness in syslog while not suffering any lossiness in the Firehose.</p> |
| <b>Purpose</b>                                    | <p>Excessive dropped messages can indicate that the RLP is overloaded and that the Traffic Controllers need to be scaled.</p> <p>The recommended scaling indicator is to look at the maximum per minute loss rate over a 5-minute window and scale if the derived loss rate value grows greater than <code>0.1</code>.</p>                                                                                                                 |
| <b>Recommended thresholds</b>                     | <b>Scale indicator:</b> $\geq 0.1$<br>If alerting:<br><b>Yellow warning:</b> $\geq 0.01$<br><b>Red critical:</b> $\geq 0.1$                                                                                                                                                                                                                                                                                                                |
| <b>How to scale</b>                               | Scale up the number of traffic controller instances to further balance log load.                                                                                                                                                                                                                                                                                                                                                           |
| <b>Additional details</b>                         | <b>Origin:</b> Firehose<br><b>Type:</b> Counter (Integer)<br><b>Frequency:</b> Emitted every 60 s<br><b>Applies to:</b> cf:cf-syslog                                                                                                                                                                                                                                                                                                       |
| <b>Alternative Metric</b>                         | PCF Healthwatch expresses this indicator with the metric <a href="#">healthwatch.SyslogDrain.RLP.LossRate.1M</a> <a href="#">↗</a> .                                                                                                                                                                                                                                                                                                       |

## CF Syslog Drain Bindings Count

| cf-syslog-drain.scheduler.drains |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>               | The number of CF syslog drain bindings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Purpose</b>                   | <p>Each Syslog Adapter can handle approximately 250 drain bindings. The recommended initial configuration is a minimum of two Syslog Adapters (to handle approximately 500 drain bindings). A new Adapter instance should be added for each 250 additional drain bindings.</p> <p>Therefore, the recommended initial scaling indicator is 450 (as a maximum value over a 1-hr window). This indicates the need to scale up to three Adapters from the initial two-Adapter configuration.</p> <p>Please note that while <code>cf-syslog-drain.scheduler.drains` is emitted by each scheduler instance, the metric emitted is the aggregated total number of active drains. Therefore this metric should not be summed across instances, as the total value is already emitted.</code></p> |
| <b>Recommended thresholds</b>    | <b>Scale indicator:</b> $\geq 450$<br>Consider this threshold to be dynamic. Adjust the threshold to the PAS deployment as adoption of CF Syslog Drain increases or decreases.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>How to scale</b>              | Increase the number of Syslog Adapter VMs in the <b>Resource Config</b> pane of the PAS tile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Additional details</b>        | <b>Origin:</b> Firehose<br><b>Type:</b> Gauge (float)<br><b>Frequency:</b> Emitted every 60 s<br><b>Applies to:</b> cf:cf-syslog                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Alternative Metric</b>        | PCF Healthwatch expresses this indicator with the metric <a href="#">healthwatch.SyslogDrain.Adapter.BindingsAverage.5M</a> <a href="#">↗</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Router Performance Scaling Indicator

There is one key capacity scaling indicator recommended for Router performance.

### Router VM CPU Utilization

| system.cpu.user of the Gorouter VM(s) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>                    | CPU utilization of the Gorouter VM(s)                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Purpose</b>                        | <p>High CPU utilization of the Gorouter VMs can increase latency and cause throughput, or requests per/second, to level-off. Pivotal recommends keeping the CPU utilization within a maximum range of 60-70% for best Gorouter performance.</p> <p>If you want to increase throughput capabilities while also keeping latency low, Pivotal recommends scaling the Gorouter while continuing to ensure that CPU utilization does not exceed the maximum recommended range.</p> |
| <b>Recommended thresholds</b>         | <p><b>Scale indicator:</b> <math>\geq 60\%</math></p> <p>If alerting:</p> <p><b>Yellow warning:</b> <math>\geq 60\%</math></p> <p><b>Red critical:</b> <math>\geq 70\%</math></p>                                                                                                                                                                                                                                                                                             |
| <b>How to scale</b>                   | Resolve high utilization by scaling the Gorouters horizontally or vertically by editing the <b>Router</b> VM in the <b>Resource Config</b> pane of the PAS tile.                                                                                                                                                                                                                                                                                                              |
| <b>Additional details</b>             | <p><b>Origin:</b> Firehose</p> <p><b>Type:</b> Gauge (float)</p> <p><b>Frequency:</b> Emitted every 60 s</p> <p><b>Applies to:</b> cf:router</p>                                                                                                                                                                                                                                                                                                                              |

## UAA Performance Scaling Indicator


There is one key capacity scaling indicator recommended for UAA performance.

### UAA VM CPU Utilization

| system.cpu.user of the UAA VM(s) |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>               | CPU utilization of the UAA VM(s)                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Purpose</b>                   | <p>High CPU utilization of the UAA VMs can increase latency and cause throughput, or requests per/second, to level-off. Pivotal recommends keeping the CPU utilization within a maximum range of 80-90% for best UAA performance.</p> <p>If you want to increase throughput capabilities while keeping latency low, Pivotal recommends scaling the UAA VMs and ensuring that CPU utilization does not exceed the maximum recommended range.</p> |
| <b>Recommended thresholds</b>    | <p><b>Scale indicator:</b> <math>\geq 80\%</math></p> <p>If alerting:</p> <p><b>Yellow warning:</b> <math>\geq 80\%</math></p> <p><b>Red critical:</b> <math>\geq 90\%</math></p>                                                                                                                                                                                                                                                               |
| <b>How to scale</b>              | Resolve high utilization by scaling UAA horizontally or vertically. To scale UAA, navigate to the <b>Resource Config</b> pane of the PAS tile and edit the number of your <b>UAA</b> VM instances or change the VM type to a type that utilizes more CPU cores.                                                                                                                                                                                 |
| <b>Additional details</b>        | <p><b>Origin:</b> Firehose</p> <p><b>Type:</b> Gauge (float)</p> <p><b>Frequency:</b> Emitted every 60 s</p> <p><b>Applies to:</b> cf:uaa</p>                                                                                                                                                                                                                                                                                                   |

## NFS/WebDAV Backed Blobstore

There is one key capacity scaling indicator for external S3 external storage.

 **Note:** This metric is only relevant if your deployment does not use an external S3 repository for external storage with no capacity constraints.

| system.disk.persistent.percent of NFS server VM(s) |                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                        | <i>If applicable:</i> Monitor the percentage of persistent disk used on the VM for the NFS Server job.                                                                                                                                                                                                    |
| Purpose                                            | <p>If you do not use an external S3 repository for external storage with no capacity constraints, you must monitor the PAS object store to push new app and buildpacks.</p> <p>If you use an internal NFS/WebDAV backed blobstore, consider scaling the persistent disk when it reaches 75% capacity.</p> |
| Recommended thresholds                             | ≥ 75%                                                                                                                                                                                                                                                                                                     |
| How to scale                                       | Give your NFS Server additional persistent disk resources.                                                                                                                                                                                                                                                |
| Additional details                                 | <p><b>Origin:</b> Firehose</p> <p><b>Type:</b> Gauge (%)</p> <p><b>Applies to:</b> cf:nfs_server</p>                                                                                                                                                                                                      |

## Selecting and Configuring a Monitoring System

This topic describes considerations for selecting and configuring a system to continuously monitor Pivotal Cloud Foundry (PCF) component performance and health.

### Selecting a Monitoring Platform

Pivotal recommends using [PCF Healthwatch](#) to monitor your deployment. PCF Healthwatch is a service tile developed and supported by Pivotal and available on [Pivotal Network](#).

Many third-party systems can also be used to monitor a PCF deployment.

### Monitoring Platform Types

Monitoring platforms support two types of monitoring:

- A *dashboard* for active monitoring when you are at a keyboard and screen
- Automated *alerts* for when your attention is elsewhere

Some monitoring solutions offer both in one package. Others require putting the two pieces together.

### Monitoring Platforms

There are many monitoring options available, both open source and commercial products. Some commonly-used platforms among PCF customers include:

- [PCF Healthwatch](#) by Pivotal
- PCF Partner Services available on [Pivotal Network](#):
  - [AppDynamics](#)
  - [Datadog](#)
  - [Dynatrace](#)
  - [New Relic](#)
  - [SignalFx](#)
  - [WaveFront by VMware](#)
- Other Commercial Services
  - [VMware vRealize Operations \(vROPS\)](#)
- Open Source Tooling
  - [Prometheus + Grafana](#)
  - [OpenTSDB](#)

### Pivotal Cloud Ops Tools

The Pivotal Cloud Ops Team manages two types of deployments for internal Pivotal use: open-source Cloud Foundry, and Pivotal Cloud Foundry (PCF).

For **Cloud Foundry**, Pivotal Cloud Ops uses several monitoring tools. The [Datadog Config repository](#) provides an example of how the Pivotal Cloud Ops team uses a customized Datadog dashboard to monitor the health of its open-source Cloud Foundry deployments.

To monitor its **PCF** deployments, Pivotal Cloud Ops leverages a combination of [PCF Healthwatch](#) and [Google Stackdriver](#).

### Key Inputs for Platform Monitoring

## BOSH VM and PCF Component Health Metrics

Most monitoring service tiles for PCF come packaged with the Firehose nozzle necessary to extract the BOSH and CF metrics leveraged for platform monitoring. Nozzles are programs that consume data from the Loggregator Firehose. Nozzles can be configured to select, buffer, and transform data, and to forward it to other apps and services.

The nozzles gather the component logs and metrics streaming from the Loggregator Firehose endpoint. For more information about the Firehose, see [Loggregator Architecture](#).

As of PCF v2.0, both BOSH VM Health metrics and Cloud Foundry component metrics stream through the Firehose by default.

- PCF component metrics originate from the Metron agents on their source components, then travel through Dopplers to the Traffic Controller.
- The Traffic Controller aggregates both metrics and log messages system-wide from all Dopplers, and emits them from its Firehose endpoint.

The following topic list high-signal-value metrics and capacity scaling indicators in a PCF deployment:

- [Key Performance Indicators](#)
- [Key Capacity Scaling Indicators](#)

## Continuous Functional Smoke Tests

PCF includes [smoke tests](#), which are functional unit and integration tests on all major system components. By default, whenever an operator upgrades to a new version of PAS, these smoke tests run as a post-deploy errand.

Pivotal recommends additional higher-resolution monitoring by the execution of continuous smoke tests, or Service Level Indicator tests, that measure user-defined features and check them against expected levels.

- [PCF Healthwatch](#) automatically executes these tests for PAS Service Level Indicators.
- The Pivotal Cloud Ops [CF Smoke Tests](#) repository offers additional testing examples.

See the [Metrics](#) topic in the Concourse documentation for how to set up Concourse to generate custom component metrics.

## Warning and Critical Thresholds

To properly configure your monitoring dashboard and alerts, you must establish what thresholds should drive alerting and red/yellow/green dashboard behavior.

Some key metrics have more fixed thresholds, with similar threshold numbers recommended across different foundations and use cases. These metrics tend to revolve around the health and performance of key components that can impact the performance of the entire system.

Other metrics of operational value are more dynamic in nature. This means that you must establish a baseline and yellow/red thresholds suitable for your system and its use cases. You can establish initial baselines by watching values of key metrics over time and noting what seems to be a good starting threshold level that divides acceptable and unacceptable system performance and health.

## Continuous Evolution

Effective platform monitoring requires continuous evolution.

After you establish initial baselines, Pivotal recommends that you continue to refine your metrics and tests to maintain the appropriate balance between early detection and reducing unnecessary alert fatigue. The dynamic measures recommended in [Key Performance Indicators](#) and [Key Capacity Scaling Indicators](#) should be revisited on occasion to ensure they are still appropriate to the current system configuration and its usage patterns.

## Pivotal Application Service for Windows

### Overview

Pivotal Application Service (PAS) for Windows enables operators to provision, operate, and manage Windows cells on Pivotal Cloud Foundry (PCF).

After operators install the PAS for Windows tile on the Ops Manager Installation Dashboard, developers can push .NET applications to Windows cells using the [Cloud Foundry Command Line Interface](#) (cf CLI).

For more information about how PAS for Windows works, see the [Product Architecture](#) topic.

For information about deploying .NET apps to PAS for Windows, see the [Tips for .NET Developers](#) topic.

For the PAS for Windows release notes, see the [PAS for Windows v2.2 Release Notes](#) topic.

### Requirements

To install the PAS for Windows tile, you must have the following:

- Ops Manager v2.2 and PAS v2.2 deployed to vSphere, Amazon Web Services (AWS), Google Cloud Platform (GCP), or Azure.
- A windows stemcell, which you can obtain by following the directions in [Downloading or Creating Windows Stemcells](#).

The minimum resource requirements for each Windows cell are as follows:

- Disk size: 64 GB
- Memory: 16 GB
- CPUs: 4

### Contents

#### About PAS for Windows

- [Product Architecture](#)

#### Installation Guide

- [Downloading or Creating Windows Stemcells](#)
- [Creating a Windows Stemcell for vSphere Manually](#)
- [Creating a Windows Stemcell for vSphere Using stembuild \(Beta\)](#)
- [Installing and Configuring PASW](#)
- [Windows Cells in Isolation Segments](#)
- [Migrating Apps to PAS for Windows](#)

#### Admin Guide

- [Upgrading Windows Cells](#)
- [Troubleshooting Windows Cells](#)

#### Developer Guide

- [Developing and Deploying .NET Apps](#)

## Limitations

PAS for Windows has the following limitations:

- Developers cannot push Docker or other OCI-compatible images to Windows Diego cells.
- Container-to-container networking is not available for Windows-hosted applications.
- OpenStack is currently not supported for PAS for Windows. Contact your Pivotal representative for information about OpenStack deployments.
- SMB is supported, but Volume Services is not supported.
- Due to [Known Issue #244](#) in Windows Server OS, applications hosted on PAS for Windows cannot route traffic when deployed with the IPsec add-on for PCF.



## Deploying .NET Apps

This topic lists resources for .NET app developers.

For general information about app deployment, see [Deploy an Application](#).

### .NET Core on Linux

[.NET Core Buildpack](#) describes how to push .NET Core apps to Linux cells on Cloud Foundry using the .NET Core buildpack. For supported ASP.NET Core versions, see [.NET Core buildpack release notes](#) in GitHub.

### .NET Framework on Windows

[HWC Buildpack](#) describes how to push .NET Framework apps to Pivotal Application Service for Windows (PASW) using the HWC buildpack. It also describes what features of IIS (Internet Information Services) and HWC (Hostable Web Core) are supported, and how to configure your .NET Framework apps to run on PASW.

[Console Applications](#) in the *.NET Cookbook* provides information about pushing compiled .NET Framework Console apps to PASW using the binary buildpack.

### .NET Core on Windows

[Binary Buildpack](#) describes how to push compiled .NET Core apps to Windows cells on PASW using the binary buildpack.

## Other Resources

[Tips for .NET Framework Developers](#) describes common errors and challenges faced when pushing .NET Framework apps to PASW.

The [.NET Cookbook](#) provides code samples, guidelines, tips, and other recipes for making changes to both new and existing .NET Framework and .NET Core apps to run successfully on PASW.

## Product Architecture

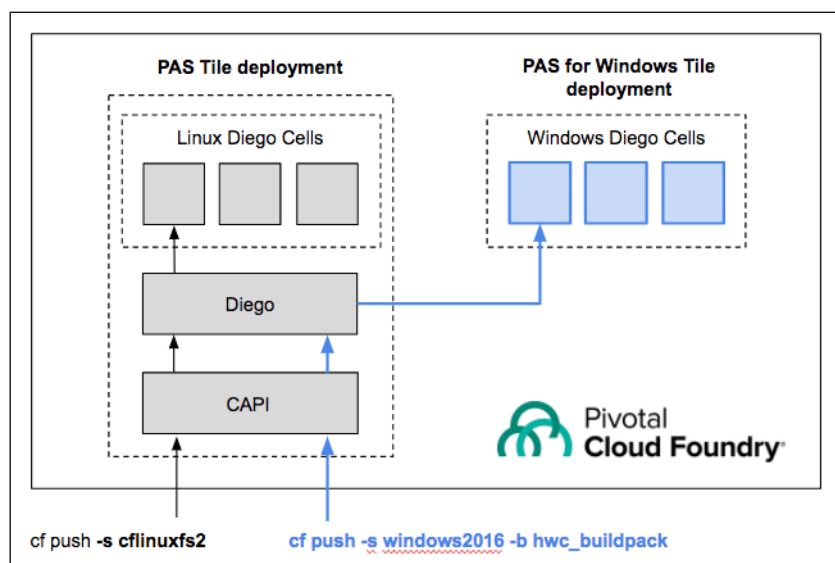
This topic describes the architecture of Windows cells that PAS for Windows deploys to run containerized .NET apps, and the stemcells that it supplies to BOSH as the operating system for the Windows cell VMs.

### Overview

Operators who want to run Windows cells in PCF to enable developers to push .NET apps can deploy the PAS for Windows tile.

Deploying this tile creates a separate BOSH deployment populated with the Garden Windows release, which runs on a Windows cell built from a Windows stemcell.

Once the Windows cell is running, developers can specify a Windows stack when pushing .NET apps from the command line. PCF passes the app to the Windows cell in the PAS for Windows BOSH deployment. The diagram below illustrates the process.



## About Windows Cells

App instances in PCF run inside containers. [Garden](#) is the API that creates and manages these containers. An implementation equivalent to that on Linux cells provides this infrastructure on Windows cells, utilizing native Windows Server Containers.

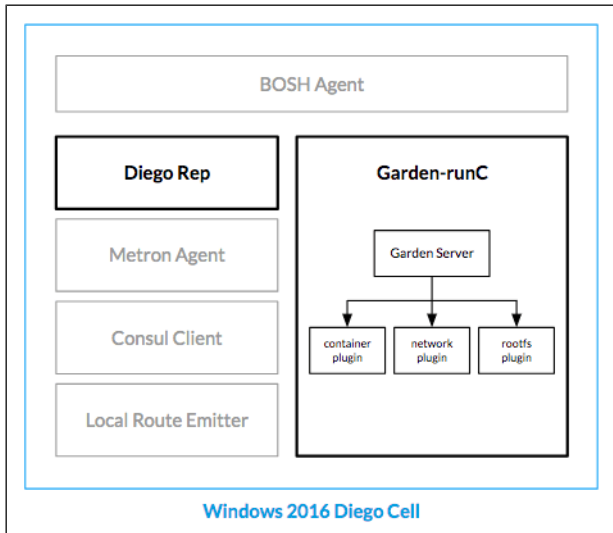
By installing the [PAS for Windows](#) tile, operators create a Windows [cell](#) from a [stemcell](#) that contains the Windows Server operating system. Garden on Windows uses [Windows Containers](#) to isolate resources on Windows cells that Cloud Foundry manages alongside Linux cells.

### Components

A Windows cell includes the following components:

- Guardian: Implements the [Garden](#) API on Windows
- [Metron Agent](#): Forwards app logs, errors, and metrics to the [Loggregator](#) system
- [BOSH Agent](#): Executes instructions from the BOSH Director
- [Consul Client](#): Registers the cell as a service in a Consul cluster
- [Diego Rep](#): Runs and manages [Tasks and Long Running Processes](#)

The following diagram illustrates the architecture of a Windows cell:



## Container Implementation

Garden on Windows uses the following runtime plugins to create and manage [Windows Containers](#) for PAS:

- Container plugin `winc`: Creates [OCI](#)-compliant containers, executes processes in the containers, and sets their CPU and RAM limits.
- Network plugin `winc-network`: Creates a network compartment for the container, applies its DNS settings, and defines its inbound/outbound network access rules.
- Rootfs image plugin `groot`: Sets up the container filesystem volume and uses the [FSRM](#) API to define its disk usage quotas.

## About Windows Stemcells

A “stemcell” is a customized operating system image containing the filesystem for BOSH-managed virtual machines. When deployed, the operating system includes the *BOSH Agent* process, which is dedicated to communicating with the orchestrating VM, the *BOSH Director*. The BOSH Agent executes and monitors BOSH jobs on its VM.

Deployments of Windows Server on PCF currently use a stemcell containing Windows Server 2016, version 1709.

See [Downloading or Creating Windows Stemcells](#) for documentation about how to obtain or create a stemcell for PAS for Windows.

## Downloading or Creating Windows Stemcells

This topic describes how to download or create the stemcell that Pivotal Application Service (PAS) for Windows needs to create VMs on an infrastructure.

### Windows Stemcells

BOSH needs a stemcell to supply the basic operating system for any new Windows Server 2016 VMs it creates. Depending on your IaaS, you can create or download a stemcell as follows:

- **Azure:** [Follow the instructions below](#) to activate and download the Azure Windows Stemcell.
- **Google Cloud Platform (GCP):** Download the **GCP light Stemcell for Windows 2016 Server Version 1709** from the **Stemcells for PCF (Windows Server)** section of [Pivotal Network](#).
- **vSphere:** Create a stemcell by following the directions in [Creating a Windows Stemcell for vSphere Manually](#) or [Creating a Windows Stemcell for vSphere Using stembuild \(Beta\)](#).
- **Amazon Web Services (AWS):** Download the **AWS light Stemcell for Windows 2016 Server Version 1709** from the **Stemcells for PCF (Windows Server)** section of [Pivotal Network](#).

### Configure the Azure Light Stemcell

On Azure, the stemcell exists as an offering in the Azure Marketplace. To start using the Azure light stemcell, perform the steps in the following sections:

- [Enable the Azure Light Stemcell](#)
- [Download the Azure Light Stemcell](#)

#### Enable the Azure Light Stemcell

To use the Azure light stemcell, you must first accept the corresponding Microsoft license agreement and enable the stemcell for your non-trial Azure Subscription through the Azure Marketplace as follows:

1. Navigate to <https://portal.azure.com> and log in.
2. From the options on the left side of the page, click **+ Create a resource**.
3. In the **Search the Marketplace** bar, search for **BOSH Stemcell for Windows Server 1709**.
4. Select **BOSH Stemcell for Windows Server 1709** from your search results. A description of the Azure stemcell offering appears.
5. Below the description, at the bottom of the page, click the blue banner that reads **Want to deploy programmatically? Get started →**.
6. Review the Terms of Use in the page “Configure Programmatic Deployment” that appears.
7. Under **Choose the subscriptions**, click **Enable** for each Azure subscription with which you want to use the stemcell.
8. Click **Save**.

#### Download the Azure Light Stemcell

To download the Azure light stemcell for use in Ops Manager, perform the following steps:


1. Navigate to [Pivotal Network](#).
2. Select **Azure Light Stemcell for Windows 2016 Server Version 1709** from the **Release Download Files** section of the Stemcells for PCF (Windows) page.

For information about how to deploy and configure the PAS for Windows tile, see [Installing and Configuring PAS for Windows](#).




## Creating a Windows Stemcell for vSphere Manually

This topic describes how to create the stemcell that Pivotal Application Service for Windows (PASW) needs to create VMs on vSphere.

 **Note:** The instructions in this topic are based on vSphere 6.0 using vSphere Web Client.

### Overview

To create a Windows stemcell for vSphere, you create a base Windows VM from a volume-licensed ISO and subsequently maintain that base template with all Windows recommended security updates, but without the BOSH dependencies.



 **Note:** The stemcell you create in this topic is based on Windows Server, version 1709.


The VM with security updates serves as the base for all future stemcells, produced from clones of that base VM. This enables you to build new stemcells without having to run Windows Updates from scratch each time. You can also use a “snapshot” feature to maintain an updated Windows image that does not contain the BOSH dependencies.

Pivotal recommends installing any available critical updates, and then rebuilding the stemcell from a clone of the original VM.

### Prerequisites

Before you create a vSphere Windows stemcell, you must have the following:



- A Windows Server, version 1709 ISO, from [Microsoft Developer Network \(MSDN\)](#)  or [Volume Licensing Service Center \(VLSC\)](#) . You can use an evaluation copy for testing, but Pivotal does not recommend an evaluation copy for production, as the licensing expires.

 **Note:** Pivotal recommends maintaining a separate, updated Windows VM based on this ISO to serve as the basis for the installation steps below. This enables you to apply Windows Updates and create new stemcells without having to reinstall all updates from scratch.

- A vSphere/vCenter account granted sufficient permissions to perform all of the following tasks:
  - Create a VM.
  - Configure a VM.
  - Open a VM in VM Remote Console on a local desktop.
  - Export a VM.
- The ability to download/transfer files and software to a vCenter Windows VM.




### Files on Local Machine

As part of completing the procedures in this topic, you download the following files to your local machine:

- The latest release of [stembuild](#) .
- [ovftool](#) .

### Files on Windows VM

As part of completing the procedures in this topic, you download the following files to your Windows VM:

- [lgpo.exe](#)  from the Microsoft Security Toolkit.
- [OpenSSH v7.7.2.0p1](#) .
- The [BOSH PS Modules and BOSH Agent](#)  for the 1709 stemcell version you want to build.

 **Note:** You must choose a stemcell version to build. Stemcells are versioned as MAJOR.MINOR, such as 1709.12. For more information about

1709 stemcells, see the [Stemcell v1709.x \(Windows Server, version 1709\) Release Notes](#).

## Step 1: Create Base VM for Stemcell

This section describes how to create, configure, and verify a base Windows VM from a volume-licensed ISO.

### Upload the Windows ISO

Perform the following steps to upload the Windows ISO:

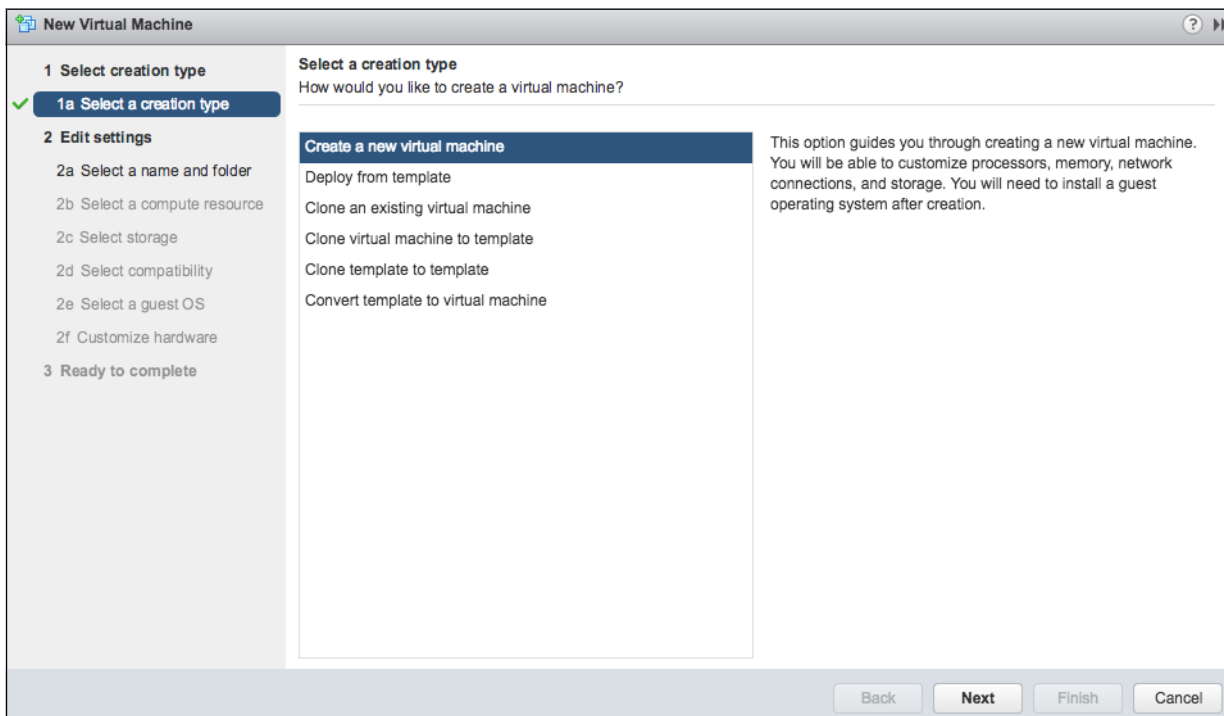
1. Log in to vCenter.
2. Click **Storage** in the vCenter menu.
3. Choose a datastore and click or create the directory where you want the Windows ISO.
4. Click **Upload a file to datastore**, and upload the Windows ISO.

**Note:** You might need to install the vSphere client web plugin to upload through your browser, or `scp` the file directly to the datastore server. For more information, see the VMware vSphere [documentation](#).

### Create and Customize a New VM

Perform the following steps to create and customize a new VM:

1. In the vSphere client, click the **VMs and Templates** view to display the inventory objects.
2. Right-click an object and select **New Virtual Machine** > **New Virtual Machine...**
3. On the **Select a creation type** page, select **Create a new virtual machine** and click **Next**.



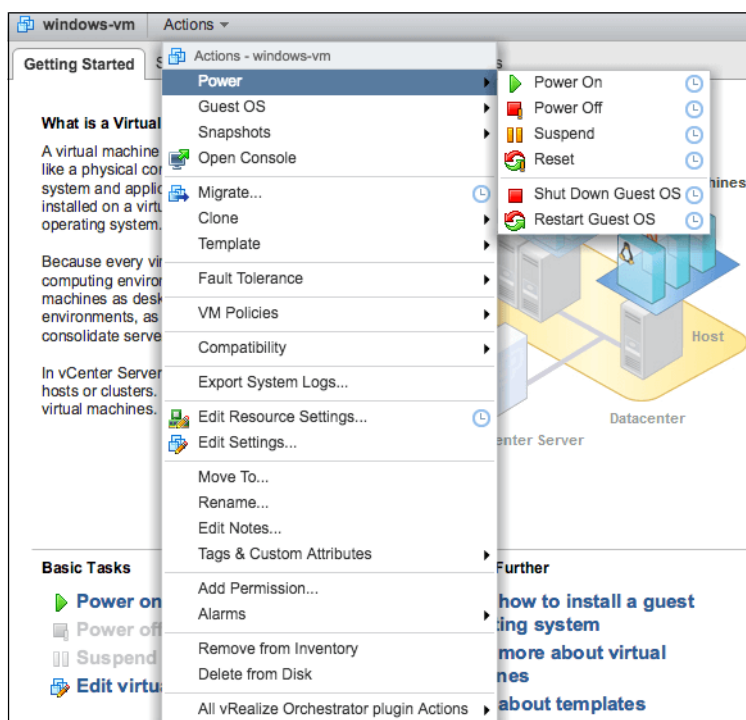
4. On the **Select a name and folder** page, perform the following steps:
  - a. Enter a name for the VM.
  - b. Select a location for the VM.
  - c. Click **Next**.

5. On the **Select a compute resource** page, select a compute resource to run the VM and click **Next**.
6. On the **Select storage** page, perform the following steps:
  - a. Select a **VM Storage Policy**.
  - b. Select the destination datastore for the VM configuration files and virtual disks.
  - c. Click **Next**.
7. On the **Select compatibility** page, for the **Compatible with** configuration setting, select **ESXi 6.0 and later** and click **Next**.
8. On the **Select a guest OS** page, perform the following steps:
  - a. For **Guest OS Family**, select **Windows**.
  - b. For **Guest OS Version**, select **Microsoft Windows Server 2016**.
  - c. Click **Next**.
9. On the **Customize hardware** page, configure the VM hardware and click **Next**. When configuring the VM hardware, select the following settings for **New Hard disk** and **New CD\DVD Drive**:
  - a. For **New Hard disk**, specify 30 GB or greater.
  - b. For **New CD\DVD Drive**, perform the following steps:
    - i. Select **Datastore ISO File**.
    - ii. Select the ISO file you uploaded to your datastore and click **OK**.
    - iii. Enable the **Connect At Power On** checkbox.
10. Review the configuration settings on the **Ready to complete** page and click **Finish**.

## Install Windows Server

Perform the following steps to install Windows Server on the base VM:


1. After creating the VM, click **Power On** in the **Actions** tab for your VM.



2. Select **Windows Server Standard**.
3. Select **Custom installation**.
4. Complete the installation process, and enter a password for the Administrator user. BOSH later randomizes this password.



## Verify OS

 **warning:** You must complete the following procedure to verify your OS version before continuing.

Ensure you are using the correct the OS version by running the following PowerShell command on the Windows VM:

```
Get-CimInstance Win32_OperatingSystem | Select-Object
Caption, Version, ServicePackMajorVersion, OSArchitecture, CSName, WindowsDirectory
```

The output includes `Version: 10.0.16299`.

## Install VMware Tools

Perform the following steps to install VMware Tools on the base VM:

1. Under the VM **Summary** tab, select **Install VMware Tools**.
2. Navigate to the `D:` drive and run `setup64.exe`.

 **Note:** The VMware Tools install window might appear behind the Command Prompt window.

3. Restart the VM as required to finish the install.

## Step 2: Install Windows Updates

This section describes how to install Windows updates on your base Windows VM.

### Install Windows Updates

Install Windows updates on the Windows VM using your preferred procedure.

One way to install Windows updates on the Windows VM is by using the **SConfig** utility. Perform the following steps:

1. On the Windows VM, run the **SConfig** utility.
2. Select option number 6, **Download and Install Updates**.
3. Select **A** for **(A)ll updates**.
4. For the **Select an option**, select **(A)ll updates**.

You might need to restart the Windows VM while installing updates.

### Enable Meltdown Mitigation

 **warning:** You must enable Meltdown mitigation. Not enabling Meltdown mitigation can lead to timeout issues while deploying the PASW tile.

Windows Server, version 1709 should receive the update containing the Meltdown mitigation automatically when you install Windows updates.

After installing Windows update, ensure that the following registry keys are set to enable Meltdown mitigation:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management"
/v FeatureSettingsOverride /t REG_DWORD /d 0 /f

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management"
/v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization"
/v MinVmVersionForCpuBasedMitigations /t REG_SZ /d "1.0" /f

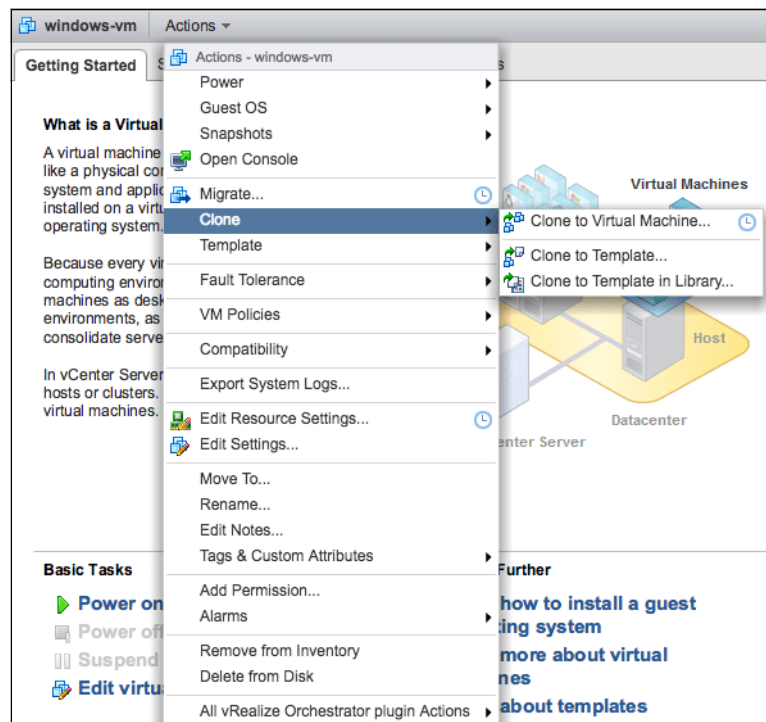
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat"
/f /v cadca5fe-87d3-4b96-b7fb-a231484277cc /t REG_DWORD /d 0
```

## Step 3: Clone the VM

Clone the VM that has the Windows updates installed. Save the original VM so that you can run updates on it in the future.

Perform the following steps:

1. In the vSphere client, right-click the current Windows VM.



2. Select **Clone** > **Clone to Virtual Machine...**

3. Ensure that you can create the VM that can be used to create a stemcell for the next Patch Tuesday Monthly Updates.

## Step 4: Install Required Software

You might need to specify an explicit execution policy for all of the PowerShell commands in the *Step 4: Install Required Software* section. You specify an execution policy with the `-ExecutionPolicy` flag.

For example:

```
powershell -ExecutionPolicy Bypass -Command "Install-CFFeatures"
```

## Transfer Files to a Windows VM

Some of the procedures described in the sections below require transferring files to a Windows VM. Many different methods exist to transfer files to a Windows VM, such as folder sharing or the PowerShell `Invoke-WebRequest` cmdlet. Use whatever method that you prefer.

As an example, the following PowerShell `Invoke-WebRequest` command uses TLS v1.2 to transfer **filename.zip** from `EXAMPLE-URL` to the current location on the Windows VM:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri "EXAMPLE-URL/filename.zip" -OutFile ".\filename.zip"
```

## Install the BOSH PS Modules

Perform the following steps to install the BOSH PS Modules:

1. Locate the [BOSH PS Modules](#) download for the 1709 stemcell version you want to build, such as 1709.12.
2. Transfer the `bosh-psmodules.zip` file to your Windows VM.
3. Start PowerShell in the Windows VM and run the following command:

```
Unblock-File PATH-TO-BOSH-PSMODULES.ZIP
```

Where `PATH-TO-BOSH-PSMODULES.ZIP` is the full path to the location of `bosh-psmodules.zip` on your Windows VM.

4. Unzip the archive with the following command:

```
Expand-Archive PATH-TO-BOSH-PSMODULES.ZIP C:\Program Files\WindowsPowerShell\Modules
```

## Install the Cloud Foundry Diego Cell Requirements

Perform the following steps to install the Cloud Foundry Diego cell requirements:

1. Start PowerShell in the Windows VM and run the following command:

```
Install-CFFeatures
```

The machine restarts automatically.

2. Apply the recommended ingress and service configuration with the following command:

```
Protect-CFCell
```

## Install the BOSH Agent

Perform the following steps to install the BOSH Agent:

1. Locate the [BOSH Agent](#) download for the 1709 stemcell version you want to build, such as 1709.12.
2. Transfer the `agent.zip` file to your Windows VM.
3. Start PowerShell in the Windows VM and run the following command:

```
Unblock-File PATH-TO-AGENT.ZIP
```

Where `PATH-TO-AGENT.ZIP` is the full path to the location of the `agent.zip` file on your Windows VM.

4. Install the BOSH Agent with the following command:

```
Install-Agent -IaaS vsphere -agentZipPath PATH-TO-AGENT.ZIP
```

## Install OpenSSH

You can use the `bosh ssh` command on BOSH-deployed Windows VMs if you install the OpenSSH dependency on the Windows VM and then enable it during deploy time. This lets an operator enter into a CMD or PowerShell session on the VM as a user with admin privileges.

Perform the following steps to install OpenSSH:

1. Transfer the [OpenSSH-Win64.zip](#) file to the Windows VM and place it in `C:\provision`.
2. Start PowerShell in the Windows VM and run the following command:


```
Unblock-File 'C:\provision\OpenSSH-Win64.zip'
```

3. Install OpenSSH with the following command:

```
Install-SSH -SSHZipFile 'C:\provision\OpenSSH-Win64.zip'
```

4. When configuring the PAS for Windows tile, you must select the **BETA: Enable BOSH-native SSH support on all VMs checkbox**. For more information, see [Installing and Configuring PAS for Windows](#).

## Optimize and Compress the Disk

 **Note:** Windows Server stemcells can be large, and can exceed the 10GB upload limit imposed by default by the BOSH Director.

Perform the following steps to reduce the stemcell size:

1. Restart the VM.
2. Start PowerShell in the Windows VM and run the following command to use `dism` to clear unnecessary files:

```
Optimize-Disk
```


3. Run the following command to defragment and zero out the disk:

```
Compress-Disk
```

## Step 5: Sysprep the System

This step “syspreps” the system, which ensures that each BOSH VM has a unique identity and applies the appropriate startup configuration at boot time.

The included policies help ensure the uptime and secure operations of the stemcell’s VMs, especially when deployed on PCF.

 **Note:** This step disables services that could cause restarts, such as Windows Automatic Updates. OS restarts are not supported on BOSH-deployed Windows VMs, and the BOSH Director resurrects the VM by destroying and repaving it.


Perform the following steps:

1. Transfer the [LGPO.ZIP](#) file to the Windows VM.
2. Start PowerShell in the Windows VM and run the following command:

```
Expand-Archive PATH-TO-LGPO.ZIP C:\Windows
```

3. Run the following command to sysprep the system:

```
Invoke-Sysprep -IaaS vsphere
[-NewPassword PASSWORD]
[-Owner OWNER] [-Organization ORGANIZATION]
```

 **Note:** All of the flags of `Invoke-Sysprep` except for `-IaaS` are optional.

Where:

- `PASSWORD` is an optional flag that enables you to set a password of your choice. Do not use any special character in the password other than `!`. For example, `Example12!` is permitted but `Example#12` is not. This is a known issue.
- `OWNER` and `ORGANIZATION` are optional flags. Set them if your organization requires it.

The `sysprep` command powers off the VM.

**⚠ warning:** Do not turn the VM back on before completing the procedure in [Step 6: Export the VMDK File](#).

## Step 6: Export the VMDK File

Perform the following steps to export the .VMDK file associated with the VM you powered off:

1. In vCenter, right-click the VM and select **Template > Export to OVF Template**.
2. Download the OVA to your local machine. You do not need to include files in the floppy or CD Drive.

**💡 Note:** You can also download the standalone vSphere client and select **File > Export > Export OVF Template**.

3. Rename the downloaded OVA file to have a `.tar` extension.
4. Expand the TAR archive and locate the VMDK file.

## Step 7: Convert the VMDK File to a BOSH Stemcell

**💡 Note:** This final step typically takes about ten to twenty minutes to complete.

Perform the following steps to convert the VMDK file to a BOSH stemcell:

1. Download the latest release of the [stembuild](#) utility to your local machine and place the executable in your command-line path.
2. Download [ovftool](#) to your local machine and place the executable in your command-line path.

**💡 Note:** On the Windows desktop, `ovftool` is installed by default in `C:\Program Files\VMware\VMware OVF Tool`.

`stembuild` invokes `ovftool` to convert the disk image to the appropriate stemcell format and apply the proper configuration.

3. Build the stemcell with the following command:

```
stembuild package -vmdk PATH-TO-VMDK -stemcell-version STEMCELL-VERSION -os 2016
```

Where:

- `PATH-TO-VMDK` is the path to the VMDK file.
- `STEMCELL-VERSION` is the 1709 stemcell version you want to build. For example, if you downloaded the [BOSH PS Modules and BOSH Agent](#) for the 1709.10 release, then specify `1709.10`.

`stembuild` creates the stemcell in the directory where you execute it. The file has a `.tgz` extension and a name similar to `bosh-stemcell-1709.10-vsphere-esxi-windows2016-go_agent.tgz`.

The stemcell is ready for use in conjunction with your BOSH deployment.

## Step 8: Apply Monthly Patch Tuesday Updates

On Patch Tuesday, run Windows Updates on the base image, and then repeat [Step 3: Clone the VM](#) through [Step 7: Convert the VMDK File to a BOSH Stemcell](#).

## Troubleshooting

### Garden Windows Logs Suggest Windows Features Not Installed

#### Symptom

You see the following error in your `garden-windows` job while deploying Windows 1709:

```
Missing required Windows Features:
Web-Webserver, Web-WebSockets, AS-Web-Support,
AS-NET-Framework, Web-WHC, Web-ASP.
Please use the most recent stemcell.
```

#### Explanation

`Install-CFFeatures` might not have run successfully.

#### Solution

Run the following commands in PowerShell on your Windows VM to verify whether `Install-CFFeatures` ran successfully:

```
Get-WindowsFeature "Containers" | Where InstallState -Eq "Installed"
Get-WindowsFeature "Windows-Defender-Features" | Where InstallState -Eq "Removed"
```

### Gorouter Returns a 502 Error When Accessing an App

#### Symptom

You cannot access a .NET app externally. When you attempt to access your app, Gorouter returns an HTTP 502 response status code. The app does not crash and is still running inside of its container.

#### Explanation

A race condition occurs when one app is deployed to a Diego cell and before it receives any traffic, a second app is deployed to the same Diego cell. As a result, the platform mistakenly removes your routing rules for the first app.

#### Solution

To resolve this issue, install Microsoft's [KB4074588](#) updates or later on your base Windows VM as described in [Step 2: Install Windows Updates](#).

Once you install the updates and create your Windows stemcell for vSphere following the instructions in [Step 3: Clone the VM](#) through [Step 7: Convert the VMDK File to a BOSH Stemcell](#), deploy the stemcell with PASW.

## Creating a Windows Stemcell for vSphere Using stembuild (Beta)

This topic describes how to create a BOSH stemcell for Pivotal Application Service (PAS) for Windows on VMware vSphere using `stembuild`.

### Overview

Before you can deploy PAS for Windows on vSphere, you must create a BOSH stemcell for Windows, a versioned operating system image. The BOSH stemcell that you create in this topic is based on Windows Server, version 1709.

To create a BOSH stemcell for Windows on vSphere, do the following:

1. [Create a Base VM for the BOSH Stemcell](#)
2. [Install Windows Updates](#)
3. [Clone the Base VM](#)
4. [Construct the BOSH Stemcell](#)
5. [Package the BOSH Stemcell](#)
6. [Upload the BOSH Stemcell to Ops Manager](#)

If you already have a BOSH stemcell for Windows on vSphere, see [Monthly Stemcell Upgrades](#).

### Prerequisites

- A vSphere environment
- A Windows Server, version 1709 ISO
- The `stembuild` command line interface (CLI) from a release in [Stemcells for PCF \(Windows\)](#) on Pivotal Network that corresponds to the operating system of your local host and the stemcell version that you want to build
- Microsoft [Local Group Policy Object Utility \(LGPO\)](#) downloaded to the same folder as your `stembuild` CLI
- The minimum vCenter user permissions required to use stembuild for vSphere stemcells, specifically:
  - `VirtualMachine.GuestOperations.Modify`
  - `VirtualMachine.GuestOperations.Execute`
  - `VirtualMachine.GuestOperations.Query`
  - `VirtualMachine.Config.AddRemoveDevice`
  - `VirtualMachine.Interact.SetCDMedia`
  - `VApp.Export`
  - `System.Anonymous` \*
  - `System.Read` \*
  - `System.View` \*

Permissions marked with an \* are generated upon creating a new user in vCenter and cannot be set within the vCenter UI.


## Step 1: Create a Base VM for the BOSH Stemcell

This section describes how to create, configure, and verify a base VM for Windows from a volume-licensed ISO.

### Upload the Windows Server, Version 1709 ISO

To upload the Windows Server, version 1709 ISO to vSphere, do the following:

1. Log in to the vSphere Web Client.

 **Note:** The instructions in this topic are based on vSphere 6.0.

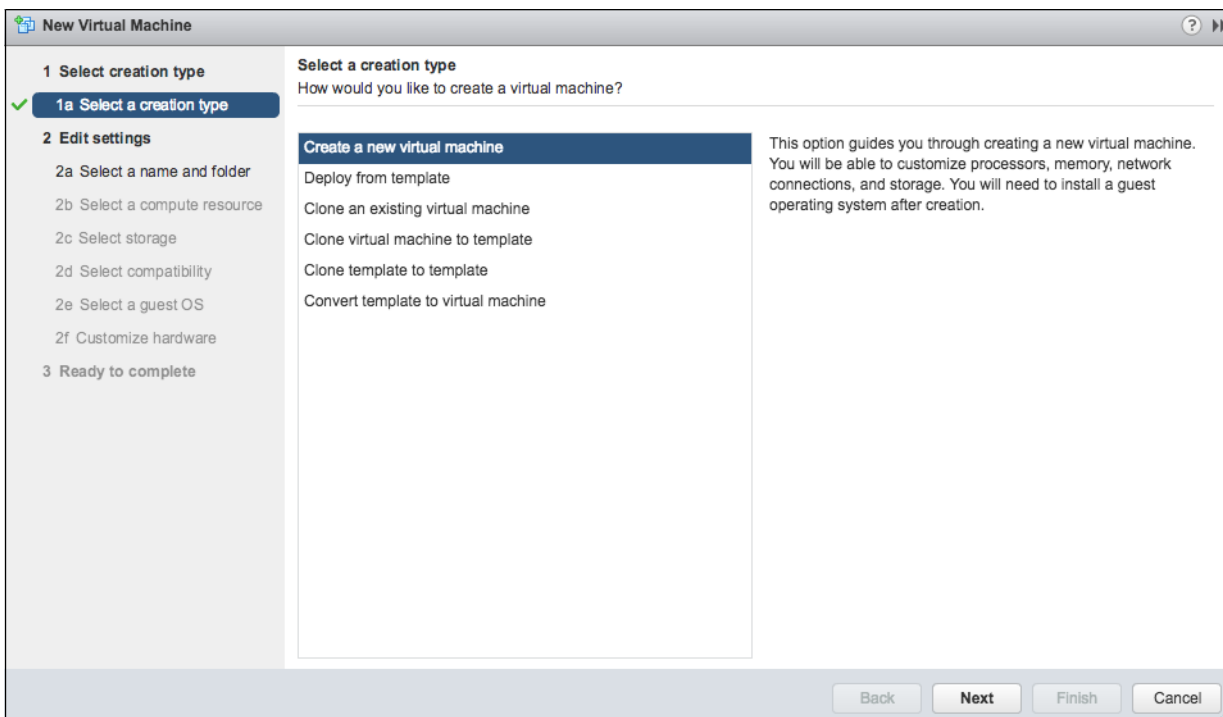
2. Click **Storage** and select a datastore.
3. Select or create a folder where you want to upload the Windows Server, version 1709 ISO.
4. Click **Upload a File** and select the Windows Server, version 1709 ISO.

You can use the `scp` utility instead of the vSphere Web Client to copy the file directly to the datastore server.

## Create and Customize a Base VM

To create and customize a base VM, do the following:

1. In the vSphere Web Client, click the **VMs and Templates** view to display the inventory objects.
2. Right-click an object and select **New Virtual Machine** > **New Virtual Machine**.
3. On the **Select a creation type** page, select **Create a new virtual machine** and click **Next**.



4. On the **Select a name and folder** page, do the following:
  - a. Enter a name for the VM.
  - b. Select a location for the VM.
  - c. Click **Next**.
5. On the **Select a compute resource** page, select a compute resource to run the VM and click **Next**.
6. On the **Select storage** page, do the following:
  - a. Select a **VM Storage Policy**.
  - b. Select the destination datastore for the VM configuration files and virtual disks.
  - c. Click **Next**.
7. On the **Select compatibility** page, for the **Compatible with** configuration setting, select **ESXi 6.0 and later** and click **Next**.
8. On the **Select a guest OS** page, do the following step:
  - a. For **Guest OS Family**, select **Windows**.
  - b. For **Guest OS Version**, select **Microsoft Windows Server 2016**.
  - c. Click **Next**.

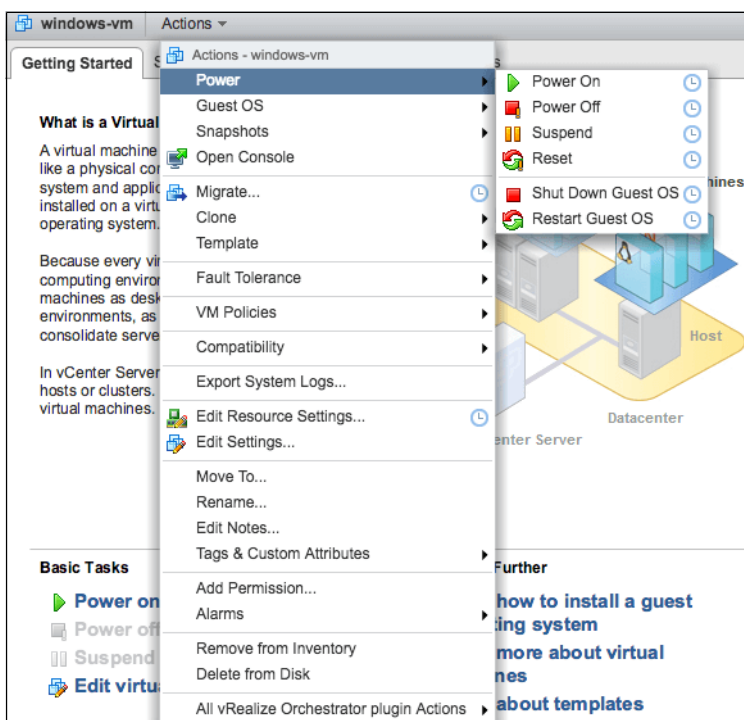


9. On the **Customize hardware** page, configure the VM hardware using the information below and click **Next**.
  - a. For **New Hard disk**, specify 30 GB or greater.
  - b. For **New CD\DVD Drive**, do the following:
    - i. Select **Datastore ISO File**.
    - ii. Select the Windows Server, version 1709 ISO file you uploaded to your datastore and click **OK**.
    - iii. Enable the **Connect At Power On** checkbox.
10. Review the configuration settings on the **Ready to complete** page and click **Finish**.

## Install Windows Server

To install Windows Server on the base VM, do the following:

1. After creating the VM, click **Power** > **Power On** in the **Actions** tab for your VM.



2. Select **Windows Server Standard**.
3. Select **Custom installation**.
4. Complete the installation process and enter a password for the Administrator user.

## Verify OS

To verify that you are using the correct OS version, run the following PowerShell command on the base VM:

```
Get-CimInstance Win32_OperatingSystem | Select-Object
Caption, Version, ServicePackMajorVersion, OSArchitecture, CSName, WindowsDirectory
```

The output should include `Version: 10.0.16299`.

## Install VMware Tools

To install VMware Tools on the base VM, do the following:

1. In the vSphere Web Client, right-click the base VM and select **Guest OS** > **Install VMware Tools**.

2. Navigate to the `D:` drive and run `setup64.exe`.
3. Restart the VM to complete the installation.

## Step 2: Install Windows Updates

Install Windows updates on the base VM using your preferred procedure. For example, you can install Windows updates by following the steps below. This procedure requires internet access.

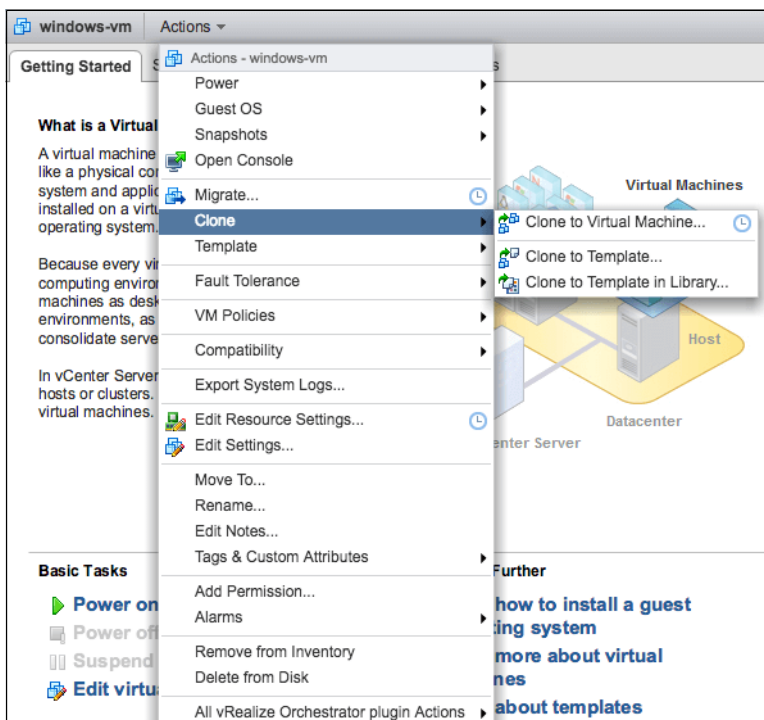
1. On the base VM, run the **SConfig** utility.
2. Select **Download and Install Updates**.
3. Enter **A** to search for all updates.
4. For **Select an option**, enter **A** to install all updates.

You may need to restart the base VM while installing the updates.

## Step 3: Clone the Base VM

To clone the base VM, do the following in the vSphere Web Client:

1. Power down the base VM.
2. Right-click the base VM.
3. Select **Clone > Clone to Virtual Machine**. This clone is your target VM.




4. Save the base VM. You will run Windows updates on this VM for future stemcells.

## Step 4: Construct the BOSH Stemcell

Before constructing the BOSH stemcell, collect the following information:

- Target VM IP address

- Target VM username
- Target VM password
- vCenter inventory path to the target VM in the `/MY-DATA-CENTER/vm/MY-FOLDER/MY-VM` format where:
  - `MY-DATA-CENTER` is the name of the data center.
  - `vm` is a static string.
  - `MY-FOLDER` is the name of the folder that contains the VM.
  - `MY-VM` is the name of the target VM.
- vCenter username
- vCenter password
- vCenter URL


 **Note:** The target VM must be routable from your local host. Before running the `construct` command, ensure you are logged out of the target VM.

To construct the BOSH stemcell, run the following command from your local host:

```
./STEMBUILD-BINARY construct -vm-ip TARGET-VM-IP -vm-username TARGET-USERNAME -vm-password TARGET-VM-PASSWORD -vcenter-url VCENTER-URL -vcenter-username VCENTER-USERNAME
```

Where:

- `STEMBUILD-BINARY` is the `stembuild` file for the version of your local host operating system and the version of the stemcell that you want to build. For example, `stembuild-windows-1709-19`.
- `TARGET-VM-IP` is the IP address of your target VM.
- `TARGET-USERNAME` is the username of an account with Administrator privileges.
- `TARGET-VM-PASSWORD` is the password for the Administrator account. The password must be enclosed in single quotes.
- `VCENTER-URL` is the URL of your vCenter.
- `VCENTER-USERNAME` is the username of your account in vCenter.
- `VCENTER-PASSWORD` is your password. The password must be enclosed in single quotes.
- `INVENTORY-PATH` is the vCenter inventory path to the target VM.

 **Note:** This operation may take up to an hour to complete and results in a powered-off target Windows VM in your vSphere environment. During `construct` execution, the WinRM connection terminates. This behavior is expected, and the `construct` command is still being executed. Do not attempt to re-run the `construct` command.

If you want to view the status of `construct`, you can log in to the target VM and do the following:

1. Start PowerShell.
2. Run the following command:

```
Get-Content -Path "C:\provision\log.log" -Wait
```

## Step 5: Package the BOSH Stemcell

Before packaging the BOSH stemcell, collect the following information:


- vCenter inventory path to the target VM in the `/MY-DATA-CENTER/vm/MY-FOLDER/MY-VM` format where:
  - `MY-DATA-CENTER` is the name of the data center.
  - `vm` is a static string.
  - `MY-FOLDER` is the name of the folder that contains the VM.
  - `MY-VM` is the name of the target VM.
- vCenter username
- vCenter password
- vCenter URL

To package the BOSH stemcell, run the following command from your local host:

```
./STEMBUILD-BINARY package -vcenter-url VCENTER-URL -vcenter-username VCENTER-USERNAME -vcenter-password VCENTER-PASSWORD -vm-inventory-path INVENTORY-PATH
```

Where:

- `STEMBUILD-BINARY` is the `stembuild` file for the version of your local host operating system and the version of the stemcell that you want to build. For example, `stembuild-windows-1709-19`.
- `VCENTER-URL` is the URL of your vCenter.
- `VCENTER-USERNAME` is the username of your account in vCenter.
- `VCENTER-PASSWORD` is your password. The password must be enclosed in single quotes.
- `INVENTORY-PATH` is the vCenter inventory path to the target VM.

 **Note:** This command creates a stemcell on your local host in the folder where you ran the command and may take up to 30 minutes to complete.

## Step 6: Upload the BOSH Stemcell to Ops Manager

To upload the BOSH stemcell to Ops Manager, do the following:

1. In Ops Manager, navigate to **Stemcell Library**.
2. Upload your BOSH stemcell.
3. Deploy the PAS for Windows tile.

## Monthly Stemcell Upgrades

After Microsoft releases operating system updates, you should upgrade your BOSH stemcell. Microsoft typically releases Windows updates on the second Tuesday of each month.

To upgrade your BOSH stemcell, do the following:

1. [Install Windows Updates](#) on the base VM.
2. [Clone the Base VM](#).
3. [Construct the BOSH Stemcell](#).
4. [Package the BOSH Stemcell](#).
5. Replace the existing stemcell in the Ops Manager stemcell library with this new stemcell.
6. Deploy the PAS for Windows tile.

## Known Issues

### Authentication Error with Special Characters in stembuild Commands

#### Symptom

```
./out/stembuild: ServerFaultCode: Cannot complete login due to an incorrect user name or password.
vcenter_client - unable to validate url: vcenter.example.com
```

#### Explanation

`stembuild` uses govc libraries. These libraries cannot parse the special characters `/`, `#`, and `:`. This results in errors when authenticating with vCenter.

## Workaround

If your vCenter username or password contains `/`, `#`, or `:`, set the following environment variables:

```
export GOVC_USERNAME=VCENTER-USERNAME
export GOVC_PASSWORD=VCENTER-PASSWORD
```

Where:

- `VCENTER-USERNAME` is your vCenter account username. For example, `johndoe`.
- `VCENTER-PASSWORD` is your vCenter account password. For example, `pass#word`.

If you are using other special characters, add single quotes around the input parameters. For example:

```
./STEMBUILD-BINARY package -vcenter-url VCENTER-URL -vcenter-username 'admin@' -vcenter-password VCENTER-PASSWORD -vm-inventory-path INVENTORY-PATH
```

## Installing and Configuring PASW

This topic describes how to install and configure the Pivotal Application Service for Windows (PASW) tile. The PASW tile installs Windows cells in your Pivotal Cloud Foundry (PCF) deployment.

### Step 1: Confirm Shared PAS Tile Settings

There are two settings in the **Pivotal Application Service** tile that affect the Windows cells installed by the **Pivotal Application Service for Windows** tile. Configure these settings as desired:

- In the **Networking** section, if you select the **Disable SSL certificate verification for this environment** checkbox, SSL certificate verification is disabled for Windows cells.
- In the **System Logging** section, if you configure an external syslog aggregator, logs are drained from Windows cells as well as non-Windows cells.

### Step 2: Install the Tile

1. Download the **Pivotal Application Service for Windows** product file from the product page of [Pivotal Network](#).
2. From the same [Pivotal Network](#) page, download the **Windows FS Injector** tool for your workstation OS.

The Injector tool, `winfs-injector`, is an executable binary that adds the Windows Server container base image into the product file. This step requires internet access and can take up to 20 minutes.

**Note:** You need the `git` and `tar` (BSD) executables on your `%PATH%` to run the `winfs-injector` bin. For example, to use `winfs-injector.exe`, `tar.exe` must be copied to a directory in your `%PATH%`.

3. Run `winfs-injector` with the following options, replacing `PAS-WINDOWS-DOWNLOADED.pivotal` with the path to the downloaded **PASW** product file and `PAS-WINDOWS-INJECTED.pivotal` with a desired output path for the importable product file:

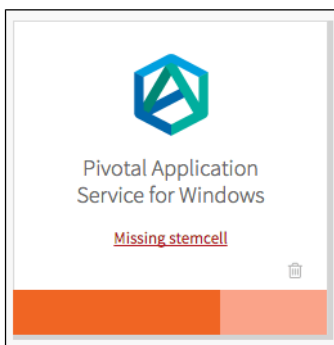
```
$ winfs-injector --input-tile PAS-WINDOWS-DOWNLOADED.pivotal \
--output-tile PAS-WINDOWS-INJECTED.pivotal
```

For troubleshooting the `winfs-injector`, see [Missing Local Certificates for Windows File System Injector](#).

4. Navigate to the Ops Manager Installation Dashboard and click **Import a Product**.
5. Select the importable `PAS-WINDOWS-INJECTED.pivotal` file on your workstation. **PASW** appears in the product list under **Import a Product**.
6. Click + under the **PASW** product listing to add it to your staging area.

### Step 3: Configure the Tile

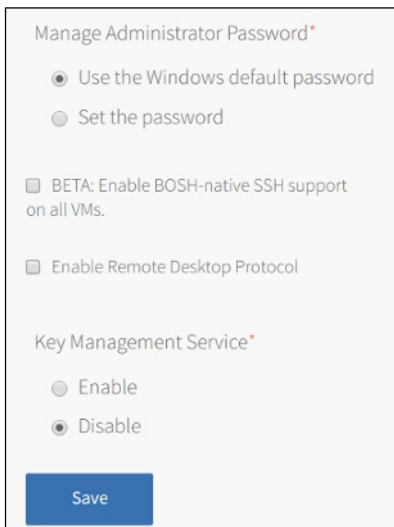
1. Click the newly added **PASW** tile.



2. Click **Assign AZs and Networks** or **Assign Networks**. The name of the section varies depending on your IaaS.

3. Assign your AZs and networks and click **Save**.


4. Click **VM Options**.



5. Specify your selection for **Manage Administrator Password**.

- **Use the Windows default password** randomizes the admin password. With this selection, the admin password is not retrievable by an operator. This is the default selection.
- **Set the password** sets the same admin password for every Windows cell. As a result, this password can be used to access any Windows cell, including, for example, Remote Desktop Protocol (RDP) sessions.

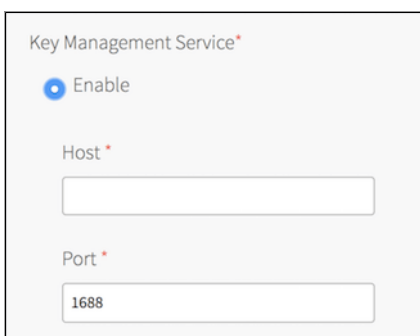
6. (Optional) Select the **BETA: Enable BOSH-native SSH support on all VMs** checkbox to start the Microsoft beta port of the OpenSSH daemon on port 22 on all VMs. Users can SSH onto Windows VMs with the `bosh ssh` command, and enter a CMD terminal as an admin user. They can then run `powershell.exe` to start a PowerShell session.

 **Note:** This feature is beta and not considered production-ready.

7. (Optional) If you want all VMs to support connection through Remote Desktop Protocol (RDP), click **Enable Remote Desktop Protocol**.

8. (Optional) If you want to configure a Key Management Service (KMS) that your volume-licensed Windows cell can register with, perform the following steps:

- a. Click **Enable**
- b. For the **Host** field, enter the KMS hostname.
- c. For the **Port** field, enter the port number. The default port number is `1688`.



9. Click **Save**.


10. (Optional) To deploy your PASW application workloads to an isolation segment, click **Application Containers** and perform the steps in the [Assign a Tile to an Isolation Segment](#) section below.

11. (Optional) To configure Windows cells to send Windows Event logs to an external syslog server, click **System Logging** and perform the steps in the [Send Cell Logs to a Syslog Server](#) section.

12. (Optional) To enable advanced features in PASW, click **Advanced Features** and perform the following steps:

a. To configure memory and disk overcommit for your Windows Diego cells, follow the steps below:

- i. Enter the total desired amount of Diego cell memory in the **Cell Memory Capacity (MB)** field. For the current cell memory capacity settings, see the Windows Diego cell row on the **Resource Config** pane.
- ii. Enter the total desired amount of Diego cell disk capacity in the **Cell Disk Capacity (MB)** field. For the current cell disk capacity settings, see the Windows Diego cell row on the **Resource Config** pane.

 **Note:** Due to the risk of app failure and the deployment-specific nature of disk and memory use, Pivotal has no recommendation about how much, if any, memory or disk space to overcommit.

Cell Memory Capacity (MB) ( min: 1 )

Cell Disk Capacity (MB) ( min: 1 )

b. Click **Save**.

13. Click **Errands**. Pivotal recommends that you set the **Install HWC Buildpack Errand** to **On**. This ensures that you receive the most up-to-date HWC Buildpack.

Post-Deploy Errands

Install HWC Buildpack Errand

On

There are no pre-delete errands for this product.


Save

14. Click **Save**.

## Step 4: Configure Tile Resources

To configure your tile resources, perform the following steps:

1. Navigate to the **Resource Config** pane of the PASW tile.
2. Use the dropdown menus to configure **Windows Diego Cell**. For more information, see [Disk Size of Windows Diego Cells](#).
3. Click **Save**.

 **Note:** Provision your **Master Compilation Job** with the minimum disk space for your IaaS as follows:

- **AWS:** 128 GB
- **Azure:** 100 GB
- **GCP:** 100 GB
- **vSphere:** 128 GB


## Disk Size of Windows Diego Cells

Before configuring the disk size of your Windows Diego cells, review the information below:




- **Windows stemcells v1709.13 and later in the 1709 line** support ephemeral disks. If your PASW deployment is based on one of these stemcells, the recommended disk size for your Windows Diego cells is as follows:

| IaaS    | Disk size of Windows Diego cell |
|---------|---------------------------------|
| AWS     | 100 GB                          |
| Azure   | 150 GB                          |
| GCP     | 150 GB                          |
| vSphere | 100 GB                          |

 **Note:** If you use vSphere, you must create your own stemcell. The default root disk size of Windows stemcell v1709.13 and later in the 1709 line is 30 GB. Pivotal recommends setting the root disk size of your Windows stemcell for vSphere to 30 GB. For more information, see [Creating a Windows Stemcell for vSphere Manually](#) or [Creating a Windows Stemcell for vSphere Using stembuild \(Beta\)](#).

- **Windows stemcells v1709.5 through v1709.12** do not support ephemeral disks. The size of the root disk of your stemcell determines the minimum root disk size of any Windows VM that the BOSH Director can create from that stemcell. If your PAS for Windows deployment is based on one of these stemcells, ensure that **Windows Diego Cell** has a minimum disk size according to the table below.

| IaaS    | Disk size of Windows stemcell v1709.5-v1709.12 |
|---------|------------------------------------------------|
| AWS     | 128 GB                                         |
| Azure   | 30 GB                                          |
| GCP     | 100 GB                                         |
| vSphere | Recommended 128 GB+                            |

 **Note:** Because you create your own stemcell on vSphere, you can control its root disk size.

## Step 5: Upload the Stemcell

1. Go to **Stemcell Library**.
2. Retrieve the stemcell that you downloaded or created in [Downloading or Creating a Windows Stemcell](#).
3. Follow the steps in [Importing and Managing Stemcells](#) to upload the Windows stemcell to **Pivotal Application Service for Windows**.

## Step 6: Deploy the Tile

1. Return to the Ops Manager Installation Dashboard and click **Apply Changes** to install the PASW tile.

## Step 7: (Optional) Create More Tiles

To run Windows cells in multiple isolation segments, you must create and configure additional PASW tiles. For more information, see [Windows Cells in Isolation Segments](#).

## Windows Cells in Isolation Segments

This topic explains how to run Windows cells in isolation segments, which are compartmentalized resource pools for Diego cells.

Cells in one isolation segment share routing, computing, and logging resources with other cells in the same segment, and do not use resources from other isolation segments.

### Overview

To run Windows cells in multiple isolation segments, you need to create and install multiple PAS for Windows tiles and configure each to run in a different isolation segment.

If the isolation segments do not already exist in the Cloud Controller Database (CCDB), you need to create them there.

See [Replicate a Tile](#) for how to create multiple copies of the PAS for Windows tile.

See [Assign a Tile to an Isolation Segment](#) for how to associate a PAS for Windows tile with an isolation segment, so that its cells run in that segment.

See the [Create an Isolation Segment](#) section of the *Managing Isolation Segments* topic for instruction about adding an isolation segment to the CCDB.

### Replicate a Tile

To make multiple copies of the **PAS for Windows** tile that you can assign to different isolation segments, use the Replicator tool as follows:

1. Download the Replicator tool from the **Pivotal Cloud Foundry Runtime for Windows** section of [Pivotal Network](#).
2. Navigate to the directory where you downloaded the Replicator tool.
3. Replicate the tile:

```
./replicator \
-name "YOUR-NAME" \
-path /PATH/TO/ORIGINAL.pivotal \
-output /PATH/TO/COPY.pivotal
```

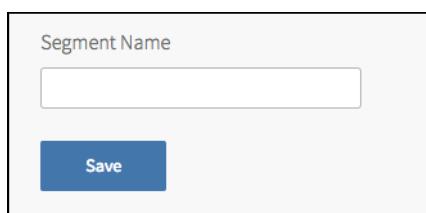
Replace the values above with the following:

- `YOUR-NAME`: Provide a unique name for the new PAS for Windows tile. The name must be ten characters or less and only contain alphanumeric characters, dashes, underscores, and spaces.
  - `/PATH/TO/ORIGINAL`: Provide the absolute path to the original PAS for Windows tile you downloaded from Pivotal Network.
  - `/PATH/TO/COPY`: Provide the absolute path for the copy of the PAS for Windows tile that the Replicator tool produces.
4. Install and configure the Windows isolation segment, using the new `.pivotal` file and following the procedures in this topic, starting with the **Import a Product** step of [Step 2: Install the Tile](#).


### Assign a Tile to an Isolation Segment

To assign a PAS for Windows tile to an isolation segment, perform the following steps:

1. Open the **Application Containers** pane.



2. Under **Segment Name**, enter the name for the isolation segment to associate the tile with. If you are creating a new isolation segment, ensure that this name is unique across your PCF deployment.

3. Click **Save**.
4. If you are creating a new isolation segment, follow the steps in the [Create an Isolation Segment](#)  section of the *Managing Isolation Segments* topic to add the isolation segment to the CCDB.

## Migrating Apps to PAS for Windows

This topic describes the process of migrating apps running on PAS for Windows 2012R2 cells to run on PAS for Windows cells, which run Windows Server 2016.

Pivotal recommends you use the blue-green deployment method for high availability. For more information about blue-green deployments, see [Using Blue-Green Deployment to Reduce Downtime and Risk](#).

### Step 1: Install and Deploy PAS for Windows Tile

To install and deploy the **PAS for Windows** tile, follow steps 1 and 2 of [Installing and Configuring PAS for Windows](#).

### Step 2: Push App to PAS for Windows Cells

Perform the following steps to redeploy a running app with zero downtime using the blue-green method:

1. Run `cf login` to log in to the Cloud Foundry Command Line Interface (cf CLI).
2. Choose your org and space.
3. Navigate to the location of your app.
4. Run `cf apps` to find the name of the app, `ORIGINAL_APP_NAME`, that you are migrating from PAS for Windows 2012R2 to PAS for Windows. Create a new name for the app to replace it. Pivotal recommends you append `-green` to your app name, `APP_NAME-green`.
5. Run `cf push` to push the renamed app `APP_NAME-green`, passing in `-s windows2016`, `--no-route`, and `--no-start`.

```
$ cf push APP_NAME-green -s windows2016 -b BUILDPACK -n HOSTNAME --no-start --no-route
```

- For **BUILDPACK**, enter your custom buildpack by name or Git URL with an optional branch or tag.
- For **HOSTNAME**, enter the subdomain name you are pushing to.
- `-s windows2016` runs the app in a Windows Server 2016-based cell.
- `--no-start` creates the instance VMs but does not start the app.
- `--no-route` prevents the push command from automatically mapping a route to the app.
- For more command options, see [cf push](#).

6. Switch the router so all incoming requests go to `ORIGINAL_APP_NAME` and `APP_NAME-green` using the `cf map-route` command. The command requires you enter your domain name after the app name. For example, `example.com`.

```
$ cf map-route APP_NAME-green DOMAIN -n HOSTNAME
```

7. Start the green app.

```
$ cf start APP_NAME-green
```

8. Run `cf apps` to confirm that both your `ORIGINAL_APP_NAME` and `APP_NAME-green` are running. If you experience a problem, see [Troubleshooting Application Deployment and Health](#).
9. Unmap the original app's route by running the `cf unmap-route` command.

```
$ cf unmap-route ORIGINAL_APP_NAME DOMAIN -n HOSTNAME
```

### Step 3: Delete App from Windows 2012R2 Server Cells

To delete the `ORIGINAL_APP_NAME`, run the `cf delete` command. To also delete any mapped routes, run the command with the `-r` flag.

```
$ cf delete ORIGINAL_APP_NAME -r
```

## Step 4: (Optional) Uninstall Old Tile

Once you have migrated all of your apps and you are no longer using the **Windows 2012R2** tile, a PCF operator can perform the following steps:

1. From the **Installation Dashboard**, click the trash icon on the tile to remove that product. In the **Delete Product** dialog box that appears, click **Confirm**.
2. In the **Pending Changes** view, click **Apply Changes**.  
After you delete a product, the product tile is removed from the installation and the **Installation Dashboard**. However, the product appears in the **Available Products** view.

## Upgrading PAS for Windows and Windows Cells

This topic describes how to upgrade the Pivotal Application Service (PAS) for Windows tile and update the Windows stemcell.

For how developers can migrate apps to PAS for Windows from either PAS for Windows 2012R2 or PCF Runtime for Windows, see [Migrating Apps to PAS for Windows](#).

## Rotating Credentials

The PAS tile handles all of the credentials for PAS for Windows.

To rotate your credentials in PAS for Windows, re-deploy PAS and PAS for Windows by navigating to the Ops Manager Installation Dashboard and clicking **Apply Changes**.

## Upgrade PAS for Windows

To upgrade PAS for Windows:

1. Follow the instructions [Upgrading PCF Products](#) with the latest PAS for Windows product download from [Pivotal Network](#).
2. If necessary, configure the product. For more information about configuring PAS for Windows, see the [Installing and Configuring PAS for Windows](#) topic.
3. Locate the **Pending Changes** section on the right-hand side of the screen and click **Apply Changes**.

## Upgrade the Windows Stemcell

1. Retrieve the stemcell by following the steps below for your IaaS:
  - For vSphere, you must build your own stemcell. For more information, see [Creating a Windows Stemcell for vSphere Manually](#) or [Creating a Windows Stemcell for vSphere Using stembuild \(Beta\)](#).
  - For AWS, GCP, and Azure, navigate to the **Stemcells for PCF (Windows Server)** section of [Pivotal Network](#).
2. Go to **Stemcell Library**.
3. Click **Import Stemcell** to import the stemcell file.
4. When prompted, enable the Ops Manager product checkbox to stage your stemcell.
5. Click **Apply Stemcell to Products**.

For more information about Windows stemcells, see [Downloading or Creating Windows Stemcells](#).

## Using SMB Volumes in .NET Apps

This topic describes how to use Server Message Block (SMB) Volumes in a .NET Application. In this example, we create an application that reads and writes to a `note.txt` file within an SMB Volume share.

### Prerequisites

The following is required to use SMB Volumes in your .NET App:

- Visual Studio
- An Azure account
- Pivotal Application Service for Windows (PASW)
- An accessible SMB Volume in Azure Cloud with a UNC path
  - If you do not have an accessible SMB Volume, refer to *Create a file share in Azure Files* in the [Azure documentation](#).
- An existing .NET Framework application
- SMB Username
- SMB Password
- Windows 1803.x or Windows 1709.x Stemcell

### Using SMB Volumes in .NET Apps with Steeltoe

Steeltoe is a set of libraries that help your team write cloud native applications. Steeltoe contains functionality for mounting SMB Volumes. Using Steeltoe requires modifying your application code. For more information, see the [Steeltoe Documentation](#).

If you are using Steeltoe, add the following environment variables to your Config Server Provider :

- `SMB_PATH`
- `SMB_USERNAME`
- `SMB_PASSWORD`

Where:

- `SMB_PATH` is the UNC path to your SMB.
  - If you are using the Windows 1709 Stemcell, your UNC is the IP of the machine you are using.
  - If you are using the Windows 1803 Stemcell, your UNC is the FQDN of the machine you are using.
- `SMB_USERNAME` is your Azure account username.
- `SMB_PASSWORD` is your Azure account password.

For more information on adding environment variables to your Config Server Provider, see [Config Server Provider](#) in the Steeltoe documentation.

After adding your environment variables to your Config Server Provider, proceed to [SMB Mounting](#).

### Using SMB Volumes in .NET Apps with Your Batch Profile

If you do not want to modify your application code to include Steeltoe, you can utilize SMB Mounting without Steeltoe.

1. Retrieve the UNC of your existing SMB share.
  - a. If you are using the Windows 1709.x Stemcell, your UNC is your machine's IP address.
    - i. To look up your machine's IP address, you can run the `nslookup` command. For more information, see [nslookup](#) in Microsoft's *Commands by Server Role* Documentation.
  - b. If you are using the Windows 1803 Stemcell, your UNC is your machine's FQDN.

2. Create a `.profile.bat` file in your .NET app's root directory.
3. Use Apps Manager or the Cloud Foundry Command Line Interface (cf CLI) to set the following environment variables:

- `SMB_PATH`
- `SMB_USERNAME`
- `SMB_PASSWORD`

4. Add the following command to your `.profile.bat` file:

```
net use z: %SMB-PATH% %SMB-PASSWORD% /USER:SMB-USERNAME%
```

5. Proceed to [SMB Mounting](#).

## SMB Mounting

1. Using CF CLI or Apps Manager, add `SMB_PATH`, `SMB_USERNAME`, and `SMB_PASSWORD` as environment variables to your local computer or the computer you are deploying using for deploying your application.
  - If you are using SMB Volumes with your batch profile and have already added these environment variables, ignore this step.



**Note:** If Visual Studio does not detect these new environment variables, restart Visual Studio.

2. In Visual Studio, create a new file in your solution named `SMBConfiguration.cs`. This file is the single representation of your SMB Volume configuration and reads the connection data from the environment variables you established previously.

```
// SMBConfiguration.cs
using System;

namespace NetFrameworkApp.Controllers
{
 public class SMBConfiguration
 {
 public String GetSharePath()
 {
 return Environment.GetEnvironmentVariable("SMB_PATH");
 }

 public String GetUserName()
 {
 return Environment.GetEnvironmentVariable("SMB_USERNAME");
 }

 public String GetPassword()
 {
 return Environment.GetEnvironmentVariable("SMB_PASSWORD");
 }
 }
}
```

3. In Visual studio, create a new MVC Controller named `NoteController`. This file creates a controller endpoint that reads a the example note file. For more information on creating a controller, see [Add a controller to an ASP.NET Core MVC app](#) in the Microsoft Documentation.
4. In the command line, add `Steeltoe.Common` and `Steeltoe.Common.Net` to your application with a Package Manager of your choice. If you are not using Steeltoe, ignore this step.
5. Edit `NoteController.cs` to read from a file named `note.txt`, which does not exist yet but the `FileMode.OpenOrCreate` method creates that file. Refer to the example code snippet below, which reads the contents of the note file and stashes the `note.txt` content in the Viewbag. If you are not using Steeltoe, ignore the reference to `Steeltoe.Common.Net` in the following code snippet.

```
// NoteController.cs
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Web;
using System.Web.Mvc;
using Steeltoe.Common.Net;
```



```
namespace NetFrameworkApp.Controllers
{
 public class NoteController : Controller
 {
 SMBConfiguration configuration = new SMBConfiguration();
 public ActionResult Index()
 {
 var credential = new NetworkCredential(configuration.GetUserName(), configuration.GetPassword());

 using (var share = new WindowsNetworkFileShare(configuration.GetSharePath(), credential))
 using (var inputStream = new FileStream(Path.Combine(configuration.GetSharePath(), "note.txt"), FileMode.OpenOrCreate))
 using (var streamReader = new StreamReader(inputStream))
 {
 // Never display raw user input as HTML. Do not do this in production code.
 ViewBag.Note = streamReader.ReadToEnd();
 }

 return View();
 }
 }
}
```

6. In Visual Studio, create a subdirectory in **Views** named `Note`.
7. In Visual Studio, create a new View named `Index`. For more information on Views, see [Views in ASP.NET Core MVC](#) and [Add a view to an ASP.NET Core MVC app](#) in the Microsoft Documentation.
8. In Visual Studio, create a `Index.cshtml` file that contains the following:

```
// Index.cshtml

@ViewBag.Note
```

Running the application now would show an empty page with no errors.

9. Modify the `Index.cshtml` file to contain a form. This form posts to a yet to be created update endpoint and also displays our note inside a text area.

```
// Index.cshtml
...
<form action="https://docs.pivotal.io/note/update" method="post">
 <textarea name="note">@ViewBag.Note</textarea>
 <div>
 <button type="submit">Update</button>
 </div>
</form>
```

10. Modify the `NoteController.cs` to have an update endpoint. This endpoint saves the data posted to the endpoint back into the `note.txt`. Refer to the example code snippet in the following step.
11. Modify the `NoteController.cs` to include the ControllerBase class `RedirectToAction` method, which redirects to the index page so the user can see what was just saved. For more information on the ControllerBase class, see the [Microsoft .NET API Browser Documentation](#).

Refer to the example code snippet below.

```
// NoteController.cs
namespace NetFrameworkApp.Controllers
{
 public class NoteController : Controller
 {
 ...

 [HttpPost]
 public ActionResult Update(String note)
 {
 var credential = new NetworkCredential(configuration.GetUserName(), configuration.GetPassword());

 using (var share = new WindowsNetworkFileShare(configuration.GetSharePath(), credential))
```

```
using (var outputStream = new FileStream(Path.Combine(configuration.GetSharePath(), "note.txt"), FileMode.Create))
using (var streamWriter = new StreamWriter(outputStream))
{
 streamWriter.Write(note);
}

return RedirectToAction("Index");
}
}
```

## Known Issue

### Inability to SSH Into App Instance

Despite an SMB mapping being successfully created, trying to `cf ssh` into that app instance to access the created mapping results in an unspecified path error.

## Troubleshooting Windows Cells

This topic describes how to troubleshoot Windows Diego cells deployed by Pivotal Application Service (PAS) for Windows.

### Installation Issues

This section describes issues that may occur during the installation process.

#### Missing Local Certificates for Windows File System Injector

##### Symptom

You run the `winfs-injector` and see the following error about certificates:

```
Get https://auth.docker.io/token?service=registry.docker.io&
scope=repository:cloudfoundry/windows2016fs:pull: x509:
failed to load system roots and no roots provided
```

##### Explanation

Local certificates are needed to communicate with Docker Hub.

##### Solution

Install the necessary certificates on your local machine. On Ubuntu, you can install certificates with the `ca-certificates` package.

#### Outdated Version for Windows File System Injector

##### Symptom

You run the `winfs-injector` and see the following error about a missing file or directory:

```
open ...windows2016fs-release/VERSION: no such file or directory
```

##### Explanation

You are using an outdated version of the `winfs-injector`.


##### Solution

From [Pivotal Network](#), download the recommended version of **PAS for Windows File System Injector** tool for the tile.

#### Missing Container Image

##### Symptom

You click the + icon in Ops Manager to add the PAS for Windows tile to the Installation Dashboard, and you see the error:

 is invalid: has an invalid release 'windows2016fs' specified for job type 'Windows Diego Cell'

##### Explanation

The product file you are trying to upload does not contain the Windows Server container base image.

## Solution

1. Delete the product file listing from Ops Manager by clicking its trash can icon under **Import a Product**.
2. Follow the PAS for Windows [installation instructions](#) to run the `wins-injector` tool locally on the product file. This step requires internet access, can take up to 20 minutes, and adds the Windows Server container base image to the product file.
3. Click **Import a Product** to upload the “injected” product file.
4. Click the + icon next to the product listing to add the PAS for Windows tile to the Installation Dashboard.

## Windows Cell Log Types

Windows cells generate two types of logs:

- **BOSH job logs**, such as `rep_windows` and `consul_agent_windows`. These logs stream to the syslog server configured in the PAS tile **System Logging** pane, along with other PCF component logs. The names of these BOSH job logs correspond to the names of the logs emitted by Linux Diego cells.
- **Windows Event logs**. These stream to the syslog server configured in the PAS for Windows **System Logging** pane and are downloadable through Ops Manager, as described [below](#).

## Access Windows Event Logs

PCF operators can access log messages from Windows Diego cells in two ways:

- Configure PAS for Windows to [send](#) all Windows cell logs to an external syslog server.
- [Download](#) archived logs from each Windows cell individually.

## Send Cell Logs to a Syslog Server

To forward Windows cell log messages to an external syslog server, complete the following steps:

1. Navigate to the Ops Manager Installation Dashboard.
2. Click the **PAS for Windows** tile.
3. Under the **Settings** tab, select the **System Logging** pane.

### Configure system logging.

Enable Syslog for VM logs?\*

☒ Enable

Address \*

Port \*


Protocol\*

Select the transport protocol for forwarding logs.

☐ Disable

**Save**

- Under **Enable Syslog for VM logs?**, click **Enable**
- Under **Address**, enter the IP address of your syslog server.
- Under **Port**, enter the port of your syslog server. The typical port for a syslog server is `514`.

 **Note:** The host must be reachable from the PAS network. Ensure your syslog server listens on external interfaces.

- Under **Protocol**, select the transport protocol to use when forwarding logs.
- Click **Save**.

## Download Cell Logs

Perform the following steps to retrieve the logs from a Windows cell:

- Navigate to the Ops Manager Installation Dashboard.
- Click the **PAS for Windows** tile.
- Click the **Status** tab.
- Under the **Logs** column, click the download icon for the Windows cell you want to retrieve logs from.
- Click the **Logs** tab.
- When the logs are ready, click the filename to download them.
- Unzip the file to examine the contents. Each component on the cell has its own logs directory:

- `/consul_agent_windows/`
- `/garden-windows/`
- `/metron_agent_windows/`
- `/rep_windows/`

## Connect to a Windows Cell

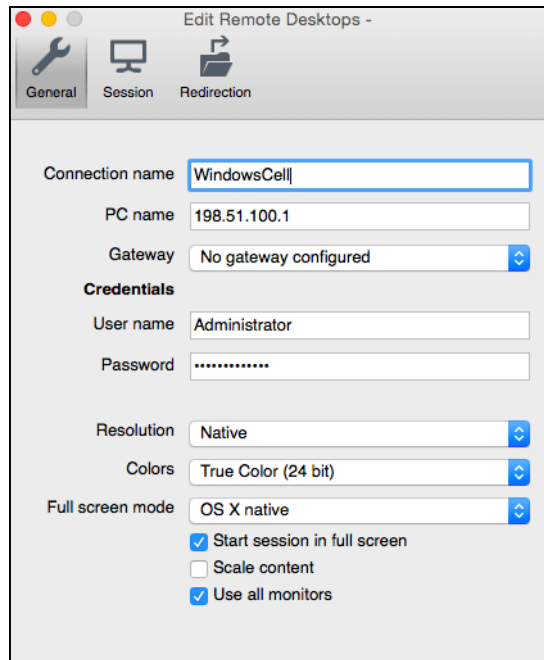
Perform the following steps to connect to a Windows cell to run diagnostics:

1. Download and install a Remote Desktop Protocol (RDP) client.
  - For Mac OS X, download the Microsoft Remote Desktop app from the [Mac App Store](#).
  - For Windows, download the Microsoft Remote Desktop app from [Microsoft](#).
  - For Linux/UNIX, download a RDP client like [rdesktop](#).
2. Follow the steps in the [Log into BOSH](#) section of the *Advanced Troubleshooting with the BOSH CLI* topic to log in to your BOSH Director. The steps vary slightly depending on whether your PCF deployment uses internal authentication or an external user store.
3. Retrieve the IP address of your Windows cell using the BOSH CLI. Run the following command, replacing `MY-ENV` with the alias you assigned to your BOSH Director:

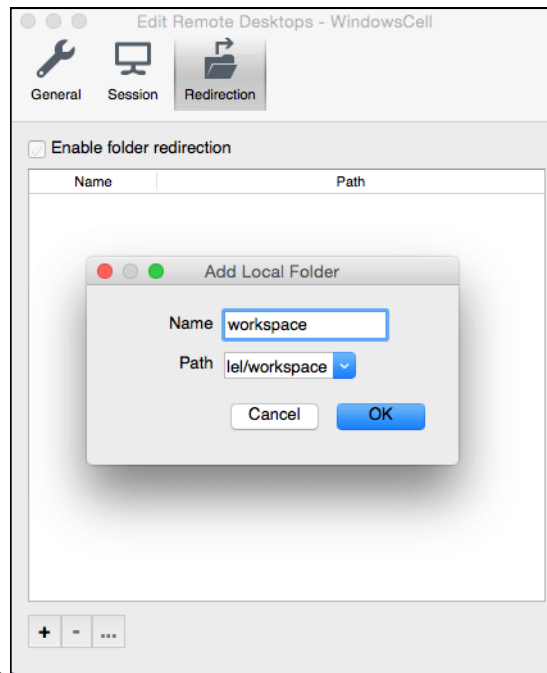
```
$ bosh -c MY-ENV -d garden-windows
Using environment 'DIRECTOR-IP' as client 'admin'
```

| Name           | Release(s) | Stemcell(s) | Team(s) | Cloud Config |
|----------------|------------|-------------|---------|--------------|
| garden-windows | ...        | ...         | -       | latest       |

4. Retrieve the Administrator password for your Windows cell by following the steps for your IaaS:
  - On vSphere, this is the value of `WINDOWS_PASSWORD` in the `consumer-vars.yml` file you used to previously build a stemcell.
  - On Amazon Web Services (AWS), navigate to the AWS EC2 console. Right-click on your Windows cell and select **Get Windows Password** from the drop-down menu. Provide the local path to the `ops_mgr.pem` private key file you used when installing Ops Manager and click **Decrypt password** to obtain the Administrator password for your Windows cell.
  - On Google Cloud Platform (GCP), navigate to the Compute Engine Dashboard. Under **VM Instances**, select the instance of the Windows VM. At the top of the page, click on **Create or reset Windows password**. When prompted, enter "Administrator" under **Username** and click **Set**. You will receive a one-time password for the Windows cell.
  - You cannot RDP into Windows cells on Azure.
5. Open your RDP client. The examples below use the Microsoft Remote Desktop app.



6. Click **New** and enter your connection information:
  - **Connection name:** Enter a name for this connection.
  - **PC name:** Enter the IP address of your Windows cell.
  - **User name:** Enter `Administrator`.
  - **Password:** Enter the password of your Windows cell that you obtained above.
7. To mount a directory on your local machine as a drive in the Windows cell, perform the following steps:
  - a. From the same **Edit Remote Desktops** window as above, click **Redirection**.



- b. Click the plus icon at the bottom left.
- c. For **Name**, enter the name of the drive as it will appear in the Windows cell. For **Path**, enter the path of the local directory.
- d. Click **OK**.

8. Close the **Edit Remote Desktops** window and double-click the newly added connection under **My Desktops** to open a RDP connection to the Windows cell.
9. In the RDP session, you can use the [Consul CLI](#) to diagnose problems with your Windows cell.

## Consul CLI

Perform the following steps to use the Consul CLI on your Windows cell to diagnose problems with your Consul cluster:

1. In your RDP session, open a PowerShell window.
2. Change into the directory that contains the Consul CLI binary:

```
PS C:\Users\Administrator> cd C:\var\vcap\packages\consul-windows\bin\
```

3. Use the Consul CLI to list the members of your Consul cluster:

```
PS C:\Users\Administrator\var\vcap\packages\consul-windows\bin> .\consul.exe members
Node Address Status Type Build Protocol DC
cell-windows-0 10.0.0.111:8301 alive client 0.6.4 2 dc1
cloud-controller-0 10.0.0.94:8301 alive client 0.6.4 2 dc1
cloud-controller-worker-0 10.0.0.99:8301 alive client 0.6.4 2 dc1
consul-server-0 10.0.0.96:8301 alive server 0.6.4 2 dc1
diego-brain-0 10.0.0.109:8301 alive client 0.6.4 2 dc1
diego-cell-0 10.0.0.103:8301 alive client 0.6.4 2 dc1
diego-cell-1 10.0.0.104:8301 alive client 0.6.4 2 dc1
diego-cell-2 10.0.0.107:8301 alive client 0.6.4 2 dc1
diego-database-0 10.0.0.92:8301 alive client 0.6.4 2 dc1
ha-proxy-0 10.0.0.254:8301 alive client 0.6.4 2 dc1
nfs-server-0 10.0.0.100:8301 alive client 0.6.4 2 dc1
router-0 10.0.0.105:8301 alive client 0.6.4 2 dc1
uaa-0 10.0.0.93:8301 alive client 0.6.4 2 dc1
```

4. Examine the output to ensure that the `cell-windows-0` service is registered in the Consul cluster and is `alive`. Otherwise, your Windows cell cannot communicate with your PCF deployment and developers cannot push .NET apps to the Windows cell. Check the configuration of your Consul cluster, and ensure that your certificates are not missing or misconfigured.

## Using Apps Manager

The web-based Apps Manager application helps you manage users, organizations, spaces, and applications.

### Table of Contents

- [Getting Started with Apps Manager](#)
- [Managing Orgs and Spaces Using Apps Manager](#)
- [Managing User Roles with Apps Manager](#)
- [Managing Apps and Service Instances Using Apps Manager](#)
- [Viewing ASGs in Apps Manager](#)
- [Monitoring Instance Usage with Apps Manager](#)
- [Configuring Spring Boot Actuator Endpoints for Apps Manager](#)
- [Using Spring Boot Actuator Endpoints with Apps Manager](#)



## Getting Started with Apps Manager

Page last updated:

This topic describes the functions and scope of Apps Manager, a web-based tool for managing Pivotal Application Service (PAS) organizations, spaces, applications, services, and users.

### Scope

Apps Manager provides a visual interface for performing the following subset of functions available through the Cloud Foundry Command Line Interface (cf CLI):

- **Orgs:** You can create and manage orgs.
- **Spaces:** You can create, manage, and delete spaces.
- **Apps:** You can scale apps, bind apps to services, manage environment variables and routes, view logs and usage information, start and stop apps, and delete apps.
- **Services:** You can bind services to apps, unbind services from apps, choose and edit service plans, and rename and delete service instances.
- **Users:** You can invite new users, manage user roles, and delete users.

To access Apps Manager as the Admin user, see the [Logging in to Apps Manager](#) topic.

### Browser Support

Apps Manager is compatible with the latest major versions of the following browsers:

- [Apple Safari](#) 
- [Google Chrome](#) 
- [Microsoft Edge](#) 
- [Microsoft Internet Explorer](#) 
- [Mozilla Firefox](#) 

Pivotal recommends using Chrome, Firefox, Edge, or Safari for the best Apps Manager experience.

### About Permissions

Your ability to perform actions in Apps Manager depends on your user role and the [feature flags](#) that the Admin sets.

The table below shows the relationship between specific org and space management actions and the non-Admin user roles who can perform them. A non-Admin user must be a member of the org and space to perform these actions.

Admin users can perform all of these actions using either the cf CLI or by logging into Apps Manager as an Org Manager, using the UAA Admin credentials.

Space Managers assign and remove users from spaces by setting and unsetting their roles within the space.

| Action                      | CLI command                 | Org Manager | Space Manager | Org Auditor, Space Developer, or Space Auditor |
|-----------------------------|-----------------------------|-------------|---------------|------------------------------------------------|
| Create an org               | <code>create-org</code>     | †           | †             | †                                              |
| Delete an org               | <code>delete-org</code>     | No          | No            | No                                             |
| Rename an org               | <code>rename-org</code>     | Yes         | No            | No                                             |
| View org members            | <code>org-users</code>      | Yes         | Yes           | Yes                                            |
| Assign user a role in org   | <code>set-org-role</code>   | †           | †             | No                                             |
| Remove org role from user   | <code>unset-org-role</code> | †           | †             | No                                             |
| View space members          | <code>space-users</code>    | Yes         | Yes           | Yes                                            |
| Assign user a role in space | <code>set-space-role</code> | †           | †             | No                                             |

|                             |                               |   |   |    |
|-----------------------------|-------------------------------|---|---|----|
| Remove space role from user | <code>unset-space-role</code> | ‡ | ‡ | No |
|-----------------------------|-------------------------------|---|---|----|

† Defaults to no. Yes if [feature flag](#) `user_org_creation` is set to `true`.

‡ Defaults to no. Yes if [feature flags](#) `set_roles_by_username` and `unset_roles_by_username` are set to `true`.

## Managing Orgs and Spaces Using Apps Manager

Page last updated:

This topic discusses how to view and manage orgs and spaces in Apps Manager.

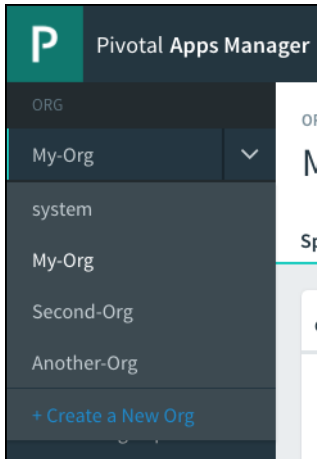
**Note:** To manage a space, you must have Space Manager permissions in that space.

To perform the following steps, you must first log in to Apps Manager with an account that has adequate permissions. See the [About Permissions](#) topic for more information.

### Manage an Org

The org page displays the spaces associated with the selected org. The left navigation of Apps Manager shows the current org.

To view spaces in a different org, use the drop-down menu to change the org.



To view the page for a particular space, click the space on the org page or on the left navigation. To create a new space, click **Add a Space** at the bottom of the org page.

| ORG                                                                                                                               | QUOTA           |                              |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------|------------------------------|
| isolated                                                                                                                          | 0 MB / 10 GB 0% | <a href="#">Usage Report</a> |
| <div> Spaces (2) Domain (1) Members (2) <b>Settings</b> </div>                                                                    |                 |                              |
| <div> <div>Org Name</div> <div>isolated</div> <div>UPDATE</div> <div>CANCEL</div> </div>                                          |                 |                              |
| <div> <div>Isolation Segment Entitlements</div> <ul style="list-style-type: none"> <li>isoseg1</li> <li>isoseg2</li> </ul> </div> |                 |                              |

To rename the current org, click the **Settings** tab. Enter the new org name in the **Org Name** section and click **Update**.

From the **Settings** tab, you can also view the spaces assigned to your isolation segment in the **Isolation Segment Entitlements** section. For more information, see [Isolation Segments](#).

### Manage a Space

The space page displays the apps, service instances, and routes associated with the selected space.

ORG

My-Org

SPACES

development

production

staging

Marketplace

Docs

Tools

SPACE

development

RUNNING

5

STOPPED

0

CRASHED

0

Apps (5)

Services (2)

Routes (2)

Settings

Apps

| Status  | Name               | Instances | Memory | Last Push   | Route                                                                                                       |
|---------|--------------------|-----------|--------|-------------|-------------------------------------------------------------------------------------------------------------|
| Running | hello-spring-cloud | 1         | 256 MB | 4 hours ago | <a href="https://docs-team-spring-app.apps.oogie-boo...">https://docs-team-spring-app.apps.oogie-boo...</a> |
| Running | my-super-app       | 1         | 20 MB  | 4 hours ago | no bound route                                                                                              |
| Running | pong-matcher       | 1         | 64 MB  | 4 hours ago | <a href="https://docs-team-broker-app.apps.oogie-boo...">https://docs-team-broker-app.apps.oogie-boo...</a> |
| Running | spring-music       | 1         | 20 MB  | 4 hours ago | no bound route                                                                                              |
| Running | the-other-app      | 1         | 20 MB  | 4 hours ago | no bound route                                                                                              |


## Apps

The **Apps** tab shows the **Status**, the **Name**, the number of **Instances**, the amount of **Memory** available, the time since the **Last Push**, and the **Route** for each app.

| Apps    |                    |           |        |             |                                                                                                             |
|---------|--------------------|-----------|--------|-------------|-------------------------------------------------------------------------------------------------------------|
| Status  | Name               | Instances | Memory | Last Push   | Route                                                                                                       |
| Running | hello-spring-cloud | 1         | 256 MB | 4 hours ago | <a href="https://docs-team-spring-app.apps.oogie-boo...">https://docs-team-spring-app.apps.oogie-boo...</a> |
| Running | my-super-app       | 1         | 20 MB  | 4 hours ago | no bound route                                                                                              |

## Services

The **Services** list shows the **Service**, the **Name**, the number of **Bound Apps**, and the **Plan** for each service instance. If you want to add a service to your space, click **Add Service**. For more information about configuring services, see the [Services Overview](#) topic.

| Services                                                                                          |               |            |                 | ADD A SERVICE |  |
|---------------------------------------------------------------------------------------------------|---------------|------------|-----------------|---------------|--|
| Service                                                                                           | Name          | Bound Apps | Plan            |               |  |
|  App Autoscaler | my-autoscaler | 0          | free - Standard |               |  |

## Routes

From the **Routes** tab, you can view and delete routes associated with your space. For each **Route**, the tab shows **Route Service** and **Bound Apps**. Refer to the [Route Services](#) topic to learn more about route services.

| Routes                                                                                                      |                  |                    |
|-------------------------------------------------------------------------------------------------------------|------------------|--------------------|
| Route                                                                                                       | Route Service    | Bound Apps         |
| <a href="https://docs-team-broker-app.apps.oogie-boogie...">docs-team-broker-app.apps.oogie-boogie...</a>   | my-service       | pong-matcher       |
| <a href="https://docs-team-spring-app.apps.oogie-boogie....">docs-team-spring-app.apps.oogie-boogie....</a> | no bound service | hello-spring-cloud |

## Settings

From the **Settings** tab, you can do the following:

- Modify the space name by entering a new name and clicking **Update**.
- View the Application Security Groups (ASGs) associated with the space in the **Security Groups** section.
- View the space's isolation segment assignment in the **Isolation Segment Assignment** section. For more information, see [Isolation Segments](#).
- Delete the space by clicking **Delete Space**.

SPACE

RUNNING

STOPPED

CRASHED

0

3

0

devspace

Apps (3)

Services (3)

Routes (3)

Members (2)

Settings

Space Name

devspace

UPDATE

CANCEL

Security Groups

A collection of egress rules that specify one or more individual protocols, ports, and destinations. [Learn more](#)

>

default\_security\_group

running, staging

Isolation Segment Assignment

devsegment


Delete Space

This will permanently delete all of the apps in this space.

DELETE SPACE

## Managing User Roles with Apps Manager

Page last updated:

 **Note:** The procedures described here are not compatible with using SAML or LDAP for user identity management. To create and manage user accounts in a SAML- or LDAP-enabled Cloud Foundry deployment, see [Adding Existing SAML or LDAP Users to a Pivotal Cloud Foundry Deployment](#).

Cloud Foundry uses role-based access control, with each role granting the permissions in either an org or an application space.

A user account can be assigned one or more roles.

The combination of these roles defines the actions a user can perform in an org and within specific app spaces in that org.

To view the actions that each role allows, see the [Organizations, Spaces, Roles, and Permissions](#) topic. For example, to assign roles to user accounts in a space, you must have Space Manager role assigned to the user in that space.

You can also modify permissions for existing users by adding or removing the roles associated with the user account. User roles are assigned on a per-space basis, so you must modify the user account for each space that you want to change.

Admins, Org Managers, and Space Managers can assign user roles with Apps Manager or with the Cloud Foundry Command Line Interface (cf CLI). For more information, see the [Users and Roles](#) section of the *Getting Started with the cf CLI* topic.

## Manage Org Roles

Valid [org roles](#) are Organization Manager and Organization Auditor.

To grant or revoke org roles, follow the steps below.

1. Log in to Apps Manager.
2. From the **Org** dropdown, select an **Org**.
3. Click the **Members** tab. Edit the roles assigned to each user by selecting or clearing the checkboxes under each user role. Apps Manager saves your changes automatically.
4. The **Members** panel displays all members of the org. Select a checkbox to grant an org role to a user, or clear a checkbox to revoke a role from a user.

## Manage App Space Roles

Valid [app space roles](#) are Space Manager, Space Developer, and Space Auditor.

To grant or revoke app space roles, do the following:

1. Go to the page for a space
2. Select the **Members** tab. The **Members** panel displays all members of the space.
3. Select a checkbox to grant an app space role to a user, or clear a checkbox to revoke a role from a user.
  - **Space Managers** can invite and manage users and enable features for a given space. Assign this role to managers or other users who need to administer the account.
  - **Space Developers** can create, delete, and manage applications and services, and have full access to all usage reports and logs. Space Developers can also edit applications, including the number of instances and memory footprint. Assign this role to app developers or other users who need to interact with applications and services.
  - **Space Auditors** have view-only access to all space information, settings, reports, and logs. Assign this role to users who need to view but not edit the application space.

## Invite New Users

**Note:** The **Enable Invitations** checkbox in the Apps Manager section of the PAS tile must be selected to invite new users.

1. On the Org dashboard, click the **Members** tab.
2. Click **Invite New Members**. The **Invite New Team Member(s)** form appears.

ORG **docs-org** QUOTA 1.62 GB / 10 GB 16% Usage Report

Space (1) Domains (2) **Members (6)** Settings

**Invite New Team Member(s)**

**Add Email Addresses**

Use commas to separate emails

**Assign Org Roles**

| Org                                 | Org Manager ⓘ            | Org Auditor ⓘ            |
|-------------------------------------|--------------------------|--------------------------|
| docs-org                            | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Select All |                          |                          |

**Assign Space Roles**

| Space ^                             | Space Manager ⓘ          | Space Developer ⓘ        | Space Auditor ⓘ          |
|-------------------------------------|--------------------------|--------------------------|--------------------------|
| docs-space                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Select All |                          |                          |                          |

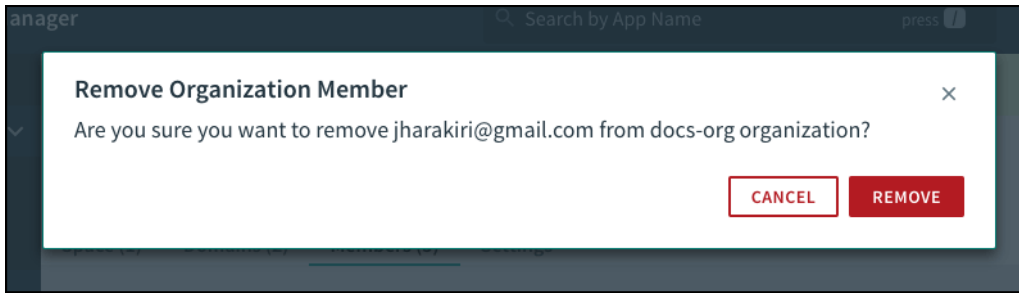
**CANCEL** **SEND INVITE**

3. In the **Add Email Addresses** text field, enter the email addresses of the users that you want to invite. Enter multiple email addresses as a comma-delimited list.
4. The **Assign Org Roles** and **Assign Space Roles** tables list the current org and available spaces with checkboxes corresponding to each possible user role. Select the checkboxes that correspond to the permissions that you want to grant to the invited users.
5. Click **Send Invite**. The Apps Manager sends an email containing an invitation link to each email address that you specified.

## Remove a User From an Org

Removing a user from org also removes them from all spaces in the org.

1. On the Org dashboard, click the **Members** tab.
2. Locate the user account that you want to remove.
3. Under the user's email address, click on the **Remove User** link. A warning dialog appears.



4. Click **Remove** to confirm user account deletion from the org.

## Remove a User From a Space

1. Go to the page for a space
2. Select the **Members** tab. The **Members** panel displays all members of the space
3. Locate the user account that you want to remove.

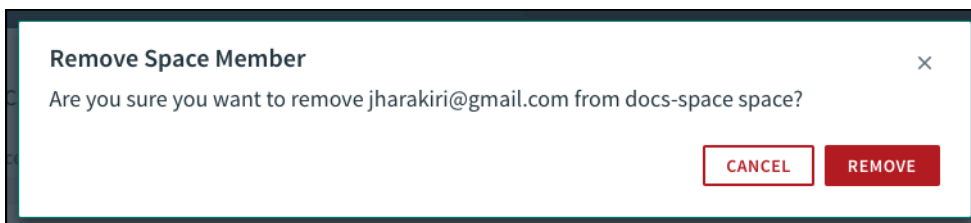
SPACE **space-0000** RUNNING 9 STOPPED 0 CRASHED 0

Apps (9) Services (7) Routes (107) **Members (301)** Settings

**Members** INVITE NEW MEMBERS

| Member                                            | Space Manager ⓘ          | Space Developer ⓘ        | Space Auditor ⓘ                     |
|---------------------------------------------------|--------------------------|--------------------------|-------------------------------------|
| admin                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            |
| space-auditor-0019<br><a href="#">Remove User</a> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| space-auditor-0003<br><a href="#">Remove User</a> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| space-auditor-0013<br><a href="#">Remove User</a> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| space-auditor-0006<br><a href="#">Remove User</a> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

4. Under the user's email address, click on the **Remove User** link. A warning dialog appears.



5. Click **Remove** to confirm user account deletion from the space.



## Managing Apps and Service Instances Using Apps Manager

Page last updated:

This topic discusses how to view and manage apps and service instances associated with a space using Apps Manager.

To perform the following steps, you must first log in to Apps Manager with an account that has adequate permissions. See the [About Permissions](#) topic for more information.

### Manage an App

From any specific app page, you can do the following to manage an app:

- Scale apps
- Bind apps to services
- Manage environment variables and routes
- View logs and usage information
- Start and stop apps
- Delete apps

APP  
**cf-nodejs**

Running

VIEW APP

Overview
Services
Route (1)
Logs
Tasks
Settings

Buildpack: N/A

Events

Last Push: 12:25 PM 02/07/18

App Summary

No recent events

Instances / Allocated

3 / 4

Memory / Allocated

0.05 / 2.63 GB

Disk / Allocated

0.10 / 1.63 GB

Processes and Instances

web

Instances

2

Memory Allocated

1 GB

Disk Allocated

512 MB

SCALE

Autoscaling

| # | CPU | Memory   | Disk     | Uptime           |
|---|-----|----------|----------|------------------|
| 0 | 0%  | 25.61 MB | 51.07 MB | 4 d 21 hr 41 min |
| 1 | 0%  | 27.83 MB | 51.07 MB | 4 d 21 hr 40 min |

worker

Instances

1

Memory Allocated

512 MB

Disk Allocated

512 MB

SCALE

| # | CPU | Memory  | Disk    | Uptime           |
|---|-----|---------|---------|------------------|
| 0 | 0%  | 0 Bytes | 0 Bytes | 4 d 21 hr 42 min |

scheduler

Instances

1

Memory Allocated

130 MB

Disk Allocated

128 MB

SCALE

## Start or Stop an App

1. To stop an app, click the stop button next to the name of the app. Click **Stop** in the pop-up to confirm.
2. To restart a stopped app, click the play button next to the name of the app.
3. To restart a running app, click the restart button next to the name of the app. Click **Restart** in the pop-up to confirm.

## Scale an App

From the app **Overview** pane, Space Developers can scale an app [manually](#) or configure [App Autoscaler](#) to scale it automatically.

### Scale an App Manually

#### Processes and Instances

web

| Instances                            | 2   | Memory Allocated | 1 GB     | Disk Allocated   | 512 MB | <b>SCALE</b> |
|--------------------------------------|-----|------------------|----------|------------------|--------|--------------|
| <input type="checkbox"/> Autoscaling |     |                  |          |                  |        |              |
| #                                    | CPU | Memory           | Disk     | Uptime           |        |              |
| 0                                    | 0%  | 6.63 MB          | 51.07 MB | 4 d 21 hr 58 min |        |              |
| 1                                    | 0%  | 27.98 MB         | 51.07 MB | 4 d 21 hr 56 min |        |              |

1. Click **Scale** to open the “Scale App” dialog.

Tasks

Settings

App Summary

Instances / Allocated  
3 / 4

Processes and Instances

web

Instances 2 Memory Allocated

# CPU

0 0%

1 0%

worker

Instances 1 Memory Allocated

Scale app

web

Instances Memory Limit Disk Limit

2 1 GB 512 MB

worker

Instances Memory Limit Disk Limit

1 512 MB 512 MB

scheduler

Instances Memory Limit Disk Limit

1 130 MB 128 MB

Usage Total

Instances Memory Limit Disk Limit

4 2.63 GB 1.63 GB

APPLY CHANGES

- Adjust the number of **Instances**, the **Memory Limit**, and the **Disk Limit** as desired.
- Click **Apply Changes**.

## Configure App Autoscaler

Processes and Instances

web

Instances 2 Memory Allocated 1 GB Disk Allocated 512 MB SCALE

Autoscaling Manage Autoscaling

# CPU Memory Disk Uptime

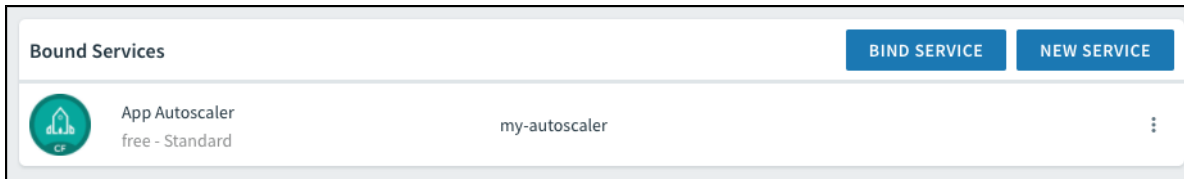
0 0% 6.63 MB 51.07 MB 4 d 21 hr 58 min

1 0% 27.98 MB 51.07 MB 4 d 21 hr 56 min

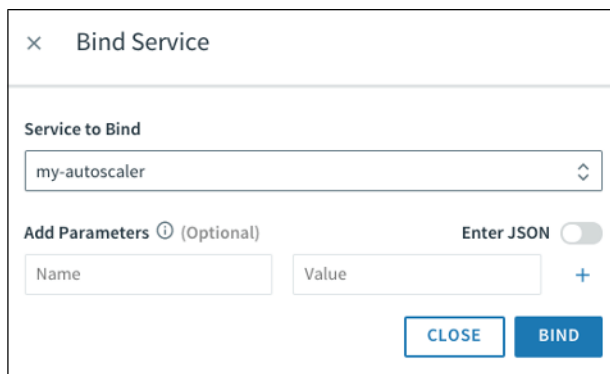
1. Use **Autoscaling** to enable App Autoscaler.
2. Click **Manage Autoscaling** to open App Autoscaler.
3. See the [Configure Autoscaling for an App](#) section of the *Scaling an Application Using Autoscaler* topic for how to configure your App Autoscaler to scale automatically based on rules or a schedule.

## Bind or Unbind a Service

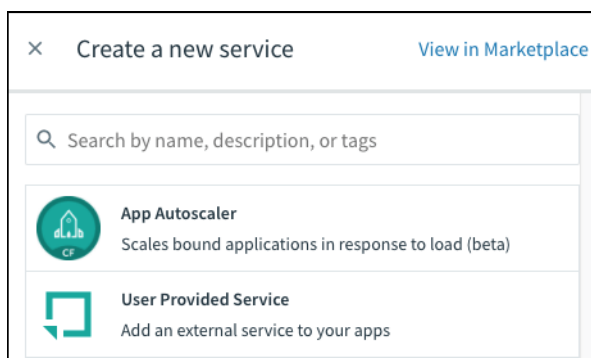
1. Click **Services**.
2. To bind your app to a service, click **Bind Service**.



3. To bind your app to an existing service instance, do the following:
  - a. Click **Bind Service**.

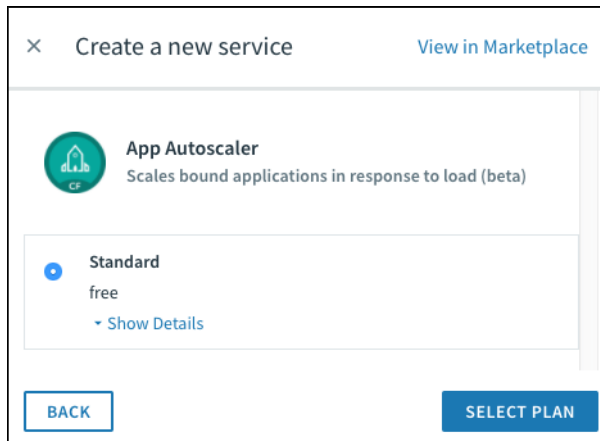


- b. Under **Service to Bind**, select the service instance from the dropdown menu.
  - c. Optionally, specify additional parameters under **Add Parameters**.
  - d. Click **Bind**.
4. To bind your app to a new service instance, do the following:
    - a. Click **New Service**.




**Note:** If you prefer to create the new service instance in the Marketplace, you can click **View in Marketplace** at any time.

- b. Click the service.



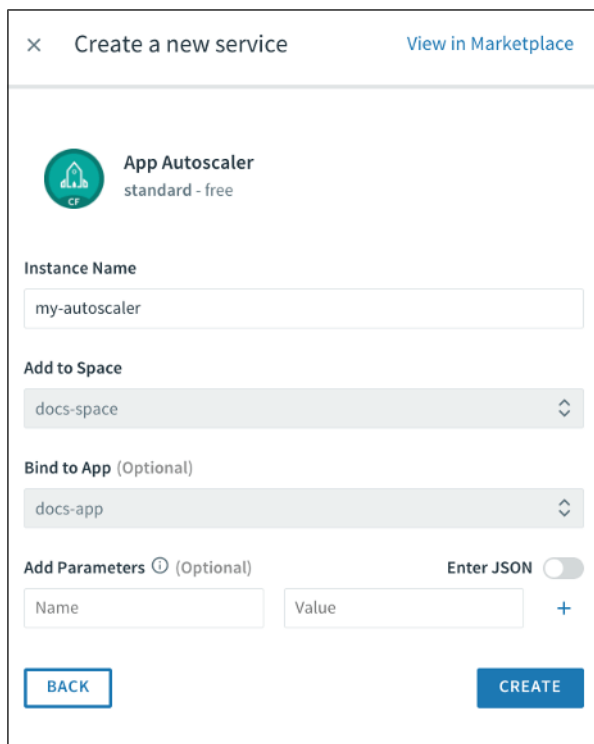
× Create a new service [View in Marketplace](#)

 **App Autoscaler**  
Scales bound applications in response to load (beta)


• **Standard**  
free  
[Show Details](#)

[BACK](#) [SELECT PLAN](#)

c. Select a plan and click **Select Plan**.



× Create a new service [View in Marketplace](#)

 **App Autoscaler**  
standard - free

**Instance Name**

**Add to Space**

**Bind to App** (Optional)

**Add Parameters** ⓘ (Optional) **Enter JSON** ☐

| Name                 | Value                |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |

[BACK](#) [CREATE](#)

d. Under **Instance Name**, enter a name for the instance.

e. Optionally, specify additional parameters under **Add Parameters**. For a list of supported configuration parameters, consult the documentation for the service.

f. Click **Create**.

5. To unbind your app from a service instance, locate the service instance in the **Bound Services** list and click the three-dot icon on the far right. Select **Unbind** from the dropdown menu.

## Map or Unmap Routes

1. Click **Routes**.


2. The page displays the routes associated with the app. To add a new route, click **Map a Route**.



**Routes** [MAP A ROUTE](#)

|                                                                                                               |                                                                                       |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <a href="http://spring-music-ageless-hydrzoate.cfapps.io">http://spring-music-ageless-hydrzoate.cfapps.io</a> |  |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|

3. Enter the route and click **Map**.

- To unmap a route, locate the route from the list and click the red . Click **Unmap** in the pop-up to confirm.

## View Logs

Logs

2016-06-15T13:45:22.512-07:00 [API] [OUT] Updated app with guid e0cb1bb7-71c6-49e2-bb6a-522991903d9f ({\"instances\"=>1})

2016-06-15T13:45:22.523-07:00 [CELL] [OUT] Exit status 0

2016-06-15T13:45:22.524-07:00 [APP] [OUT] [CONTAINER] org.apache.coyote.http11.Http11NioProtocol INFO Pausing ProtocolHandler [\"http-nio-8080\"]

2016-06-15T13:45:22.578-07:00 [APP] [OUT] [CONTAINER] org.apache.catalina.core.StandardService INFO Stopping service Catalina



2016-06-15T13:45:22.582-07:00 [APP] [OUT] [CONTAINER] lina.core.ContainerBase.[Catalina].[localhost].[/] INFO Destroying Spring FrameworkServlet 'dispatcher'


- Click **Logs** to view the logs for the app.
- Click the play button to view a live version of the logs.

## View Tasks

- Click the **Tasks** tab within Apps Manager.
- This page displays a table containing **Task ID**, **State**, **Start Time**, **Task Name**, and **Command**.

APP

pong-matcher   ● Running

VIEW APP 

Overview

Services

Route (1)

Logs

**Tasks**

Settings

Buildpack: ruby\_buildpack

Tasks

RUN TASK

| Task ID | State | Start Time | Task Name | Command |
|---------|-------|------------|-----------|---------|
|---------|-------|------------|-----------|---------|

## Run a Task

- Click **Run Task** to create a task.

Run Task 

Task Name (optional)

Task Command

RUN

CANCEL

- (Optional) Enter a **Task Name**.
- Enter the **Task Command**.
- Click **Run**.

## Enable Task Scheduling

In the **Tasks** tab, click **Enable Scheduling** to bind the PCF Scheduler service to your app. For more about the PCF Scheduler, see [Scheduling Jobs](#).

APP  
dev-app [Play] [Refresh] ● Stopped [VIEW APP](#)

Overview Services Route (1) Logs **Tasks** Settings Buildpack: N/A

**Jobs**

The scheduler service has not been enabled yet.

**ENABLE SCHEDULING**

**Tasks** **RUN TASK**

No tasks have run for this application.

## Schedule a Task

1. Navigate to the **Tasks** tab.

Overview Service (1) Route (1) Logs **Tasks** Settings Buildpack: N/A

**Jobs** **CREATE JOB**

No tasks are currently scheduled.

2. Click **Create Job** to schedule a task.

3. Enter a **Job Name**.

× Create Job

**Job Name**

**Command**

**Cron Expressions**

Value +

Syntax is described in the [docs](#). Example: 0 12 \* \* ?

**CREATE JOB**

4. Enter a **Command**.
5. Enter one or more **Cron Expressions** for your desired task schedule or schedules. See [Schedule a Job](#) for more information on cron expression syntax.
6. Click **Create Job**

## View Settings

Click the **Settings** tab. In this tab, you can do the following:

- Rename the app.
- View information about the buildpack(s), start command, stack, and health check.
- Enable the **Metrics Forwarder** service. The service allows the app to emit metrics into Loggregator. For more information about metrics forwarding, see [Emitting Metrics to Metrics Forwarder for PCF](#).
- View or add Environment Variables associated with the app.
- View the Application Security Groups (ASGs) associated with the app.
- Delete the app.

Overview
Services
Route (1)
Logs
Tasks
**Settings**

Buildpack: N/A

App Name

development

UPDATE

CANCEL

Info

Buildpack: staticfile\_buildpack, php\_buildpack  
Start Command: \$HOME/.bp/bin/start  
Stack: cflinuxfs2 (Cloud Foundry Linux-based filesystem)  
Health check type: port

Metrics Forwarder

☐

Metrics Forwarder allows applications to emit metrics into loggregator and consume those metrics from the firehose.

User Provided Environment Variables

REVEAL USER PROVIDED ENV VARS

Environment Variables

Defined by the runtime and buildpack. [Learn more](#)

REVEAL ENV VARS

Security Groups

A collection of egress rules that specify one or more individual protocols, ports, and destinations. [Learn more](#)

> default\_security\_group  
running, staging

Delete App

This will permanently delete the app and all of its data.

DELETE APP

## View Health Checks

Follow the steps below to view information about a health check you have configured for your app. For more information, see the [Using Application Health Checks](#) topic.

1. Click the **Settings** tab.
2. Under **Info**, find the **Health check type**. If your health check type is HTTP, Apps Manager also displays the **Health check endpoint**.



Health check type: http  
Health check endpoint: /

## View or Add Environment Variables

Follow the steps below to add a user-provided environment variable.

1. Click the **Settings** tab.
2. Click **Reveal User Provided Env Vars**.
3. Enter the **Name** and **Value** of the variable. Alternatively, enter your variable using the **Enter JSON** toggle.
4. Click **Save**.

User Provided Environment Variables

Enter JSON ☐

+

SAVE

CANCEL

To view all environment variables, click **Reveal Env Vars**.

Environment Variables

Defined by the runtime and buildpack. [Learn more](#)

```
{
 "staging_env_json": {},
 "running_env_json": {},
 "system_env_json": {
 "VCAP_SERVICES": {
 "fake-service-a455f60c-f166-42a5-bbab-dfadbfa0531c": [
 {
 "credentials": {
```

**Note:** Changes to environment variables, service bindings, and service unbindings require restarting the app to take effect. You can restart the app from the Apps Manager or with the Cloud Foundry Command Line Interface `cf restage` command.

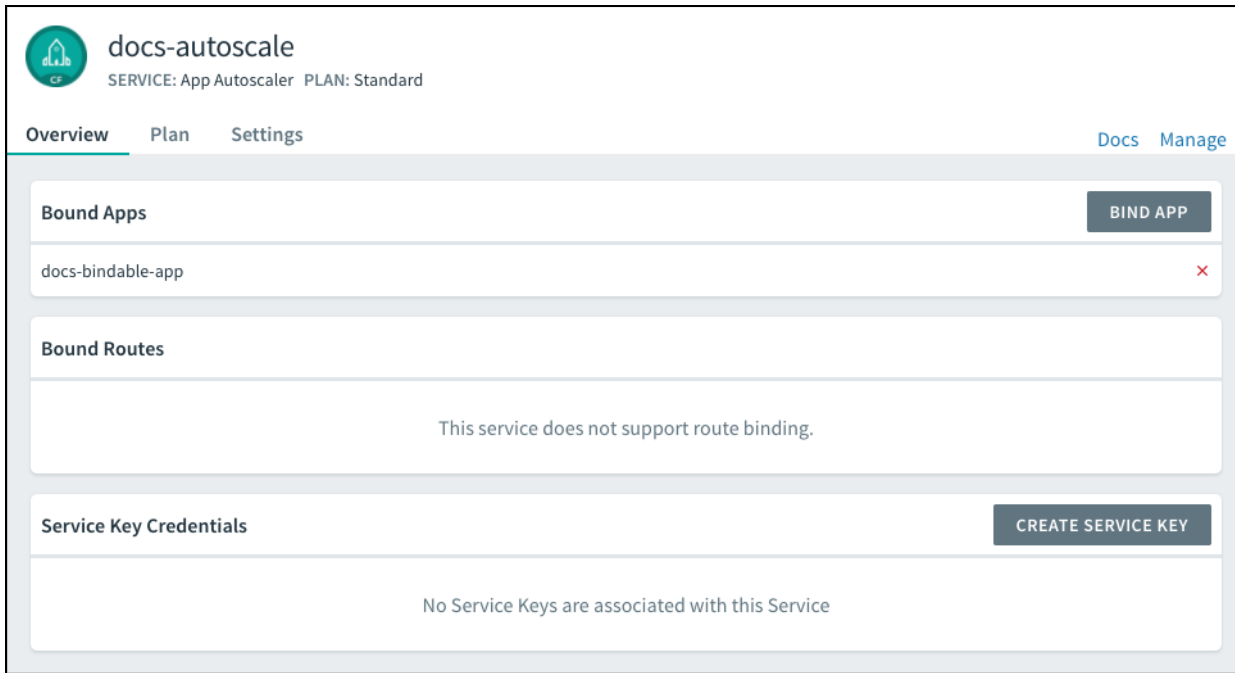
## Manage a Service Instance

From the **Services** tab on the space page, you can bind or unbind apps, bind or unbind routes, view or change your service plan, manage service keys, and rename or delete your service instance.

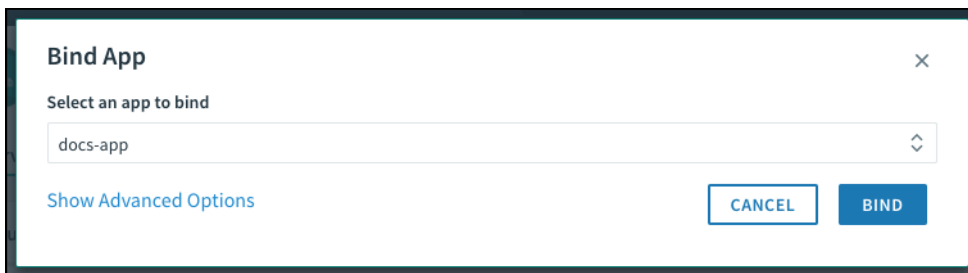
For services that use on-demand brokers, the service broker will create, update, or delete the service instance in the background and notify you when it finishes.

## Bind an App

1. From the space page **Services** tab, click the service instance you want to bind to an app.



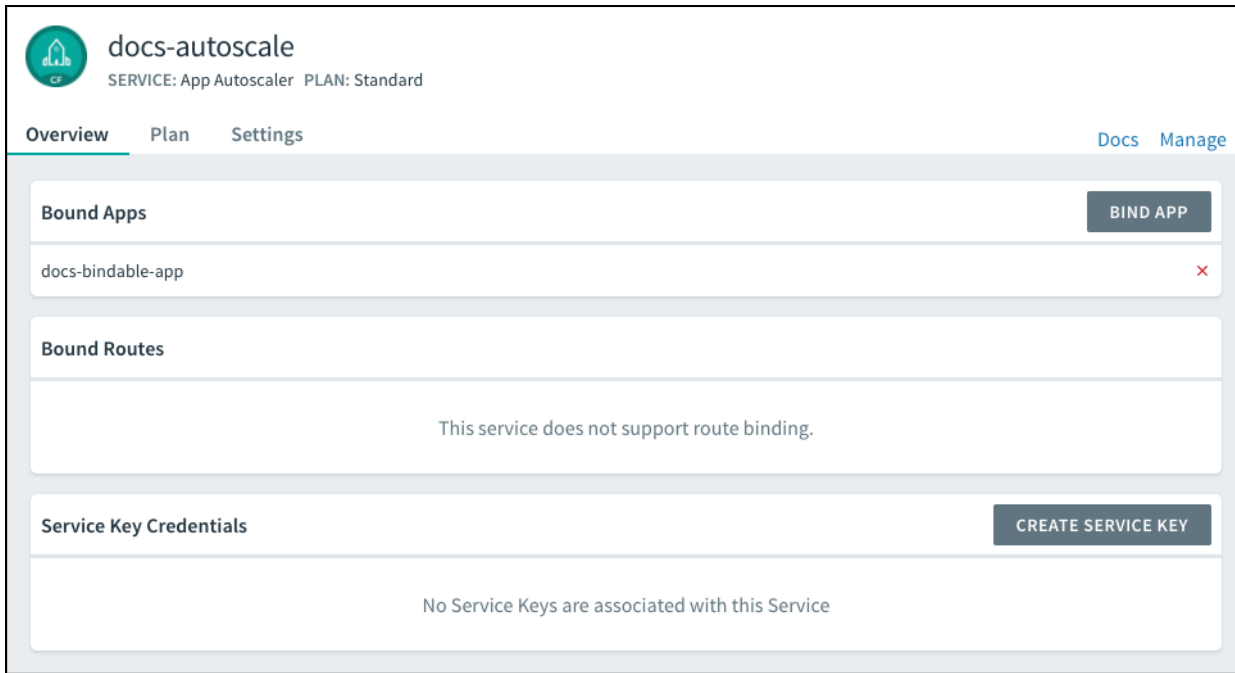
2. Click **Bind App**. A popup appears.
3. In the **Bind App** popup, select the app you want to bind to your service instance.



4. (Optional) To attach parameters to the binding, click **Show Advanced Options**. Under **Arbitrary Parameters**, enter any additional service-specific configuration.
5. Click **Bind**.

## Unbind an App

1. From the space page **Services** tab, click the service instance you want to unbind from an app.



**docs-autoscale**  
SERVICE: App Autoscaler PLAN: Standard

Overview Plan Settings Docs Manage

**Bound Apps** BIND APP

docs-bindable-app ×

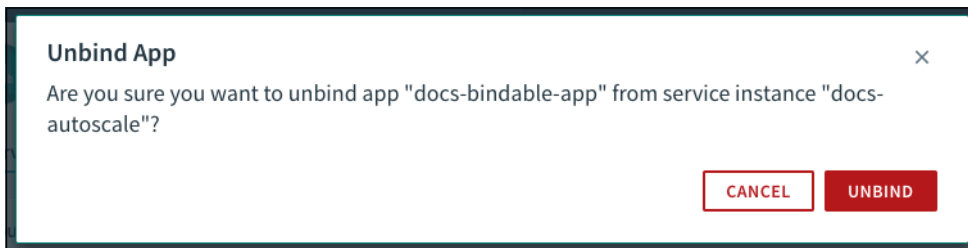
**Bound Routes**

This service does not support route binding.

**Service Key Credentials** CREATE SERVICE KEY

No Service Keys are associated with this Service

- Locate the app under **Bound Apps** and click the red **×** on the right. An **Unbind App** popup appears.



**Unbind App** ×

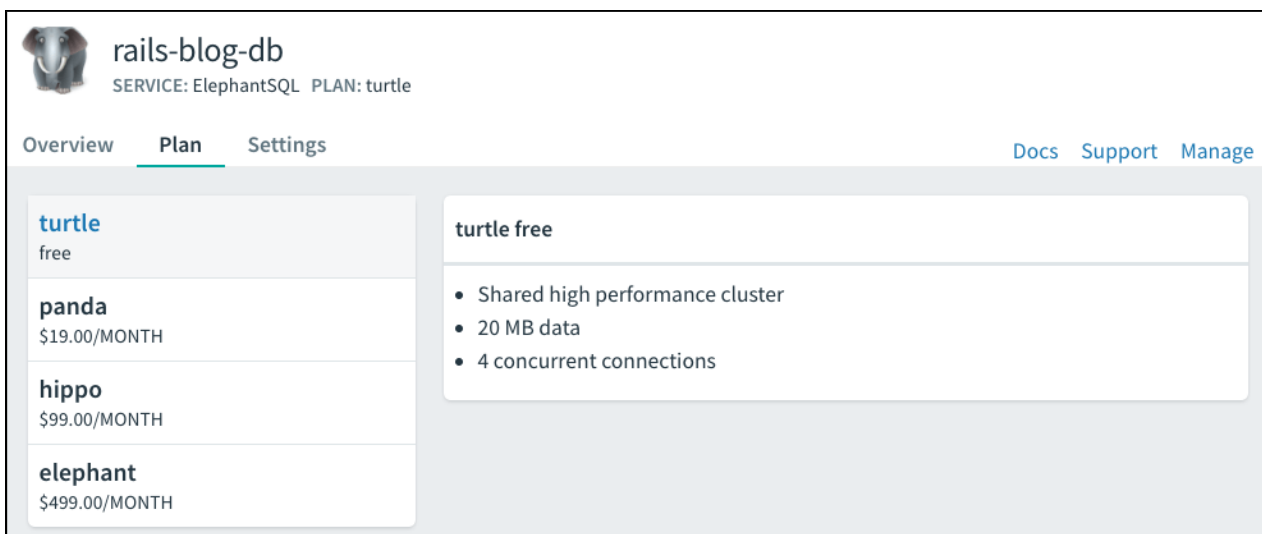
Are you sure you want to unbind app "docs-bindable-app" from service instance "docs-autoscale"?

CANCEL UNBIND

- Click **Unbind** to confirm.

## View or Change Your Service Plan

- From the space page **Services** tab, click the service instance you want to view or change the plan for.
- Click **Plan**.



**rails-blog-db**  
SERVICE: ElephantSQL PLAN: turtle

Overview Plan Settings Docs Support Manage

**turtle**  
free

**panda**  
\$19.00/MONTH

**hippo**  
\$99.00/MONTH


**elephant**  
\$499.00/MONTH

**turtle free**

- Shared high performance cluster
- 20 MB data
- 4 concurrent connections

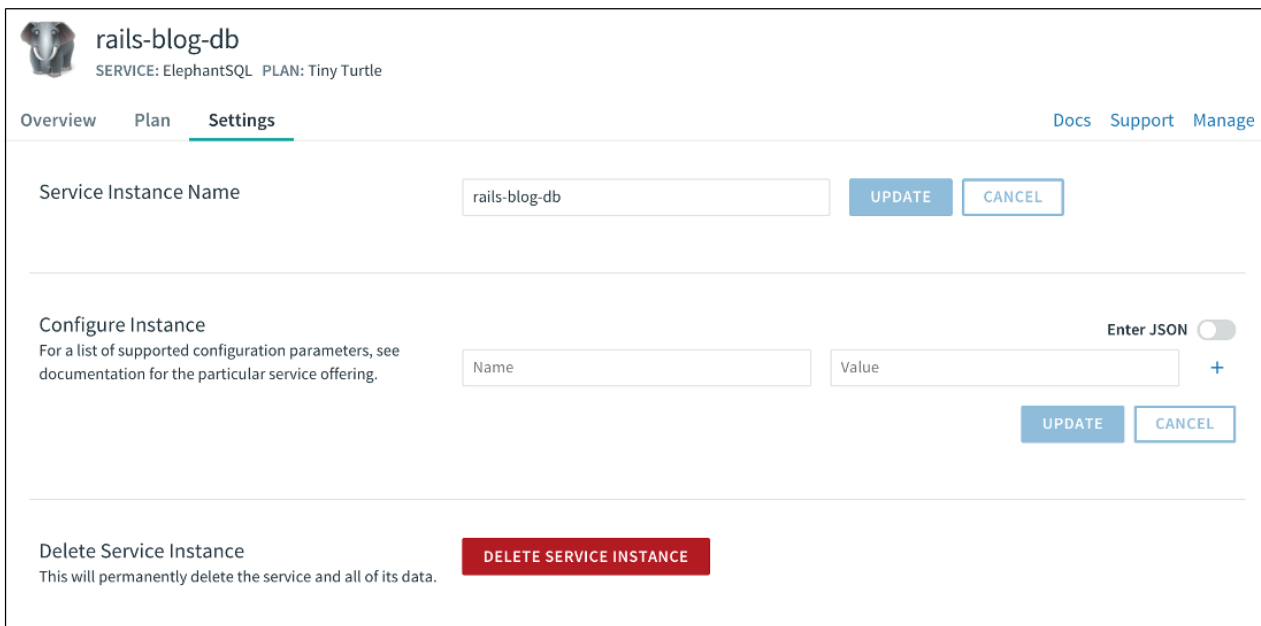
- Review your current plan information.

4. To change your plan, select a new plan from the list and click **Select This Plan** or **Upgrade Your Account**.

 **Note:** Not all services support upgrading. If your service does not support upgrading, the service plan page only displays the selected plan.

## Rename or Delete Your Service Instance


1. From the space page **Services** tab, click the service instance you want to rename or delete.
2. Click **Settings**.



The screenshot shows the 'rails-blog-db' service instance settings page. At the top, there's a header with the service name and details: 'rails-blog-db', 'SERVICE: ElephantSQL', and 'PLAN: Tiny Turtle'. Below this are tabs for 'Overview', 'Plan', and 'Settings' (which is selected). To the right of the tabs are links for 'Docs', 'Support', and 'Manage'. The main content area is divided into three sections:

- Service Instance Name:** A text input field containing 'rails-blog-db', with 'UPDATE' and 'CANCEL' buttons to its right.
- Configure Instance:** A section with a description: 'For a list of supported configuration parameters, see documentation for the particular service offering.' It includes a text input for 'Name', a text input for 'Value', and an 'Enter JSON' toggle switch (currently off). There are 'UPDATE' and 'CANCEL' buttons at the bottom right of this section.
- Delete Service Instance:** A section with a description: 'This will permanently delete the service and all of its data.' It features a prominent red 'DELETE SERVICE INSTANCE' button.

- To change the service instance name, enter the new name and click **Update**.
- To add configuration parameters to the service instance, enter the parameters in the **Name** and **Value** fields and then click **Update**. Alternatively, enter your configuration parameters using the **Enter JSON** toggle and then click **Update**.
- To delete the service instance, click **Delete Service Instance**.

 **Note:** The service broker supports creating, updating, and deleting service instances asynchronously. When the service broker completes one of these operations, a status banner appears in Apps Manager.

## Update Your User-Provided Service Instance

Follow the steps below to update an existing user-provided service instance. You can create a user-provided service instance from the Marketplace. For more information, see the [User-Provided Service Instances](#) topic.

1. Click **Configuration**. This tab only appears for user-provided service instances.

Overview
Configuration
Settings

### Configuration

Credential Parameters ⓘ (Optional)

Enter JSON ☐

NameValue-

NameValue+

Syslog Drain Url ⓘ (Optional)

Route Service Url ⓘ (Optional)

CANCEL

UPDATE SERVICE

2. Enter your **Credential Parameters**, **Syslog Drain Url**, and **Route Service Url**, and click **Update Service**.

## Manage Service Keys

On the space page, click **Services**, then click the service instance that you want to manage service keys for. This directs you to the service instance **Overview** page, where you can generate a new service key, get the credentials for a service key, and delete a service key.

mysql

SERVICE: ClearDB MySQL Database PLAN: Spark DB

Overview
Plan
Settings

DocsSupportManage

Bound Apps

BIND APP

springpong
spring-music

Bound Routes

This service does not support route binding.

Service Key Credentials

CREATE SERVICE KEY

external-app

## Generate a Service Key

Follow the steps below to generate a service key.

1. In the **Service Key Credentials** section, click **Create Service Key**.
2. Edit the **Service Key Name**.

Create Service Key

×

Service Key Name

Show Advanced Options

CANCEL

CREATE

- (Optional) Click **Show Advanced Options**. Under **Arbitrary Parameters**, enter any additional service-specific configuration in the **Name** and **Value** fields.

Create Service Key

×

Service Key Name

Arbitrary Parameters

Enter JSON ☐

Name

Value

+

Hide Advanced Options

CANCEL

CREATE

- Click **Create** to generate the service key.

## View Credentials for a Service Key

Follow the steps below to view the credentials for a service key.

- To view the credentials for a particular service instance, click the service instance name under **Service Key Credentials**. The JSON object containing the credentials appears.

Service Key Credentials

×

external-app

```
{
 "hostname": "external-app.com",
 "password": " ",
 "port": "12345"
}
```

Close

- Click **Close**.

## Delete Service Key

To delete a service key, click the red **x** next to the service instance name.

Service Key Credentials

CREATE SERVICE KEY

external-app

×

## Manage Route Services

For more information about route services, see the [Route Services](#) topic.

You can bind a [new service instance](#) to a route when creating the instance in the Marketplace, or you can manage route services for an [existing service instance](#) on the service instance page.

### Bind a New Service Instance to a Route

Follow the steps below to bind a new service instance to a route.

1. Select the service from the Marketplace.
2. Under **Bind to Route**, either bind the service instance to an existing route or click **Create Route** to create a new custom route.



**Note:** You must choose a Marketplace service compatible with route services for the **Bind to Route** field to appear.

3. Complete the remaining fields and click **Add** to create the service instance.

### Bind an Existing Service Instance to a Route

Follow the steps below to bind an existing service instance to a route.

1. On the space page, click **Services**.
2. Click the service instance that you want to manage route services for.



**Note:** If the service is not compatible with route services, the text “This service does not support route binding” appears under **Bound Routes**.

3. To bind the service instance to a route, click **Bind Route**.

### Bind Route

×

Select a route to bind

•

[select a route]

⌵

Create Custom Route

☐ Hostname

.

docs-team-domain.com

⌵

/

Path (optional)

Show Advanced Options

CANCEL

BIND

4. Select an existing route under **Select a route to bind** or enter a new route under **Create Custom Route**.

5. Click **Bind**.


To unbind a route from a service instance, click the red  next to the name of the route under **Bound Routes**.



## Scaling an Application Using App Autoscaler

This topic describes how Pivotal Cloud Foundry (PCF) users with the Space Developer role can set up and configure the App Autoscaler service in the Apps Manager UI to automatically scale apps based on rules that they set.

You can use the App Autoscaler command-line interface (CLI) plugin to configure App Autoscaler rules from the command line. For more information, see [Using the App Autoscaler CLI](#).


 **Note:** Space Managers, Space Auditors, and all Org roles do not have permission to use App Autoscaler. For help managing user roles, see [Managing User Accounts and Permissions Using the Apps Manager](#).

## App Autoscaler Overview

App Autoscaler is a marketplace service that helps control the cost of running apps while maintaining app performance.



To balance app performance and cost, Space Developers can use App Autoscaler to do the following:

- Configure rules that adjust instance counts based on metrics thresholds, such as CPU Usage
- Modify the maximum and minimum number of instances for an app, either manually or following a schedule

 **Breaking Change:** App Autoscaler relies on API endpoints from Loggregator's Log Cache. If you disable Log Cache, App Autoscaler will fail. For more information about Log Cache, see [Loggregator Introduces Log Cache](#).

## Set Up App Autoscaler

To use App Autoscaler, you must create an instance of the App Autoscaler service and bind it to any app you want to autoscale. You can do this using either the Apps Manager or from the Cloud Foundry Command Line Interface (cf CLI):

- **Apps Manager:**
  1. [Create an instance of the service](#) .
  2. [Bind the service to an app](#) .
- **cf CLI:**
  1. [Create an instance of the service](#).
  2. [Bind the service to an app](#).

To enable App Autoscaler for the app, do the following:

1. In Apps Manager, select an app from the space in which you created the App Autoscaler service.
2. Under **Processes and Instances**, enable **Autoscaling**.

| Processes and Instances                         |     |                  |          |                                             |
|-------------------------------------------------|-----|------------------|----------|---------------------------------------------|
| web                                             |     |                  |          |                                             |
| Instances                                       | 2   | Memory Allocated | 1 GB     | Disk Allocated 512 MB <a href="#">SCALE</a> |
| <input checked="" type="checkbox"/> Autoscaling |     |                  |          | <a href="#">Manage Autoscaling</a>          |
| #                                               | CPU | Memory           | Disk     | Uptime                                      |
| 0                                               | 0%  | 6.63 MB          | 51.07 MB | 4 d 21 hr 58 min                            |
| 1                                               | 0%  | 27.98 MB         | 51.07 MB | 4 d 21 hr 56 min                            |

- Click [Manage Autoscaling](#) to configure instance limits, scaling rules, and scheduled limit changes for the app. For more information, see [Configure Autoscaling for an App](#).

×

Manage Autoscaling

[Download Autoscaler CLI](#)

**INSTANCE LIMITS**  
 Currently in use: 2

Minimum  Maximum  [APPLY CHANGES](#)

**SCALING RULES** [EDIT](#)

| Metric          | Low | High |
|-----------------|-----|------|
| CPU Utilization | 20% | 80%  |

**SCHEDULED LIMITS** [EDIT](#)

Next: Mon June 11th, 2018 3:12:00 PM

**EVENT HISTORY**

Most Recent: Mon June 4, 2018 at 3:12 PM  
 Rule Applied: Scaling Limits set to 2 to 5 instances  
[VIEW MORE](#)

## Manual Scaling Overrides Autoscaler

If you manually scale an app bound to an App Autoscaler service instance, the App Autoscaler instance automatically unbinds from that app, and the app scales to the manual setting. For more information, see [Managing Apps and Service Instances Using Apps Manager](#).

## Configure Autoscaling for an App

App Autoscaler keeps instance counts within an allowable range defined by minimum and maximum values, or *instance limits*.

Follow the procedures in the sections below to set any of the following:

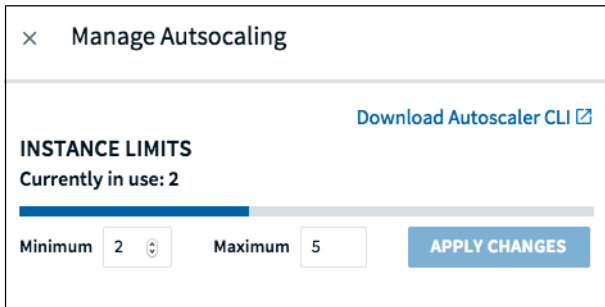
- [Instance Limits](#)
- [Scaling Rules](#)
- [Scheduled Limit Changes](#)

## Instance Limits

Follow these steps to manually modify instance limits:

 **Note:** You can also schedule changes to your instance limits for a specific date and time. For more information, see [Scheduled Limit Changes](#).

1. In Apps Manager, navigate to the **Overview** page for your app and click **Manage Autoscaling** under **Processes and Instances**.
2. In the **Instance Limits** section, set values for **Minimum** and **Maximum**.



3. Click **Apply Changes**.

## Scaling Rules

To keep your apps available without wasting resources, App Autoscaler increments or decrements instance counts based on how current metrics compare with configurable minimum and maximum thresholds.

### How App Autoscaler Determines When to Scale

Every 35 seconds, App Autoscaler makes a decision about whether to scale up, scale down, or keep the same number of instances. To make a scaling decision, App Autoscaler averages the values of a given metric for the most recent 120 seconds.

App Autoscaler scales apps as follows:

- Increment by one instance when any metric exceeds its maximum threshold
- Decrement by one instance only when all metrics fall below their minimum thresholds

For example, an app may have a maximum threshold of 200 milliseconds and a minimum threshold of 80 milliseconds for an HTTP latency metric. If HTTP latency averages 300 milliseconds over the past 120 seconds, App Autoscaler scales the app up one instance. If HTTP latency then averages 70 milliseconds over the next 120 second window and the app's other scaling metrics also fall below their minimum thresholds, App Autoscaler scales the app down one instance.

You can also set a maximum and minimum number of instances. For example, if an app exceeds the maximum threshold of a given metric, but the number of instances is already at the maximum number of allowed instances, App Autoscaler does not scale up the app. For more information about setting a maximum and minimum number of instances, see [Instance Limits](#).

### Scaling Rule Metrics

The table below lists the metrics that you can base App Autoscaler rules on:

| Metric                       | Description                                                                                                                                                                                                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Utilization              | Average CPU percentage for all instances of the app.                                                                                                                                                       |
| Container Memory Utilization | Average memory percentage for all instances of the app.                                                                                                                                                    |
| HTTP Throughput              | Total HTTP requests per second (divided by the total number of app instances).                                                                                                                             |
| HTTP Latency                 | Average latency of apps response to HTTP requests. This does not include Gorouter processing time or other network latency.<br>Average is calculated on the middle 99% or middle 95% of all HTTP requests. |

RabbitMQ Depth | The queue length of the specified queue.

## Add a Scaling Rule

1. In the **Manage Autoscaling** pane, click **Edit** next to **Scaling Rules**. The **Edit Scaling Rules** pane appears.
2. Click **Add Rule**.
3. In the **Select type** dropdown, select the metric for the new scaling rule.

4. Set the minimum and maximum thresholds for the metric using the table in the [Scaling Rule Metrics](#) section above as a guide.
5. Select or fill in any other fields that appear under the threshold fields:
  - If you are adding an **HTTP Latency** rule, configure **Percent of traffic to apply**.
  - If you are adding a **RabbitMQ** depth rule, provide the name of the queue to measure.
6. Click **Save**.

## Delete a Scaling Rule

1. Click the × icon next to the rule you want to delete.
2. Click **Save**.

## Scheduled Limit Changes

Because app demand often follows a weekly, daily, or hourly schedule, you can schedule App Autoscaler to change the allowable instance range to track expected surges or quiet periods.

### Create or Modify a Scheduled Limit Change

1. Click **Edit** next to **Scheduled Limits**.
2. Click **Add New** to add a new scheduled limit or select an existing entry to modify by clicking **EDIT** next to the entry.
3. Edit the following values:
  - **Date** and **Time (local)**: Set the date and time of the change.
  - **Repeat (Optional)**: Set the day of the week for which you want to repeat the change.
  - **Min** and **Max**: Set the allowable range within which App Autoscaler can change the instance count for an app.

< Scheduled Limit Changes: rails-docs-sample

### Configure

Date
Time (local)

June 4 2018 4 32 PM

Repeat (Optional)
Min
Max

☐ Su ☐ Mo ☐ Tu ☐ We ☐ Th ☐ Fr ☐ Sa

SAVE

### Scheduled

ADD NEW

| Date         | Time    | Repeat | Min | Max |        |
|--------------|---------|--------|-----|-----|--------|
| Jun 11, 2018 | 3:12 PM | Mo     | 2   | 5   | EDIT X |

4. Click **Save**.

To delete an existing entry, click the x icon next to the entry you want to delete.

## Example: Scale Down for the Weekend

To schedule an app to scale down for a weekend, you can enter two rules as follows:

1. Scale down to a single instance on Friday evening:

- o **Date and Time (local):** Dec , 2 , 2018 and 7:00 PM
- o **Repeat (Optional):** Fr
- o **Min and Max:** 1 and 1

2. Increase instances to between 3 and 5 on Monday morning:

- o **Date and Time (local):** Dec , 5 , 2018 and 7:00 AM
- o **Repeat (Optional):** M
- o **Min and Max:** 3 and 5

## App Autoscaler Events and Notifications

App Autoscaler logs all autoscaling events.

### View Event History

To view all autoscaling events in the past 24 hours, click **View More** in the **Event History** section of the **Manage Autoscaling** pane.

### EVENT HISTORY

Most Recent:
Mon June 4, 2018 at 3:12 PM

Rule Applied: Scaling Limits set to 2 to 5 instances

VIEW MORE

### Manage App Autoscaler Notifications

Autoscaler emails or texts its event notifications to all space users by default.

To subscribe or unsubscribe from autoscaling event notifications, do the following:

1. Navigate to the **Manage Notifications** page of PCF.



**Note:** If installed, Notifications Management should be available at <https://notifications-ui.YOUR-SYSTEM-DOMAIN/preferences>.

2. Choose which notifications you want to receive from App Autoscaler:

## Manage Notifications

You will receive email notifications from checked items

- ☒ Cloud Foundry Autoscaling Service
  - ☒ Scaling Down
  - ☒ Manual Scaling Detected
  - ☒ Maximum Instance Limit Reached
  - ☒ Quota Limit Reached
  - ☒ Scaling Up

## Using the App Autoscaler CLI

This topic explains how to use the App Autoscaler command-line interface (CLI).

The App Autoscaler automatically scales Cloud Foundry apps in response to demand. The App Autoscaler CLI lets you control the App Autoscaler from your local command line by extending the Cloud Foundry command-line interface (cf CLI).

## Install the App Autoscaler CLI Plugin

Before you can run App Autoscaler CLI commands on your local machine, you must install the App Autoscaler CLI plugin.

To install the plugin, do the following:

1. Download the plugin from [Pivotal Network](#).



**Note:** Ensure that you download the App Autoscaler CLI plugin v2.0 or later. In addition, the plugin requires Pivotal Application Service v2.2 or later..

2. To install the App Autoscaler CLI plugin, run the following command:

```
cf install-plugin LOCATION-OF-PLUGIN
```

Where `LOCATION-OF-PLUGIN` is the path to the binary file you downloaded from Pivotal Network. For example:

```
$ cf install-plugin ~/Downloads/autoscaler-for-pcf-cliplugin-macosx64-binary-2.0.91
```

For more information about installing cf CLI plugins, see [Installing a Plugin](#).

## View Apps

Run `cf autoscaling-apps` to view all the apps that are bound to an autoscaler service instance in a space, their instance limits, and whether or not they are enabled.

```
$ cf autoscaling-apps
```

```
Presenting autoscaler apps in org my-org / my-space autoscaling as user
Name Guid Enabled Min Instances Max Instances
test-app guid true 1 4
test-app-2 guid-2 false 10 40
OK
```

## Enable Autoscaling

Run `cf enable-autoscaling APP-NAME` to enable autoscaling on your app. Replace `APP-NAME` with the name of your app.

```
$ cf enable-autoscaling test-app-2
```

```
Enabled autoscaling for app test-app-2 for org my-org / my-space testing as admin
OK
```

## Disable Autoscaling

Run `cf disable-autoscaling APP-NAME` to disable autoscaling on your app. Replace `APP-NAME` with the name of your app.

```
$ cf disable-autoscaling test-app
```

```
Disabled autoscaling for app test-app for org my-org / my-space testing as admin
OK
```

## Update Instance Limits

Run `cf update-autoscaling-limits APP-NAME MIN-INSTANCE-LIMIT MAX-INSTANCE-LIMIT` to update the upper and lower app instance limits. The App Autoscaler will not attempt to scale beyond these limits. Replace `APP-NAME` with the name of your app. Replace `MIN-INSTANCE-LIMIT` with the minimum number of apps, and `MAX-INSTANCE-LIMIT` with the maximum number of apps.

```
$ cf update-autoscaling-limits test-app 10 40
```

```
Updated autoscaling instance limits for app test-app for org my-org / my-space testing as admin
OK
```

## View Rules

Run `cf autoscaling-rules APP-NAME` to view the rules that the App Autoscaler uses to determine when to scale your app. Replace `APP-NAME` with the name of your app.

```
$ cf autoscaling-rules test-app
```

```
Presenting autoscaler rules for app test-app for org my-org / my-space autoscaling as user
Rule Guid Rule Type Rule Sub Type Min Threshold Max Threshold
guid cpu 10 20
guid-2 http_throughput 20 30
OK
```

## Create a Rule

Run `create-autoscaling-rule APP-NAME RULE-TYPE MIN-THRESHOLD MAX-THRESHOLD [--subtype SUBTYPE] [--metric METRIC] [--comparison-metric COMPARISON-METRIC]`

to create a new autoscaling rule.

Replace the placeholders as follows:

- `APP-NAME` is the name of your app.
- `RULE-TYPE` is the type of your scaling rule.
- `MIN-THRESHOLD` is the minimum threshold for the metric.
- `MAX-THRESHOLD` is the maximum threshold for the metric.

You can use the following command options:

- `--metric`, `-m` is the metric for a Custom rule.
- `--comparison-metric`, `-c` is the comparison metric for a Compare rule.
- `--subtype`, `-s` is the rule subtype.

For example:

```
$ cf create-autoscaling-rule test-app http_latency 10 20 -s avg_99th
```

```
Created autoscaler rule for app test-app for org my-org / space my-space as user
Rule Guid Rule Type Rule Sub Type Min Threshold Max Threshold
guid-3 http_latency avg_99th 10 20
```



```
$ cf create-autoscaling-rule test-app custom 9380 9381 --metric jvm.classes.loaded
Created autoscaler rule for app test-app in org my-org / space my-space as user
OK
Guid Type Metric Sub Type Min Threshold Max Threshold
guid-7 custom jvm.classes.loaded 9380.00 9381.00
```

```
$ cf create-autoscaling-rule test-app compare .79 .8 --metric jvm.memory.used --comparison-metric jvm.memory.max
Created autoscaler rule for app test-app in org my-org / space my-space as user
OK
Guid Type Metric Sub Type Min Threshold Max Threshold
guid-8 compare jvm.memory.used / jvm.memory.max 0.79 0.80
```

## Valid Rule Types and Subtypes

For a list of valid types and subtypes, see the following:

- type `CPU`
- type `memory`
- type `http_throughput`
- type `http_latency`
- type `rabbit-mq`
  - `queue_name` `YOUR-QUEUE-NAME`
- type `custom`
  - `metric` `METRIC-NAME`
- type `compare`
  - `metric` `METRIC-NAME`
  - `comparison_metric` `METRIC-NAME`

## Delete a Rule

Run `delete-autoscaling-rule APP-NAME RULE-GUID [--force]` to delete a single autoscaling rule. Replace `APP-NAME` with the name of your app, and replace `RULE-GUID` with the GUID.

```
$ cf delete-autoscaling-rule test-app guid-2

Really delete rule guid-2 for app test-app?> [yN]:y
Deleted rule guid-2 for autoscaler app test-app for org my-org / space my-space as admin
OK
```

## Delete All Rules

Run `delete-autoscaling-rules APP-NAME [--force]` to delete all autoscaling rules. Replace `APP-NAME` with the name of your app.

```
$ cf delete-autoscaling-rules test-app

Really delete ALL rules for app test-app?> [yN]:y
Deleted rules for autoscaler app test-app for org my-org / space my-space as admin
OK
```

## View Autoscaling Events

Run `cf autoscaling-events APP-NAME` to view recent events related to autoscaling for your app. Replace `APP-NAME` with the name of your app.

```
$ cf autoscaling-events test-app
```

| Time                 | Description                                                                        |
|----------------------|------------------------------------------------------------------------------------|
| 2032-01-01T00:00:00Z | Scaled up from 3 to 4 instances. Current cpu of 20 is above upper threshold of 10. |

## View Autoscaler Scheduled Instance Limit Changes

Run `cf autoscaling-sls APP-NAME` to view all scheduled instance limit changes. Replace `APP-NAME` with the name of your app.

For example:

```
$ cf autoscaling-sls test-app
```

| Guid   | First Execution      | Min Instances | Max Instances | Recurrence     |
|--------|----------------------|---------------|---------------|----------------|
| guid-5 | 2018-06-12T22:00:00Z | 0             | 1             | Mo,Tu,We,Th,Fr |

## Create Autoscaler Scheduled Instance Limit Change

Run `create-autoscaling-slc APP-NAME DATE-TIME MIN-INSTANCES MAX-INSTANCES [--recurrence RECURRENCE]` to create a new scheduled instance limit change.

Replace the placeholders as follows:

- `APP-NAME` is the name of your app.
- `DATE-TIME` is the date and time of the change.
- `MIN-INSTANCES` and `MAX-INSTANCES` are the minimum and maximum values of the range within which App Autoscaler can change the instance count for an app.
- `RECURRENCE` (optional) is the day of the week for which you want to repeat the change.

For example:

```
$ cf create-autoscaling-slc test-app 2018-06-14T15:00:00Z 1 2 --recurrence Sa
```

```
Created scheduled autoscaler instance limit change for app test-app in org my-org / space my-space as user
OK
Guid First Execution Min Instances Max Instances Recurrence
guid-6 2018-06-14T15:00:00Z 1 2 Sa
```

## Delete Autoscaler Scheduled Instance Limit Change

Run `delete-autoscaling-slc APP-NAME SLC-GUID [--force]` to delete a scheduled instance limit change. Replace `APP-NAME` with the name of your app and `SLC-GUID` with the GUID of your scheduled instance limit change.

For example:

```
$ cf delete-autoscaling-slc test-app slc-guid
```

```
Really delete scheduled limit change slc-guid for app test-app?> [yN]:y
Deleted scheduled limit change slc-guid for app test-app in org my-org / space my-space as user
OK
```

## Configure with a Manifest

Run `configure-autoscaling APP-NAME MANIFEST-FILE-PATH` to use a service manifest to configure your rules, add instance limits, and set scheduled limit

changes at the same time. Replace `APP-NAME` with the name of your app, and replace `MANIFEST-FILE-PATH` with the path and name of your Autoscaler manifest.

An example manifest:

```

instance_limits:
 min: 1
 max: 2
rules:
- rule_type: "http_latency"
 rule_sub_type: "avg_99th"
 threshold:
 min: 10
 max: 20
scheduled_limit_changes:
- recurrence: 10
 executes_at: "2032-01-01T00:00:00Z"
 instance_limits:
 min: 10
 max: 20
```

```
$ cf configure-autoscaling test-app autoscaler-manifest.yml
```

```
Setting autoscaler settings for app test-app for org my-org / space my-space as user
OK
```

A `rules` block must be present in your Autoscaler manifest. If your app does not require any rules changes, include an empty block:

```

instance_limits:
 min: 1
 max: 1
rules: []
scheduled_limit_changes:
- recurrence: 365
 executes_at: "2032-01-01T00:00:00Z"
 instance_limits:
 min: 0
 max: 0
```

A `scheduled_limit_changes` block must be present in your Autoscaler manifest. If your app does not require any scheduled instance limit changes, include an empty block:

```

instance_limits:
 min: 1
 max: 2
rules:
- rule_type: "http_latency"
 rule_sub_type: "avg_99th"
 threshold:
 min: 10
 max: 20
scheduled_limit_changes: []
```

## App Autoscaler CLI Known Issues

The App Autoscaler CLI has the following known issues:

- The CLI returns an error message if you have more than one instance of the App Autoscaler service running in the same space.
  - To prevent this error, delete all but one App Autoscaler service instance from any space that the App Autoscaler service runs in.
- The CLI may output odd characters in Windows shells that do not support text color.
  - To prevent this error, run `SET CF_COLOR=false` in your Windows shell pane before you run App Autoscaler CLI commands.
  - Note that some Windows shells do not support the `CF_COLOR` setting.

## Viewing ASGs in Apps Manager

Page last updated:

### About ASGs

Application Security Groups (ASGs) are a collections of egress rules that specify the protocols, ports, and IP address ranges where app or task instances send traffic. The platform sets up rules to filter and log outbound network traffic from app and task instances. ASGs apply to both buildpack-based and Docker-based apps and tasks.

When apps or tasks begin staging, they need traffic rules permissive enough to allow them to pull resources from the network. After an app or task is running, the traffic rules can be more restrictive and secure. To distinguish between these two security requirements, administrators can define one ASG for app and task staging, and another for app and task runtime. For more information about staging and running apps, see [Application Container Lifecycle](#).

To provide granular control when securing a deployment, an administrator can assign ASGs to apply to all app and task instances for the entire deployment, or assign ASGs to spaces to apply only to apps and tasks in a particular space.

Only admin users can create and modify ASGs. For information about creating and configuring ASGs, see [Application Security Groups](#).

### Displaying ASGs for a Space

To view the ASGs associated with a space, perform the following steps.

1. Log in to Apps Manager.
2. From the **Org** dropdown, select the **Org** that contains the space you want to view.
3. Select the **Space** you want to view.
4. Click on the **Settings** tab.
5. In the **Security Groups** section, Apps Manager displays ASGs associated with the selected space.
6. Click on an ASG to expand its egress rules.

#### Security Groups

A collection of egress rules that specify one or more individual protocols, ports, and destinations. [Learn more](#)

public\_networks

running, staging

destination: 0.0.0.0-9.255.255.255

protocol: all

destination: 11.0.0.0-169.253.255.255

protocol: all

destination: 169.255.0.0-172.15.255.255

protocol: all

destination: 172.32.0.0-192.167.255.255

protocol: all

destination: 192.169.0.0-255.255.255.255

protocol: all

dns

running, staging

sshfs-service

running

p-mysql

running



## Configuring Spring Boot Actuator Endpoints for Apps Manager

Page last updated:

The Apps Manager UI supports several production-ready endpoints from Spring Boot Actuator. This topic describes the Actuator endpoints and how you can configure your app to display data from the endpoints in Apps Manager.

For more information about Spring Boot Actuator, see the [Spring Boot Actuator documentation](#).

 **Note:** This feature requires Spring Boot v1.5 or later.

### Overview

The Apps Manager integration with Spring Boot does not use the standard Spring Boot Actuators. Instead, it uses a specific set of actuators that are secured using the Space Developer role for the space that the application runs in. Authentication and authorization are automatically delegated to the [Cloud Controller](#) and the [User Account and Authentication](#) server without any configuration from the user.

By default, actuators are secure and cannot be accessed without explicit configuration by the user, even if [Spring Security](#) is not included. This allows users to take advantage of the Spring Boot Apps Manager integration without accidentally exposing their actuators without security.

### Actuator Endpoints

The table below describes the Spring Boot Actuator endpoints supported by Apps Manager. To integrate these endpoints with Apps Manager, you must first [Activate Spring Boot Actuator for Your App](#).

| Endpoint               | About                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/info</code>     | <ul style="list-style-type: none"> <li><b>Description:</b> Exposes details about app environment, git, and build. To send build and Git information to this endpoint, see <a href="#">Configure the Info Actuator</a>.</li> <li><b>How to use in Apps Man:</b> See <a href="#">View Build and Git Information for Your App</a>.</li> </ul>                                                                                                                                                                                                                       |
| <code>/health</code>   | <ul style="list-style-type: none"> <li><b>Description:</b> Shows health status or detailed health information over a secure connection. Spring Boot Actuator includes the auto-configured health indicators specified in the <a href="#">Auto-configured HealthIndicators</a> section of the Spring Boot documentation. If you want to write custom health indicators, see the <a href="#">Writing custom HealthIndicators</a> section of the Spring Boot documentation.</li> <li><b>How to use in Apps Man:</b> See <a href="#">View App Health</a>.</li> </ul> |
| <code>/loggers</code>  | <ul style="list-style-type: none"> <li><b>Description:</b> Lists and allows modification of the levels of the loggers in an app.</li> <li><b>How to use in Apps Man:</b> See <a href="#">Manage Log Levels</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| <code>/dump</code>     | <ul style="list-style-type: none"> <li><b>Description:</b> Generates a thread dump.</li> <li><b>How to use in Apps Man:</b> See <a href="#">View Thread Dump</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>/trace</code>    | <ul style="list-style-type: none"> <li><b>Description:</b> Displays trace information from your app for each of the last 100 HTTP requests. For more information, see the <a href="#">Tracing</a> section of the Spring Boot documentation.</li> <li><b>How to use in Apps Man:</b> See <a href="#">View Request Traces</a>.</li> </ul>                                                                                                                                                                                                                          |
| <code>/heapdump</code> | <ul style="list-style-type: none"> <li><b>Description:</b> Generates a heap dump and provides a compressed file containing the results.</li> <li><b>How to use in Apps Man:</b> See <a href="#">Download Heap Dump</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                               |
| <code>/mappings</code> | <ul style="list-style-type: none"> <li><b>Description:</b> Displays the endpoints an app serves and other related details.</li> <li><b>How to use in Apps Man:</b> See <a href="#">View Mappings</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                 |

### Activate Spring Boot Actuator for Your App

You must add a `spring-boot-starter-actuator` dependency to your app project for the production-ready HTTP endpoints to return values. For more information, see the [Enabling production-ready features](#) section of the Spring Boot documentation.

1. Follow the instructions below that correspond to your project type.

- **Maven:** If you use Maven, add the following to your project:

```
<dependencies>
 <dependency>
 <groupId>org.springframework.boot</groupId>
 <artifactId>spring-boot-starter-actuator</artifactId>
 </dependency>
</dependencies>
```

- **Gradle:** If you use Gradle, add the following to your project:

```
dependencies {
 compile("org.springframework.boot:spring-boot-starter-actuator")
}
```

2. If you use self-signed certificates in your PCF deployment for UAA or the Cloud Controller, specify in your `application.properties` file to skip SSL validation:

```
management.cloudfoundry.skip-ssl-validation=true
```

See [Cloud Foundry support](#) in the Spring Boot Actuator documentation for more information.

## Configure the Info Actuator

The `/info` endpoint provides information about the project build for your app, as well as its git details.

### Add Build Information

To add build information to the `/info` endpoint, follow the instructions below that correspond to your project type.

#### Maven

Add the following to your app project:

```
<build>
 <plugins>
 <plugin>
 <groupId>org.springframework.boot</groupId>
 <artifactId>spring-boot-maven-plugin</artifactId>
 <version>1.4.2.RELEASE</version>
 <executions>
 <execution>
 <goals>
 <goal>build-info</goal>
 </goals>
 </execution>
 </executions>
 </plugin>
</plugins>
</build>
```

#### Gradle

Add the following to your app project:

```
springBoot {
 buildInfo()
}
```

## Add Git Information

To add git information to the `/info` endpoint, follow these instructions:

1. Add the following property to your `application.properties` file:

```
management.info.git.mode=full
```

2. Follow the instructions below that correspond to your project type.

### Maven

Add the following plugin to your project:

```
<build>
 <plugins>
 <plugin>
 <groupId>pl.project13.maven</groupId>
 <artifactId>git-commit-id-plugin</artifactId>
 </plugin>
 </plugins>
</build>
```

### Gradle

Add the following plugin to your project:

```
plugins {
 id "com.gorylenko.gradle-git-properties" version "1.4.17"
}
```



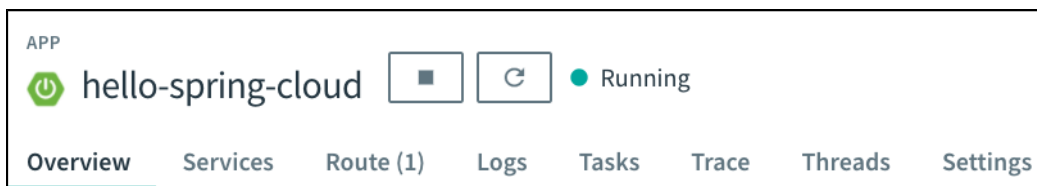
## Using Spring Boot Actuators with Apps Manager

This document describes how to view and manage app information from Spring Boot Actuator in Apps Manager.

### Prerequisites



The Apps Manager integration with Spring Boot Actuator requires the following:

- A PCF user with the `SpaceDeveloper` role. See [App Space Roles](#).
  - Spring Boot v1.5 or later.
  - Completing the procedures in [Configure Spring Boot Actuator Endpoints for Apps Manager](#).
- After you configure your app, Apps Manager displays the Spring Boot logo next to the name of your app on the app page:



### View Build and Git Information for Your App

To view the data that your app sends to its `/info` Actuator endpoint, select the **Settings** tab:

|                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| App Name                                                                                                                                           | <input type="text" value="hello-spring-cloud"/> <input type="button" value="UPDATE"/> <input type="button" value="CANCEL"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Info                                                                                                                                               | <p>Buildpack: java_buildpack_offline</p> <p>Start Command: CALCULATED_MEMORY=\$(PWD/.java-buildpack/open_jdk_jre/bin/java-buildpack-memory-calculator-2.0.2_RELEASE -memorySizes=metaspace:64m.,stack:228k.. -memoryWeights=heap:65,metaspace:10,native:15,stack:10 -memoryInitials=heap:100%,metaspace:100% -stackThreads=300 -totMemory=\$MEMORY_LIMIT) &amp;&amp; JAVA_OPTS="-Djava.io.tmpdir=\$TMPDIR -XX:OnOutOfMemoryError=\$PWD/.java-buildpack/open_jdk_jre/bin/killjava.sh \$CALCULATED_MEMORY -Djavax.net.ssl.trustStore=\$PWD/.java-buildpack/container_certificate_trust_store/truststore.jks -Djavax.net.ssl.trustStorePassword=java-buildpack-trust-store-password" &amp;&amp; SERVER_PORT=\$PORT eval exec \$PWD/.java-buildpack/open_jdk_jre/bin/java \$JAVA_OPTS -cp \$PWD/.org.springframework.boot.loader.JarLauncher</p> <p>Stack: cflinuxfs2 (Cloud Foundry Linux-based filesystem)</p> <p>Health check type: port</p> |
|  Spring Info                                                       | <input type="button" value="VIEW RAW JSON"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Git                                                                                                                                                | <p>SHA: <a href="#">c91dff0</a></p> <p>Message: "Skip SSL validation [#137189187]"</p> <p>Date: 01/06/17 08:50PM UTC</p> <p>Email: jberney@users.noreply.github.com</p> <p>Remote: git@github.com:pivotal-cf/spring-actuator-acceptance.git</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Build                                                                                                                                              | <p>Time: 04/21/17 09:03PM UTC</p> <p>Name:</p> <p>User Email: Pivotal Default</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| User Provided Environment Variables                                                                                                                | <input type="button" value="REVEAL USER PROVIDED ENV VARS"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Environment Variables<br>Defined by the runtime and buildpack. <a href="#">Learn more</a>                                                          | <input type="button" value="REVEAL ENV VARS"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Security Groups<br>A collection of egress rules that specify one or more individual protocols, ports, and destinations. <a href="#">Learn more</a> | <div>  default_security_group<br/>             running, staging           </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Delete App<br>This will permanently delete the app and all of its data.                                                                            | <input type="button" value="DELETE APP"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

In the upper right of the app page, Apps Manager also displays the SHA of your app code repository from the latest build:

[Git: 9c91991](#)


Buildpack: <https://github.com/cl...>

## View App Health

To view the health-check data that your app sends to its `/health` Actuator endpoints, select the **Overview** tab and click an instance under the **Instances** section:

Instances

| # | App Health | CPU | Memory    | Disk      | Uptime |
|---|------------|-----|-----------|-----------|--------|
| 0 | Up         | 0%  | 209.97 MB | 137.75 MB | 1 min  |

Health Check

```

status: UP
diskSpace
 status: UP
 free: 912412672
 threshold: 10485760
 total: 1056858112
mysql
 status: UP
 database: MySQL
 timestamp: Thu May 11 18:44:46 UTC 2017
postgresql
 status: UP
 database: PostgreSQL

```

View JSON

## View Thread Dump

To trigger and view a thread dump from your app to its `/dump` Actuator endpoint, select the **Threads** tab and click **Refresh**.

APP

amjs-test-spring-app

Running

VIEW APP

Overview

Services

Route (1)

Logs

Tasks

Trace

Threads

Settings

Git: c91dff0

Buildpack: java\_buildpack\_offline

Instance 0

Show ALL

DOWNLOAD

Last refresh: 05/8/17 16:48 PM

REFRESH

container-0

TIMED\_WAITING

```

"container-0" #15
 java.lang.Thread.State: TIMED_WAITING (sleeping)
 at java.lang.Thread.sleep(Native Method)
 at org.apache.catalina.core.StandardServer.await(StandardServer.java:427)
 at org.springframework.boot.context.embedded.tomcat.TomcatEmbeddedServletContainer$1.run(TomcatEmbeddedServletContainer$1.java:44)
 at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:511)
 at java.util.concurrent.FutureTask.run(FutureTask.java:266)
 at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$201(ScheduledThreadPoolExecutor.java:178)
 at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.poll(ScheduledThreadPoolExecutor.java:184)
 at java.util.concurrent.ScheduledThreadPoolExecutor$DelayedWorkItem.run(ScheduledThreadPoolExecutor.java:204)
 at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
 at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
 at java.lang.Thread.run(Thread.java:745)

Locked ownable synchronizers:
- None

```

ContainerBackgroundProcessor[StandardEngine[Tomcat]]

TIMED\_WAITING

DestroyJavaVM

RUNNABLE

Finalizer

WAITING

http-nio-8080-Acceptor-0

RUNNABLE

You can click each thread to expand and view its details. You can also modify which threads appear on the page using the **Instance** and **Show** drop-down menus.

## View Request Traces

To retrieve and view tracing information from the `/trace` Actuator endpoint of your app, select the **Trace** tab and click **Refresh**.

APP

amjs-test-spring-app

Running

VIEW APP

Git: c91dff0

Buildpack: java\_buildpack\_offline

Overview

Services

Route (1)

Logs

Tasks

Trace

Threads

Settings

Instance

ALL

☒ Hide Pivotal Apps Manager Requests

Last refresh: 05/8/17 16:39 PM

REFRESH

16:39:17.939

200

OPTIONS /cloudfoundryapplication/trace

0ms

Request:

host: amjs-test-spring-app.apps.oogie-boogie.gcp.appsman.cf-app.com  
 user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_12\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari  
 accept: \*/\*  
 accept-encoding: gzip, deflate, sdch, br  
 accept-language: en-US,en;q=0.8  
 access-control-request-headers: authorization,x-cf-app-instance  
 access-control-request-method: GET  
 origin: https://apps.sys.oogie-boogie.gcp.appsman.cf-app.com  
 via: 1.1 google  
 x-b3-spanid: bbf508bcd3118db  
 x-b3-traceid: bbf508bcd3118db  
 x-cf-applicationid: 2d2028b0-33ab-4e9a-b575-d63a6f2f8582  
 x-cf-instanceid: 29f8bf49-5b12-4131-475e-68360548cb6a  
 x-cloud-trace-context: 39945641373be76ef67bebf185e09575/10770927836782894347  
 x-forwarded-for: 209.234.137.222, 35.186.230.30  
 x-forwarded-proto: https  
 x-request-start: 1494286757937  
 x-vcap-request-id: 75012830-8a64-432e-792b-d88ba0cb55e3  
 connection: close

Response:  
 X-Application-Context: amjs-test-spring-app:cloud:0  
 Access-Control-Allow-Origin: \*  
 Vary: Origin  
 Access-Control-Allow-Methods: GET,POST  
 Access-Control-Allow-Headers: authorization, x-cf-app-instance  
 Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS, PATCH  
 status: 200

> 16:39:14.845 200 GET /cloudfoundryapplication/info

> 16:39:14.842 200 GET /cloudfoundryapplication/health

> 16:39:14.734 200 OPTIONS /cloudfoundryapplication/info

> 16:39:14.732 200 OPTIONS /cloudfoundryapplication/health

> 16:39:14.653 200 GET /cloudfoundryapplication

> 16:39:14.542 200 OPTIONS /cloudfoundryapplication

> 16:38:50.619 200 GET /favicon.ico

> 16:38:50.359 404 GET /

This page displays the last 100 requests from your app. You can click each individual request to expand and view its trace details. You can modify which requests appear on the page using the **Instance** drop-down menu.

By default, the **Trace** tab does not show requests and responses from Apps Manager polling app instances for data. To include these requests, clear the **Hide Pivotal Apps Manager Requests** checkbox next to the **Instance** drop-down menu.

## Download Heap Dump

To trigger and view a heap dump from your app to its `/heapdump` endpoint, select the settings drop-down menu for an instance of your app and click **Heap Dump**. This downloads a `.zip` file.

| Instances                                                                       |            |     |           |           |             |
|---------------------------------------------------------------------------------|------------|-----|-----------|-----------|-------------|
| #                                                                               | App Health | CPU | Memory    | Disk      | Uptime      |
| > 0                                                                             | ↑ Up       | 27% | 206.21 MB | 137.75 MB | 1 hr 11 min |
| <div> <div>Heap Dump</div> <div>View Trace</div> <div>View Threads</div> </div> |            |     |           |           |             |

## View Mappings

To view a collated list of the endpoints an app serves, select the **Settings** tab and click **View Mappings**.

Overview
Services
Route (1)
Logs
Tasks
Trace
Threads
Settings

App Name
docs-spring-app
UPDATE
CANCEL

Info
Buildpack: java\_buildpack\_offline
Start Command:
Stack: cflinuxfs2 (Cloud Foundry Linux-based filesystem)
Health check type: port

Metrics Forwarder
Metrics Forwarder allows applications to emit metrics into loggregator and consume those metrics from the firehose.

Spring Info
VIEW RAW JSON

Git
SHA: c91dff0
Message: "Skip SSL validation [#137189187]"
Date: 01/06/17 08:50PM UTC
Email: jberney@users.noreply.github.com
Remote: git@github.com:pivotal-cf/spring-actuator-acceptance.git

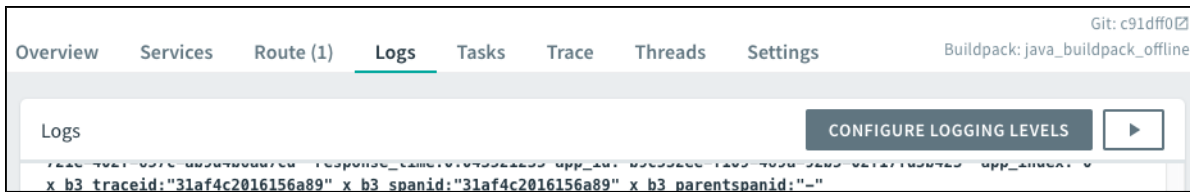
Build
Time: 04/21/17 09:03PM UTC
Name:
User Email: Pivotal Default

Mappings
VIEW MAPPINGS

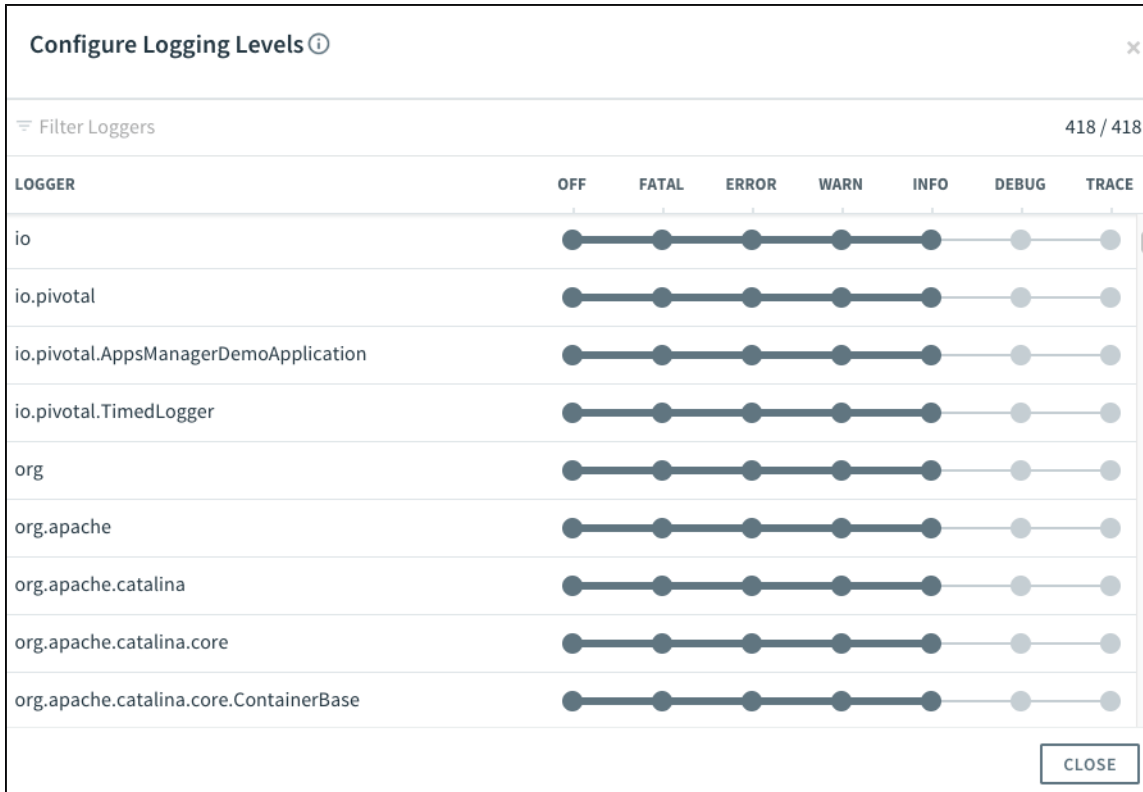
## Manage Log Levels

Spring Boot apps include *loggers* for many provided and user components of the app. You can set the log level for each logger in Apps Manager.

To view the **Configure Logging Levels** screen, select the **Logs** tab and click **Configure Logging Levels**.




Apps Manager displays the default log level for each logger in gray.



You can modify the log level for a logger by clicking the desired level in the logger row, as shown in the image below. Whenever you set a log level, the following happens:

- The log level displays in blue to indicate that it is user-configured.
- Each child namespace of the logger inherits the log level.

 **Note:** You can manually set any of the child loggers to override this inheritance.

Configure Logging Levels ⓘ

Filter Loggers

418 / 418

| LOGGER                                                   | OFF                      | FATAL                    | ERROR                    | WARN                                | INFO                     | DEBUG                    | TRACE                    |
|----------------------------------------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|
| org.springframework.boot.actuate.autoconfigure.CrshAu... | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| io.pivotal                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| io.pivotal.AppsManagerDemoApplication                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| io.pivotal.TimedLogger                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.apache                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.apache.catalina                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

All of the loggers with user-configured logging levels float to the top of the list.

Configure Logging Levels ⓘ

Filter Loggers

418 / 418

| LOGGER                                      | OFF                      | FATAL                    | ERROR                    | WARN                                | INFO                     | DEBUG                    | TRACE                    |
|---------------------------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|
| ROOT                                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| io.pivotal                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| io.pivotal.AppsManagerDemoApplication       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.apache.catalina.startup.DigesterFactory | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.apache.catalina.util.LifecycleBase      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.apache.coyote.http11.Http11NioProtocol  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.apache.sshd.common.util.SecurityUtils   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.apache.tomcat.util.net.NioSelectorPool  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| org.crsh.plugin                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Close

You can reset log levels by clicking the white dot displayed on the current log level.

| OFF                      | FATAL                    | ERROR                    | WARN                                | INFO                     | DEBUG                    |
|--------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> |

You can also filter which loggers you see using the **Filter Loggers** textbox.

| Configure Logging Levels ⓘ |
|----------------------------|
| ≡ org                      |
| LOGGER                     |
| org                        |
| org.apache                 |
| org.apache.catalina        |
| org.apache.catalina.core   |

## Troubleshoot Spring Boot Actuator Integration

This section describes how to troubleshoot common issues with the integration of Apps Manager and Spring Boot Actuator.

### /cloudfoundryapplication Failed Request

#### Symptom

You see the following failed request message in your app logs:

```
Could not find resource for relative : /cloudfoundryapplication of full path: http://example.com/cloudfoundryapplication
```

#### Explanation

Apps Manager uses the `/cloudfoundryapplication` endpoint as the root for Spring Boot Actuator integrations. It calls this endpoint for an app when you view the app in the Apps Manager UI, regardless of whether you have [configured Spring Boot Actuator endpoints for Apps Manager](#).

#### Solution

If you are not using the Spring Boot Actuator integrations for Apps Manager, you can ignore this failed request message.



## Using the Cloud Foundry Command Line Interface (cf CLI)

This guide explains the Cloud Foundry Command Line Interface (cf CLI), a tool you use to deploy and manage your applications.

Contents in this section:


- [Installing the cf CLI](#)
- [Getting Started with the cf CLI](#)
- [Using the cf CLI with an HTTP Proxy Server](#) [↗](#)
- [Using the cf CLI with a Self-Signed Certificate](#)
- [Using cf CLI Plugins](#)
- [Developing cf CLI Plugins](#)
- [Cloud Foundry CLI Reference Guide](#)

## Installing the cf CLI

Page last updated:

This topic describes how to install the Cloud Foundry Command Line Interface (cf CLI). Follow the instructions below for your operating system. If you previously used the cf CLI v5 Ruby gem, [uninstall](#) this gem first.


You can install the cf CLI with a package manager, an installer, or a compressed binary.

 **Note:** For use with Pivotal Cloud Foundry v1.10, the recommended minimum version is cf CLI v6.23 or later.

## Use a Package Manager

### Mac OS X Installation

For Mac OS X, perform the following steps to install the cf CLI with [Homebrew](#) :

1. Tap the Cloud Foundry formula [repository](#) :

```
$ brew tap cloudfoundry/tap
```

2. Install the cf CLI:

```
$ brew install cf-cli
```

### Linux Installation

For Debian and Ubuntu-based Linux distributions, perform the following steps:

1. Add the Cloud Foundry Foundation public key and package repository to your system:

```
$ wget -q -O - https://packages.cloudfoundry.org/debian/cli.cloudfoundry.org.key | sudo apt-key add -
```

```
$ echo "deb https://packages.cloudfoundry.org/debian stable main" | sudo tee /etc/apt/sources.list.d/cloudfoundry-cli.list
```

2. Update your local package index:

```
$ sudo apt-get update
```

3. Install the cf CLI:

```
$ sudo apt-get install cf-cli
```

For Enterprise Linux and Fedora systems (RHEL6/CentOS6 and up), perform the following steps:

1. Configure the Cloud Foundry Foundation package repository:

```
$ sudo wget -O /etc/yum.repos.d/cloudfoundry-cli.repo https://packages.cloudfoundry.org/fedora/cloudfoundry-cli.repo
```

2. Install the cf CLI, which also downloads and adds the public key to your system:

```
$ sudo yum install cf-cli
```

## Use an Installer

Follow the instructions for your operating system below.

### Windows Installation

You can run cf CLI in either the Windows Subsystem for Linux (WSL), also known as Bash on Windows, or in the Windows command line.

To use WSL, follow the [Linux Installation](#) instructions.

To use the cf CLI installer for the Windows command line, perform the following steps:

1. Download [the Windows installer](#).
2. Unpack the zip file.
3. Right click on the 'cf\_installer' executable and select "Run as Administrator"
4. When prompted, click **Install**, then **Finish**.
5. To verify your installation, open a command prompt and type `cf`. If your installation was successful, the cf CLI help listing appears.

### Mac OS X Installation

To use the cf CLI installer for Mac OS X, perform the following steps:

1. Download [the OS X installer](#).
2. Open the `.pkg` file.
3. In the installer wizard, click **Continue**.
4. Select an install destination and click **Continue**.
5. When prompted, click **Install**.
6. To verify your installation, open a terminal window and type `cf`. If your installation was successful, the cf CLI help listing appears.

### Linux Installation

To use the cf CLI installer for Linux, perform the following steps:

1. Download the Linux installer for your [Debian/Ubuntu](#) or [Red Hat](#) system.
2. Install using your system's package manager. Note these commands may require `sudo`.

- For Debian/Ubuntu, run the following command:

```
$ dpkg -i path/to/cf-cli-*.deb && apt-get install -f
```

- For Red Hat, run the following command:

```
rpm -i path/to/cf-cli-*.rpm
```

3. To verify your installation, open a terminal window and type `cf`. If your installation was successful, the cf CLI help listing appears.

## Use a Compressed Binary

Download the compressed binary for Mac OS X, Windows, or Linux from the cf CLI GitHub [repository](#) and install it on your system.

The specific procedures vary by operating system, but the following example illustrates downloading and installing the binary on Mac OS X:

1. Download and extract the Mac OS X binary:

```
$ curl -L "https://cli.run.pivotal.io/stable?release=macosx64-binary&source=github" | tar -zx
```

2. Move it to `/usr/local/bin`, or another location in your `$PATH`:

```
$ mv cf /usr/local/bin
```

3. Confirm your cf CLI version:

```
$ cf --version
```

## Next Steps

See [Getting Started with cf CLI](#) for more information about how to use the cf CLI.

We recommend that you review our [CLI releases page](#) to learn when updates are released, and download a new binary or a new installer when you want to update to the latest version.

## Uninstall the cf CLI

### Package Manager

If you previously installed the cf CLI with a package manager, follow the instructions specific to your package manager to uninstall the cf CLI.

The specific procedures vary by package manager, but the following example illustrates uninstalling the cf CLI with Homebrew:

```
$ brew uninstall cf-cli
```

### Installer

If you previously installed the cf CLI with an installer, perform the instructions specific to your operating system to uninstall the cf CLI:

- For Mac OS, delete the binary `/usr/local/bin/cf`, and the directory `/usr/local/share/doc/cf-cli`.
- For Windows, navigate to the **Control Panel**, click **Programs and Features**, select `Cloud Foundry CLI VERSION` and click **Uninstall**.

### Binary

If you previously installed a cf CLI binary, remove the binary from where you copied it.

### cf CLI v5

To uninstall, run `gem uninstall cf`.



**Note:** To ensure that your Ruby environment manager registers the change, close and reopen your terminal.

## Getting Started with the cf CLI

Page last updated:

This topic describes configuring and getting started with the Cloud Foundry Command Line Interface (cf CLI). This page assumes you have the latest version of the cf CLI. See the [Installing the Cloud Foundry Command Line Interface](#) topic for installation instructions.

## Localize

The cf CLI translates terminal output into the language that you select. The default language is `en-US`. The cf CLI supports the following languages:

- Chinese (simplified): `zh-Hans`
- Chinese (traditional): `zh-Hant`
- English: `en-US`
- French: `fr-FR`
- German: `de-DE`
- Italian: `it-IT`
- Japanese: `ja-JP`
- Korean: `ko-KR`
- Portuguese (Brazil): `pt-BR`
- Spanish: `es-ES`


Use [cf config](#) to set the language. To set the language with `cf config`, use the syntax: `$ cf config --locale YOUR_LANGUAGE`.

For example, to set the language to Portuguese and confirm the change by running `cf help`:

```
$ cf config --locale pt-BR
$ cf help
NOME:
 cf - Uma ferramenta de linha de comando para interagir com Cloud Foundry

USO:
 cf [opções globais] comando [argumentos...] [opções de comando]

VERSÃO:
 6.14.1+dc6adf6-2015-12-22
 ...
```

 **Note:** Localization with `cf config --locale` affects only messages that the cf CLI generates.

## Login

Use [cf login](#) to log in to PAS. The `cf login` command uses the following syntax to specify a target API endpoint, an org (organization), and a space:

```
$ cf login [-a API_URL] [-u USERNAME] [-p PASSWORD] [-o ORG] [-s SPACE] .
```

- `API_URL`: This is your API endpoint, [the URL of the Cloud Controller in your PAS instance](#).
- `USERNAME`: Your username.
- `PASSWORD`: Your password. Use of the `-p` option is discouraged as it may record your password in your shell history.
- `ORG`: The org where you want to deploy your apps.
- `SPACE`: The space in the org where you want to deploy your apps.

The cf CLI prompts for credentials as needed. If you are a member of multiple orgs or spaces, `cf login` prompts you for which ones to log into. Otherwise it targets your org and space automatically.

```
$ cf login -a https://api.example.com -u username@example.com
API endpoint: https://api.example.com
```

```
Password>
Authenticating...
OK
```

```
Select an org (or press enter to skip):
1. example-org
2. example-other-org
```

```
Org> 1
Targeted org example-org
```

```
Select a space (or press enter to skip):
1. development
2. staging
3. production
```

```
Space> 1
Targeted space development
```

Alternatively, you can write a script to log in and set your target using the non-interactive [cf api](#), [cf auth](#), and [cf target](#) commands.

Upon successful login, the cf CLI saves a `config.json` file containing your API endpoint, org, space values, and access token. If you change these settings, the `config.json` file is updated accordingly.

By default, `config.json` is located in your `~/.cf` directory. The `CF_HOME` environment variable allows you to locate the `config.json` file wherever you like.

## Users and Roles

The cf CLI includes commands that list users and assign roles in orgs and spaces. See the [Orgs, Spaces, Roles, and Permissions](#) topic.

### Commands for Listing Users

These commands take an org or space as an argument:

- [cf org-users](#)
- [cf space-users](#)

For example, to list the users who are members of an org:

```
$ cf org-users example-org
Getting users in org example-org as username@example.com...
```

```
ORG MANAGER
username@example.com
```

```
BILLING MANAGER
huey@example.com
dewey@example.com
```

```
ORG AUDITOR
louie@example.com
```

### Commands for Managing Roles

These commands require PAS admin permissions and take username, org or space, and role as arguments:


- [cf set-org-role](#)
- [cf unset-org-role](#)
- [cf set-space-role](#)
- [cf unset-space-role](#)

Available roles are `OrgManager`, `BillingManager`, `OrgAuditor`, `SpaceManager`, `SpaceDeveloper`, and `SpaceAuditor`. For example, to grant the Org Manager role to

a user within an org:

```
$ cf set-org-role huey@example.com example-org OrgManager
```

```
Assigning role OrgManager to user huey@example.com in org example-org as username@example.com...
OK
```

 **Note:** If you are not a PAS admin, you see this message when you try to run these commands:

```
error code: 10003, message: You are not authorized to perform the requested
action
```

## Identical Usernames in Multiple Origins

If a username corresponds to multiple accounts from different user stores, such as both the internal UAA store and an external SAML or LDAP store, the

`set` and `unset` role commands above return an error: `The user exists in multiple origins. Specify an origin for the requested user from: 'uaa', 'other'`

To resolve this ambiguity, the operator can construct a `curl` command that uses the CF API to perform the desired role-management function. For an example, see the [PUT v2/organizations/:guid/auditors](#) API function.


## Push

The [cf push](#) command pushes a new app or syncs changes to an existing app.

If you do not provide a hostname (also known as subdomain), `cf push` routes your app to a URL of the form `APPNAME.DOMAIN` based on the name of your app and your default domain. If you want to map a different route to your app, see the [Routes and Domains](#) topic for information about creating routes.

The `cf push` command supports many options that determine how and where the app instances are deployed. For details about the `cf push` command, see the [push](#) page in the Cloud Foundry CLI Reference Guide.

The following example pushes an app called `my-awesome-app` to the URL `http://my-awesome-app.example.com` and specifies the Ruby buildpack with the `-b` flag.

 **Note:** When you push an app and specify a buildpack with the `-b` flag, the app remains permanently linked to that buildpack. To use the app with a different buildpack, you must delete the app and re-push it.

```
$ cf push my-awesome-app -b ruby_buildpack
Creating app my-awesome-app in org example-org / space development as username@example.com...
OK
```

```
Creating route my-awesome-app.example.com...
OK
...
```

```
1 of 1 instances running
```

```
App started
...
```

```
requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: my-awesome-app.example.com
last uploaded: Wed Jun 8 23:43:15 UTC 2016
stack: cflinuxfs2
buildpack: ruby_buildpack
```

```
state since cpu memory disk details
#0 running 2016-06-08 04:44:07 PM 0.0% 0 of 1G 0 of 1G
```

For more information about available buildpacks, see the [Buildpacks](#) topic.

## User-Provided Service Instances

To create or update a user-provided service instance, you need to supply basic parameters. For example a database service might require a username, password, host, port, and database name.

The cf CLI has three ways of supplying these parameters to create or update an instance of a service: interactively, non-interactively, and in conjunction with third-party log management software as described in [RFC 6587](#). When used with third-party logging, the cf CLI sends data formatted according to [RFC 5424](#).

You create a service instance with `cf cups` and update one with `cf uups` as described below.

## The cf create-user-provided-service (cups) Command

Use [cf create-user-provided-service](#) (alias `cf cups`) creates a new service instance.

**To supply service instance parameters interactively:** Specify parameters in a comma-separated list after the `-p` flag. This example command-line session creates a service instance for a database service.

```
$ cf cups sql-service-instance -p "host, port, dbname, username, password"
host> mysql.example.com
port> 1433
dbname> mysqlpdb
username> admin
password> Pa55w0rd
Creating user provided service sql-service-instance in org example-org / space development as username@example.com...
OK
```

**To supply service instance parameters to `cf cups` non-interactively:** Pass parameters and their values in as a JSON hash, bound by single quotes, after the `-p` tag. This example is a non-interactive version of the `cf cups` session above.

```
$ cf cups sql-service-instance -p '{"host":"mysql.example.com", "port":"1433", "dbname":"mysqlpdb", "username":"admin", "password":"pa55woRD"}'
Creating user provided service sql-service-instance in org example-org / space development as username@example.com...
OK
```

**To create a service instance that sends data to a third-party:** Use the `-l` option followed by the external destination URL. This example creates a service instance that sends log information to the syslog drain URL of a third-party log management service. For specific log service instructions, see the [Service-Specific Instructions for Streaming Application Logs](#) topic.

```
$ cf cups mylog -l syslog://logs4.example.com:25258
Creating user provided service mylog in org example-org / space development as username@example.com...
OK
```

After you create a user-provided service instance, you bind it to an app with [cf bind-service](#), unbind it with [cf unbind-service](#), rename it with [cf rename-service](#), and delete it with [cf delete-service](#).

## The cf update-user-provided-service (uups) Command

Use [cf update-user-provided-service](#) (alias `cf uups`) to update one or more of the parameters for an existing user-provided service instance. The `cf uups` command uses the same syntax as `cf cups` above to set parameter values. The `cf uups` command does not update any parameter values that you do not supply.

## cf CLI Return Codes

The cf CLI uses exit codes, which help with scripting and confirming that a command has run successfully. For example, after you run a cf CLI command, you can retrieve its return code by running `echo $?` (on Windows, `echo %ERRORLEVEL%`). If the return code is `0`, the command was successful.

## The cf help Command

The [cf help](#) command lists the cf CLI commands and a brief description of each. Passing the `-h` flag to any command lists detailed help, including any



aliases. For example, to see detailed help for `cf delete`, run:

```
$ cf delete -h
NAME:
 delete - Delete an app

USAGE:
 cf delete APP_NAME [-f -r]

ALIAS:
 d

OPTIONS:
 -f Force deletion without confirmation
 -r Also delete any mapped routes
```

## Using the cf CLI with a Proxy Server

Page last updated:

If you have an HTTP or SOCKS5 proxy server on your network between a host running the cf CLI and your Cloud Foundry API endpoint, you must set `https_proxy` with the hostname or IP address of the proxy server.

The `https_proxy` environment variable holds the hostname or IP address of your proxy server.

`https_proxy` is a standard environment variable. Like any environment variable, the specific steps you use to set it depends on your operating system.

### Format of https\_proxy

`https_proxy` is set with hostname or IP address of the proxy server in URL format: `https_proxy=http://proxy.example.com`


If the proxy server requires a user name and password, include the credentials: `https_proxy=http://username:password@proxy.example.com`

If the proxy server uses a port other than 80, include the port number: `https_proxy=http://username:password@proxy.example.com:8080`

If the proxy server is a SOCKS5 proxy, specify the SOCKS5 protocol in the URL: `https_proxy=socks5://socks_proxy.example.com`

### Using SOCKS5 with v3-ssh

The `cf v3-ssh` command supports SOCKS5 proxies. To specify the SOCKS5 proxy server, set the `ALL_PROXY` environment variable using the following format: `ALL_PROXY=socks5://socks_proxy.example.com`.

 **Note:** `cf ssh` does not work through a SOCKS5 proxy.

### Setting https\_proxy in Mac OS or Linux

Set the `https_proxy` environment variable using the command specific to your shell. For example, in bash, use the `export` command.

Example:

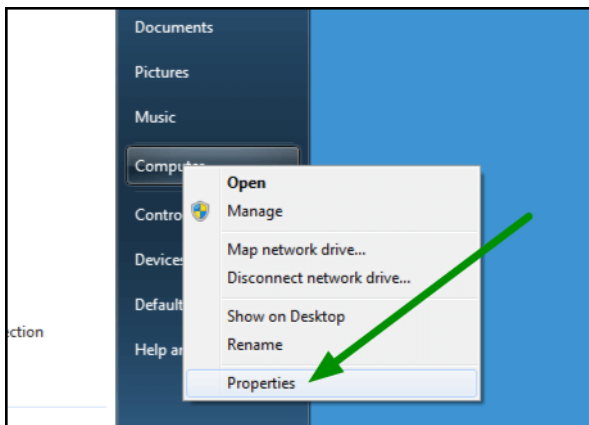
```
$ export https_proxy=http://my.proxyserver.com:8080
```

To make this change persistent, add the command to the appropriate profile file for the shell. For example, in bash, add a line like the following to your `.bash_profile` or `.bashrc` file:

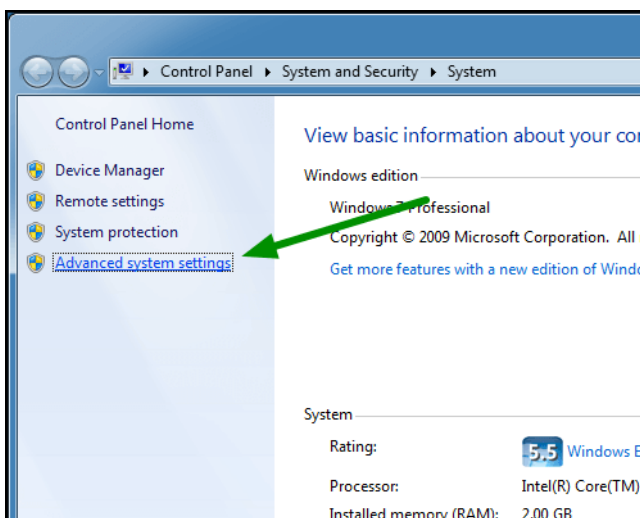
```
https_proxy=http://username:password@hostname:port
export $https_proxy
```

### Setting https\_proxy in Windows

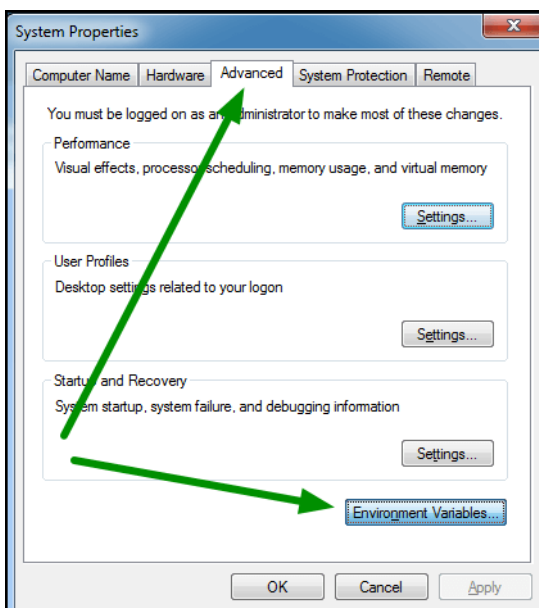
1. Open the Start menu. Right-click **Computer** and select **Properties**.



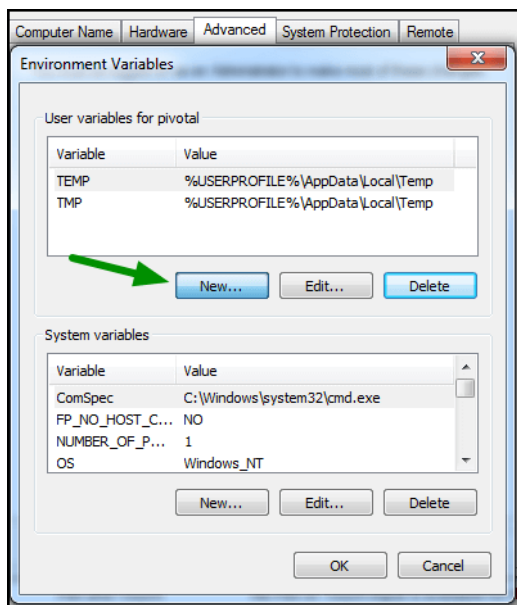
2. In the left pane of the System window, click **Advanced system settings**.



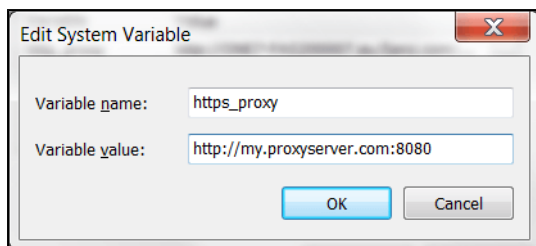
3. In the System Properties window, select the **Advanced** tab, then click **Environment Variables**.



4. In the Environment Variables window, under User variables, click **New**.



5. In the Variable name field, input `https_proxy`. In the Variable value field, input your proxy server information.



6. Click **OK**.

## Using the cf CLI with a Self-Signed Certificate

Page last updated:

This topic describes how developers can use the cf CLI to communicate securely with a Pivotal Cloud Foundry (PCF) deployment without specifying `--skip-ssl-validation` under the following circumstances:

- The deployment uses a self-signed certificate.
- The deployment uses a certificate that is signed by a self-signed certificate authority (CA), or a certificate signed by a certificate that's signed by a self-signed CA.

Before following the procedure below, the developer must obtain either the self-signed certificate or the intermediate and CA certificate(s) used to sign the deployment's certificate. The developer can obtain these certificates from the PCF operator.

## Install the Certificate on Local Machines

The certificates that developers must insert into their local truststore vary depending on the configuration of the deployment.

- If the deployment uses a self-signed certificate, the developer must insert the self-signed certificate into their local truststore.
- If the deployment uses a certificate that is signed by a self-signed certificate authority (CA), or a certificate signed by a certificate that's signed by a self-signed CA, the developer must insert the self-signed certificate and any intermediate certificates into their local truststore.

## Installing the Certificate on Mac OS X

Enter the following command to place a certificate file `server.crt` into your local truststore:

```
$ sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain server.crt
```

## Installing the Certificate on Linux

Perform the following steps specific to your distribution to place the certificate file `server.crt` into your truststore:

- Debian/Ubuntu/Gentoo:

```
$ cat server.crt >> /etc/ssl/certs/ca-certificates.crt
```

- Fedora/RHEL:

```
$ cat server.crt >> /etc/pki/tls/certs/ca-bundle.crt
```

The above example will set certificate permanently on your machine accross all users and requires sudo permissions. You can also run the following command to set certificate in your current terminal/script:

```
$ export SSL_CERT_FILE=/path/to/server.crt
```

or

```
$ export SSL_CERT_DIR=/path/to/server/dir
```

## Installing the Certificate on Windows

1. Right-click on the certificate file and click **Install Certificate**.
2. Choose to install the certificate as the **Current User** or **Local Machine**. Choose the **Trusted Root Certification Authorities** as the certification store.



## Using cf CLI Plugins

Page last updated:

The Cloud Foundry Command Line Interface (cf CLI) includes plugin functionality. These plugins enable developers to add custom commands to the cf CLI. You can install and use plugins that Cloud Foundry developers and third-party developers create. You can review the [Cloud Foundry Community CLI Plugin page](#) for a current list of community-supported plugins. You can find information about submitting your own plugin to the community in the [Cloud Foundry CLI plugin repository](#) on GitHub.

**⚠ warning:** Plugins are not vetted in any way, including for security or functionality. Use plugins at your own risk.

The cf CLI identifies a plugin by its binary filename, its developer-defined plugin name, and the commands that the plugin provides. You use the binary filename only to install a plugin. You use the plugin name or a command for any other action.

**💡 Note:** The cf CLI uses case-sensitive commands, but plugin management commands accept plugin and repository names irrespective of their casing.

## Changing the Plugin Directory

By default, the cf CLI stores plugins on your workstation in `$CF_HOME/.cf/plugins`, which defaults to `$HOME/.cf/plugins`. To change the root directory of this path from `$CF_HOME`, set the `CF_PLUGIN_HOME` environment variable. The cf CLI appends `.cf/plugins` to the `CF_PLUGIN_HOME` path that you specify and stores plugins in that location.

For example, if you set `CF_PLUGIN_HOME` to `/my-folder`, cf CLI stores plugins in `/my-folder/.cf/plugins`.

## Installing a Plugin

1. Download a binary or the source code for a plugin from a trusted provider.

**💡 Note:** The cf CLI requires a binary file compiled from source code written in Go. If you download source code, you must compile the code to create a binary.

2. Run `cf install-plugin BINARY-FILENAME` to install a plugin. Replace `BINARY-FILENAME` with the path to and name of your binary file.

**💡 Note:** You cannot install a plugin that has the same name or that uses the same command as an existing plugin. You will be prompted to uninstall the existing plugin.

**💡 Note:** The cf CLI prohibits you from implementing any plugin that uses a native cf CLI command name or alias. For example, if you attempt to install a third-party plugin that includes the command `cf push`, the cf CLI halts the installation.

## Running a Plugin Command

Use the contents of the `cf help` CLI plugin management and Commands offered by installed plugins sections to manage plugins and run plugin commands.

1. Run `cf plugins` to list all installed plugins and all commands that the plugins provide.
2. Run `cf PLUGIN-COMMAND` to execute a plugin command.

## Checking for Plugin Updates

Run `cf plugins --outdated` to check all registered plugin repositories for newer versions of currently installed plugins.

Example:

```
$ cf plugins --outdated
Searching CF-Community, company-repo for newer versions of installed plugins...
plugin version latest version
coffeemaker 1.1.2 1.2.0
Use 'cf install-plugin' to update a plugin to the latest version.
```

For more information about the `cf plugins` command, see [cf plugins](#).

## Uninstalling a Plugin

Use the `PLUGIN-NAME` to remove a plugin, not the `BINARY-FILENAME`.

1. Run `cf plugins` to view the names of all installed plugins.
2. Run `cf uninstall-plugin PLUGIN-NAME` to remove a plugin.

## Adding a Plugin Repository

Run `cf add-plugin-repo REPOSITORY-NAME-URL` to add a plugin repository.

Example:

```
$ cf add-plugin-repo CF-Community https://plugins.cloudfoundry.org
https://plugins.cloudfoundry.org added as CF-Community
```

## Listing Available Plugin Repositories

Run [cf list-plugin-repos](#) to view your available plugin repositories.

Example:

```
$ cf list-plugin-repos
OK
Repo Name Url
CF-Community https://plugins.cloudfoundry.org
```

## Listing All Plugins by Repository

Run [cf repo-plugins](#) to show all plugins from all available repositories.

## Troubleshooting

The cf CLI provides the following error messages to help you troubleshoot installation and usage issues. Third-party plugins can provide their own error messages.

### Permission Denied

If you receive a `permission denied` error message, you lack required permissions to the plugin. You must have `read` and `execute` permissions to the plugin binary file.



## Plugin Command Collision

Plugin names and commands must be unique. The CLI displays an error message if you attempt to install a plugin with a non-unique name or command.

If the plugin has the same name or command as a currently installed plugin, you must first uninstall the existing plugin to install the new plugin.

If the plugin has a command with the same name as a native cf CLI command or alias, you cannot install the plugin.

## Developing cf CLI Plugins

Page last updated:

Users can create and install Cloud Foundry Command Line Interface (cf CLI) plugins to provide custom commands. These plugins can be submitted and shared to the [CF Community repository](#).

### Requirements

Using plugins requires cf CLI v.6.7 or higher. Refer to the [Installing the Cloud Foundry Command Line Interface](#) topic for information about downloading, installing, and uninstalling the cf CLI.

### Installing the Architecture

1. Implement the [predefined plugin interface](#).
2. Clone the [template repository](#). You will need the [basic GO plugin](#).

### Initializing the Plugin

To initialize a plugin, call `plugin.Start(new(MyPluginStruct))` from within the `main()` method of your plugin. The `plugin.Start(...)` function requires a new reference to the `struct` that implements the defined interface.

### Invoking cf CLI Commands

Invoke cf CLI commands with `cliConnection.CliCommand([]args)` from within a plugin's `Run(...)` method. The `Run(...)` method receives the `cliConnection` as its first argument. The `cliConnection.CliCommand([]args)` returns the output printed by the command and an error.

The output is returned as a slice of strings. The error will be present if the call to the cf CLI command fails.

For more information, see the [API commands documentation](#).

### Installing a Plugin

To install a plugin, run `cf install-plugin PATH_TO_PLUGIN_BINARY`.

For additional information about developing plugins, see the [plugin development guide](#).

## Cloud Foundry CLI Reference Guide

### Name

cf - A command line tool to interact with Cloud Foundry









### Usage

cf [global options] command [arguments...] [command options]














### Version

6.37.0+a40009753.2018-05-25

## Getting Started

| Command                                                                                                     | Description                           |
|-------------------------------------------------------------------------------------------------------------|---------------------------------------|
| <a href="#">help</a>      | Show help                             |
| <a href="#">version</a>  | Print the version                     |
| <a href="#">login</a>    | Log user in                           |
| <a href="#">logout</a>   | Log user out                          |
| <a href="#">passwd</a>   | Change user password                  |
| <a href="#">target</a>   | Set or view the targeted org or space |
| <a href="#">api</a>      | Set or view target api url            |
| <a href="#">auth</a>     | Authenticate non-interactively        |

## Apps

| Command                                                                                                                  | Description                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">apps</a>                  | List all apps in the target space                                                                                                                         |
| <a href="#">app</a>                   | Display health and status for an app                                                                                                                      |
| <a href="#">push</a>                  | Push a new app or sync changes to an existing app                                                                                                         |
| <a href="#">scale</a>                 | Change or view the instance count, disk space limit, and memory limit for an app                                                                          |
| <a href="#">delete</a>                | Delete an app                                                                                                                                             |
| <a href="#">rename</a>                | Rename an app                                                                                                                                             |
| <a href="#">start</a>                 | Start an app                                                                                                                                              |
| <a href="#">stop</a>                  | Stop an app                                                                                                                                               |
| <a href="#">restart</a>               | Stop all instances of the app, then start them again. This causes downtime.                                                                               |
| <a href="#">restage</a>               | Recreate the app's executable artifact using the latest pushed app files and the latest environment (variables, service bindings, buildpack, stack, etc.) |
| <a href="#">restart-app-instance</a>  | Terminate, then restart an app instance                                                                                                                   |
| <a href="#">run-task</a>              | Run a one-off task on an app                                                                                                                              |
| <a href="#">tasks</a>                 | List tasks of an app                                                                                                                                      |

| Command                             | Description                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <a href="#">terminate-task</a>      | Terminate a running task of an app                                                                                  |
| <a href="#">events</a>              | Show recent app events                                                                                              |
| <a href="#">files</a>               | Print out a list of files in a directory or the contents of a specific file of an app running on the DEA backend    |
| <a href="#">logs</a>                | Tail or show recent logs for an app                                                                                 |
| <a href="#">env</a>                 | Show all env variables for an app                                                                                   |
| <a href="#">set-env</a>             | Set an env variable for an app                                                                                      |
| <a href="#">unset-env</a>           | Remove an env variable                                                                                              |
| <a href="#">stacks</a>              | List all stacks (a stack is a pre-built file system, including an operating system, that can run apps)              |
| <a href="#">stack</a>               | Show information for a stack (a stack is a pre-built file system, including an operating system, that can run apps) |
| <a href="#">copy-source</a>         | Copies the source code of an application to another existing application (and restarts that application)            |
| <a href="#">create-app-manifest</a> | Create an app manifest for an app that has been pushed successfully                                                 |
| <a href="#">get-health-check</a>    | Show the type of health check performed on an app                                                                   |
| <a href="#">set-health-check</a>    | Change type of health check performed on an app                                                                     |
| <a href="#">enable-ssh</a>          | Enable ssh for the application                                                                                      |
| <a href="#">disable-ssh</a>         | Disable ssh for the application                                                                                     |
| <a href="#">ssh-enabled</a>         | Reports whether SSH is enabled on an application container instance                                                 |
| <a href="#">ssh</a>                 | SSH to an application container instance                                                                            |

## Services

| Command                                      | Description                                                |
|----------------------------------------------|------------------------------------------------------------|
| <a href="#">marketplace</a>                  | List available offerings in the marketplace                |
| <a href="#">services</a>                     | List all service instances in the target space             |
| <a href="#">service</a>                      | Show service instance info                                 |
| <a href="#">create-service</a>               | Create a service instance                                  |
| <a href="#">update-service</a>               | Update a service instance                                  |
| <a href="#">delete-service</a>               | Delete a service instance                                  |
| <a href="#">rename-service</a>               | Rename a service instance                                  |
| <a href="#">create-service-key</a>           | Create key for a service instance                          |
| <a href="#">service-keys</a>                 | List keys for a service instance                           |
| <a href="#">service-key</a>                  | Show service key info                                      |
| <a href="#">delete-service-key</a>           | Delete a service key                                       |
| <a href="#">bind-service</a>                 | Bind a service instance to an app                          |
| <a href="#">unbind-service</a>               | Unbind a service instance from an app                      |
| <a href="#">bind-route-service</a>           | Bind a service instance to an HTTP route                   |
| <a href="#">unbind-route-service</a>         | Unbind a service instance from an HTTP route               |
| <a href="#">create-user-provided-service</a> | Make a user-provided service instance available to CF apps |
| <a href="#">update-user-provided-service</a> | Update user-provided service instance                      |

## Orgs

| Command | Description |
|---------|-------------|
|         |             |

| Command                    | Description   |
|----------------------------|---------------|
| <a href="#">orgs</a>       | List all orgs |
| <a href="#">org</a>        | Show org info |
| <a href="#">create-org</a> | Create an org |
| <a href="#">delete-org</a> | Delete an org |
| <a href="#">rename-org</a> | Rename an org |

## Spaces

| Command                            | Description                               |
|------------------------------------|-------------------------------------------|
| <a href="#">spaces</a>             | List all spaces in an org                 |
| <a href="#">space</a>              | Show space info                           |
| <a href="#">create-space</a>       | Create a space                            |
| <a href="#">delete-space</a>       | Delete a space                            |
| <a href="#">rename-space</a>       | Rename a space                            |
| <a href="#">allow-space-ssh</a>    | Allow SSH access for the space            |
| <a href="#">disallow-space-ssh</a> | Disallow SSH access for the space         |
| <a href="#">space-ssh-allowed</a>  | Reports whether SSH is allowed in a space |

## Domains

| Command                              | Description                                               |
|--------------------------------------|-----------------------------------------------------------|
| <a href="#">domains</a>              | List domains in the target org                            |
| <a href="#">create-domain</a>        | Create a domain in an org for later use                   |
| <a href="#">delete-domain</a>        | Delete a domain                                           |
| <a href="#">create-shared-domain</a> | Create a domain that can be used by all orgs (admin-only) |
| <a href="#">delete-shared-domain</a> | Delete a shared domain                                    |
| <a href="#">router-groups</a>        | List router groups                                        |

## Routes

| Command                                | Description                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------|
| <a href="#">routes</a>                 | List all routes in the current space or the current organization            |
| <a href="#">create-route</a>           | Create a url route in a space for later use                                 |
| <a href="#">check-route</a>            | Perform a simple check to determine whether a route currently exists or not |
| <a href="#">map-route</a>              | Add a url route to an app                                                   |
| <a href="#">unmap-route</a>            | Remove a url route from an app                                              |
| <a href="#">delete-route</a>           | Delete a route                                                              |
| <a href="#">delete-orphaned-routes</a> | Delete all orphaned routes (i.e. those that are not mapped to an app)       |

## Network Policies

| Command                          | Description                                                           |
|----------------------------------|-----------------------------------------------------------------------|
| <a href="#">network-policies</a> | List direct network traffic policies                                  |
|                                  | Create policy to allow direct network traffic from one app to another |

| Command                               | Description                             |
|---------------------------------------|-----------------------------------------|
| <a href="#">add-network-policy</a>    |                                         |
| <a href="#">remove-network-policy</a> | Remove network traffic policy of an app |

## Buildpacks

| Command                          | Description         |
|----------------------------------|---------------------|
| <a href="#">buildpacks</a>       | List all buildpacks |
| <a href="#">create-buildpack</a> | Create a buildpack  |
| <a href="#">update-buildpack</a> | Update a buildpack  |
| <a href="#">rename-buildpack</a> | Rename a buildpack  |
| <a href="#">delete-buildpack</a> | Delete a buildpack  |

## User Admin

| Command                          | Description                     |
|----------------------------------|---------------------------------|
| <a href="#">create-user</a>      | Create a new user               |
| <a href="#">delete-user</a>      | Delete a user                   |
| <a href="#">org-users</a>        | Show org users by role          |
| <a href="#">set-org-role</a>     | Assign an org role to a user    |
| <a href="#">unset-org-role</a>   | Remove an org role from a user  |
| <a href="#">space-users</a>      | Show space users by role        |
| <a href="#">set-space-role</a>   | Assign a space role to a user   |
| <a href="#">unset-space-role</a> | Remove a space role from a user |

## Org Admin

| Command                                | Description                          |
|----------------------------------------|--------------------------------------|
| <a href="#">quotas</a>                 | List available usage quotas          |
| <a href="#">quota</a>                  | Show quota info                      |
| <a href="#">set-quota</a>              | Assign a quota to an org             |
| <a href="#">create-quota</a>           | Define a new resource quota          |
| <a href="#">delete-quota</a>           | Delete a quota                       |
| <a href="#">update-quota</a>           | Update an existing resource quota    |
| <a href="#">share-private-domain</a>   | Share a private domain with an org   |
| <a href="#">unshare-private-domain</a> | Unshare a private domain with an org |

## Space Admin

| Command                            | Description                                                                  |
|------------------------------------|------------------------------------------------------------------------------|
| <a href="#">space-quotas</a>       | List available space resource quotas                                         |
| <a href="#">space-quota</a>        | Show space quota info                                                        |
| <a href="#">create-space-quota</a> | Define a new space resource quota                                            |
| <a href="#">update-space-quota</a> | Update an existing space quota                                               |
| <a href="#">delete-space-quota</a> | Delete a space quota definition and unassign the space quota from all spaces |

| Command                           | Description                                |
|-----------------------------------|--------------------------------------------|
| <a href="#">set-space-quota</a>   | Assign a space quota definition to a space |
| <a href="#">unset-space-quota</a> | Unassign a quota from a space              |

## Service Admin

| Command                                   | Description                                                                                                                     |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">service-auth-tokens</a>       | List service auth tokens                                                                                                        |
| <a href="#">create-service-auth-token</a> | Create a service auth token                                                                                                     |
| <a href="#">update-service-auth-token</a> | Update a service auth token                                                                                                     |
| <a href="#">delete-service-auth-token</a> | Delete a service auth token                                                                                                     |
| <a href="#">service-brokers</a>           | List service brokers                                                                                                            |
| <a href="#">create-service-broker</a>     | Create a service broker                                                                                                         |
| <a href="#">update-service-broker</a>     | Update a service broker                                                                                                         |
| <a href="#">delete-service-broker</a>     | Delete a service broker                                                                                                         |
| <a href="#">rename-service-broker</a>     | Rename a service broker                                                                                                         |
| <a href="#">migrate-service-instances</a> | Migrate service instances from one service plan to another                                                                      |
| <a href="#">purge-service-offering</a>    | Recursively remove a service and child objects from Cloud Foundry database without making requests to a service broker          |
| <a href="#">purge-service-instance</a>    | Recursively remove a service instance and child objects from Cloud Foundry database without making requests to a service broker |
| <a href="#">service-access</a>            | List service access settings                                                                                                    |
| <a href="#">enable-service-access</a>     | Enable access to a service or service plan for one or all orgs                                                                  |
| <a href="#">disable-service-access</a>    | Disable access to a service or service plan for one or all orgs                                                                 |

## Security Group

| Command                                       | Description                                                                              |
|-----------------------------------------------|------------------------------------------------------------------------------------------|
| <a href="#">security-group</a>                | Show a single security group                                                             |
| <a href="#">security-groups</a>               | List all security groups                                                                 |
| <a href="#">create-security-group</a>         | Create a security group                                                                  |
| <a href="#">update-security-group</a>         | Update a security group                                                                  |
| <a href="#">delete-security-group</a>         | Deletes a security group                                                                 |
| <a href="#">bind-security-group</a>           | Bind a security group to a particular space, or all existing spaces of an org            |
| <a href="#">unbind-security-group</a>         | Unbind a security group from a space                                                     |
| <a href="#">bind-staging-security-group</a>   | Bind a security group to the list of security groups to be used for staging applications |
| <a href="#">staging-security-groups</a>       | List security groups in the staging set for applications                                 |
| <a href="#">unbind-staging-security-group</a> | Unbind a security group from the set of security groups for staging applications         |
| <a href="#">bind-running-security-group</a>   | Bind a security group to the list of security groups to be used for running applications |
| <a href="#">running-security-groups</a>       | List security groups in the set of security groups for running applications              |
| <a href="#">unbind-running-security-group</a> | Unbind a security group from the set of security groups for running applications         |

## Environment Variable Groups

| Command                                                | Description                                                            |
|--------------------------------------------------------|------------------------------------------------------------------------|
| <a href="#">running-environment-variable-group</a>     | Retrieve the contents of the running environment variable group        |
| <a href="#">staging-environment-variable-group</a>     | Retrieve the contents of the staging environment variable group        |
| <a href="#">set-staging-environment-variable-group</a> | Pass parameters as JSON to create a staging environment variable group |
| <a href="#">set-running-environment-variable-group</a> | Pass parameters as JSON to create a running environment variable group |

## Isolation Segments

| Command                                             | Description                                                           |
|-----------------------------------------------------|-----------------------------------------------------------------------|
| <a href="#">isolation-segments</a>                  | List all isolation segments                                           |
| <a href="#">create-isolation-segment</a>            | Create an isolation segment                                           |
| <a href="#">delete-isolation-segment</a>            | Delete an isolation segment                                           |
| <a href="#">enable-org-isolation</a>                | Entitle an organization to an isolation segment                       |
| <a href="#">disable-org-isolation</a>               | Revoke an organization's entitlement to an isolation segment          |
| <a href="#">set-org-default-isolation-segment</a>   | Set the default isolation segment used for apps in spaces in an org   |
| <a href="#">reset-org-default-isolation-segment</a> | Reset the default isolation segment used for apps in spaces of an org |
| <a href="#">set-space-isolation-segment</a>         | Assign the isolation segment for a space                              |
| <a href="#">reset-space-isolation-segment</a>       | Reset the space's isolation segment to the org default                |

## Feature Flags

| Command                              | Description                                     |
|--------------------------------------|-------------------------------------------------|
| <a href="#">feature-flags</a>        | Retrieve list of feature flags with status      |
| <a href="#">feature-flag</a>         | Retrieve an individual feature flag with status |
| <a href="#">enable-feature-flag</a>  | Allow use of a feature                          |
| <a href="#">disable-feature-flag</a> | Prevent use of a feature                        |

## Advanced

| Command                     | Description                                                  |
|-----------------------------|--------------------------------------------------------------|
| <a href="#">curl</a>        | Executes a request to the targeted API endpoint              |
| <a href="#">config</a>      | Write default values to the config                           |
| <a href="#">oauth-token</a> | Retrieve and display the OAuth token for the current session |
| <a href="#">ssh-code</a>    | Get a one time password for ssh clients                      |

## Add/remove Plugin Repository

| Command                            | Description                                                                     |
|------------------------------------|---------------------------------------------------------------------------------|
| <a href="#">add-plugin-repo</a>    | Add a new plugin repository                                                     |
| <a href="#">remove-plugin-repo</a> | Remove a plugin repository                                                      |
| <a href="#">list-plugin-repos</a>  | List all the added plugin repositories                                          |
| <a href="#">repo-plugins</a>       | List all available plugins in specified repository or in all added repositories |



## Add/remove Plugin

| Command                          | Description                        |
|----------------------------------|------------------------------------|
| <a href="#">plugins</a>          | List commands of installed plugins |
| <a href="#">install-plugin</a>   | Install CLI plugin                 |
| <a href="#">uninstall-plugin</a> | Uninstall CLI plugin               |

## Environment Variables


| Variable                           | Description                                                                    |
|------------------------------------|--------------------------------------------------------------------------------|
| CF_COLOR=false                     | Do not colorize output                                                         |
| CF_DIAL_TIMEOUT=5                  | Max wait time to establish a connection, including name resolution, in seconds |
| CF_HOME=path/to/dir/               | Override path to default config directory                                      |
| CF_PLUGIN_HOME=path/to/dir/        | Override path to default plugin config directory                               |
| CF_TRACE=true                      | Print API request diagnostics to stdout                                        |
| CF_TRACE=path/to/trace.log         | Append API request diagnostics to a log file                                   |
| https_proxy=proxy.example.com:8080 | Enable HTTP proxying for API requests                                          |

## Global Options



| Option    | Description                             |
|-----------|-----------------------------------------|
| -help, -h | Show help                               |
| -v        | Print API request diagnostics to stdout |

## Apps (experimental)

| Command                                 | Description                                                                      |
|-----------------------------------------|----------------------------------------------------------------------------------|
| <a href="#">v3-apps</a>                 | List all apps in the target space                                                |
| <a href="#">v3-app</a>                  | Display health and status for an app                                             |
| <a href="#">v3-create-app</a>           | Create a V3 App                                                                  |
| <a href="#">v3-push</a>                 | Push a new app or sync changes to an existing app                                |
| <a href="#">v3-scale</a>                | Change or view the instance count, disk space limit, and memory limit for an app |
| <a href="#">v3-delete</a>               | Delete a V3 App                                                                  |
| <a href="#">v3-start</a>                | Start an app                                                                     |
| <a href="#">v3-stop</a>                 | Stop an app                                                                      |
| <a href="#">v3-restart</a>              | Stop all instances of the app, then start them again. This causes downtime.      |
| <a href="#">v3-stage</a>                | Create a new droplet for an app                                                  |
| <a href="#">v3-restart-app-instance</a> | Terminate, then instantiate an app instance                                      |
| <a href="#">v3-droplets</a>             | List droplets of an app                                                          |
| <a href="#">v3-set-droplet</a>          | Set the droplet used to run an app                                               |
| <a href="#">v3-set-env</a>              | Set an env variable for an app                                                   |
| <a href="#">v3-unset-env</a>            | Remove an env variable from an app                                               |
| <a href="#">v3-get-health-check</a>     | Show the type of health check performed on an app                                |
| <a href="#">v3-set-health-check</a>     | Change type of health check performed on an app's process                        |



| Command                                                                                                             | Description             |
|---------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">v3-packages</a>        | List packages of an app |
| <a href="#">v3-create-package</a>  | Uploads a V3 Package    |

## Services (experimental)

| Command                                                                                                           | Description                                    |
|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <a href="#">share-service</a>    | Share a service instance with another space    |
| <a href="#">unshare-service</a>  | Unshare a shared service instance from a space |

## Developer Guide

This guide provides instructions for deploying and managing apps and services.

 Check out the 15-minute [Getting Started with PCF](#)  tutorial for learning Pivotal Cloud Foundry app deployment concepts.

See the following topics:

- [cf push](#)
- [SSH for Apps and Services](#)
- [Routes and Domains](#)
- [Managing Services](#)
- [Streaming App Logs](#)
- [Managing Apps with the cf CLI](#)
- [Cloud Foundry Environment Variables](#)
- [Cloud Controller API Client Libraries](#)
- [Considerations for Designing and Running and App in the Cloud](#)

## cf push

This topic provides an overview of the documentation available for `cf push`.

## How to Use cf push

The following topics provide procedures for deploying apps with `cf push`:

- [Deploying an App](#)
- [Deploying with App Manifests](#)
- [Deploying an App with Docker](#)
- [Deploying a Large App](#)
- [Starting, Restarting, and Restaging Apps](#)
- [Pushing an Application with Multiple Buildpacks](#)
- [Pushing an App with Multiple Processes \(Beta\)](#)
- [Running cf push Sub-Step Commands \(Beta\)](#)

## How to Troubleshoot

For information about troubleshooting when running `cf push`, see [Troubleshooting App Deployment and Health](#).


## How cf push Works

The following topics provide information about how `cf push` works:

- The [Push](#) section of *Getting Started with the cf CLI*.
- [App Container Lifecycle](#)
- [How Apps Are Staged](#)

## Deploy an Application

Page last updated:

 **Note:** See the [buildpacks](#) documentation for deployment guides specific to your app language or framework, such as the [Getting Started Deploying Ruby on Rails Apps](#) guide.

### Overview of Deployment Process

You deploy an app to Cloud Foundry by running a `cf push` command from the Cloud Foundry Command Line Interface (cf CLI). Refer to the [Installing the cf CLI](#) topic for more information. Between the time that you run `cf push` and the time that the app is available, Cloud Foundry performs the following tasks:

- Uploads and stores app files
- Examines and stores app metadata
- Creates a “droplet” (the Cloud Foundry unit of execution) for the app
- Selects an appropriate Diego [cell](#) to run the droplet
- Starts the app

For more information about the lifecycle of an app, see the [Application Container Lifecycle](#) topic.

An app that uses services, such as a database, messaging, or email server, is not fully functional until you provision the service and, if required, bind the service to the app. For more information about services, see the [Services Overview](#) topic.

### Step 1: Prepare to Deploy

Before you deploy your app to Cloud Foundry, make sure that:

- Your app is *cloud-ready*. Cloud Foundry behaviors related to file storage, HTTP sessions, and port usage may require modifications to your app.
- All required app resources are uploaded. For example, you may need to include a database driver.
- Extraneous files and artifacts are excluded from upload. You should explicitly exclude extraneous files that reside within your app directory structure, particularly if your app is large.
- An instance of every service that your app needs has been created.
- Your Cloud Foundry instance supports the type of app you are going to deploy, or you have the URL of an externally available buildpack that can stage the app.

For help preparing to deploy your app, see:

- [Considerations for Designing and Running an Application in the Cloud](#)
- [Buildpacks](#)

### Step 2: Know Your Credentials and Target


Before you can push your app to Cloud Foundry you need to know:

- The API endpoint for your Cloud Foundry instance. Also known as the target URL, this is [the URL of the Cloud Controller in your PAS instance](#).
- Your username and password for your Cloud Foundry instance.
- The organization and space where you want to deploy your app. A Cloud Foundry workspace is organized into organizations, and within them, spaces. As a Cloud Foundry user, you have access to one or more organizations and spaces.


### Step 3: (Optional) Configure Domains

Cloud Foundry directs requests to an app using a route, which is a URL made up of a host and a domain.

- The name of an app is the default host for that app, unless you specify the host name with the `-n` flag.
- Every app is deployed to an app space that belongs to a domain. Every Cloud Foundry instance has a default domain defined. You can specify a non-default, or custom, domain when deploying, provided that the domain is registered and is mapped to the organization which contains the target app space.

 **Note:** CF allows app names, but not app URLs, to include underscores. CF converts underscores to hyphens when setting a default app URL from an app name.

- The URL for your app must be unique from other apps hosted by PAS. Use the following options with the [cf CLI](#) to help create a unique URL:
  - `-n` to assign a different HOST name for the app
  - `--random-route` to create a URL that includes the app name and random words


 **Note:** Use `cf help push` to view other options for this command.

For more information about domains, see [Routes and Domains](#).

## Step 4: Determine Deployment Options

Before you deploy, you need to decide on the following:

- **Name:** You can use any series of alpha-numeric characters as the name of your app.
- **Instances:** Generally speaking, the more instances you run, the less downtime your app will experience. If your app is still in development, running a single instance can simplify troubleshooting. For any production app, we recommend a minimum of two instances.
- **Memory Limit:** The maximum amount of memory that each instance of your app can consume. If an instance exceeds this limit, Cloud Foundry restarts the instance.

 **Note:** Initially, Cloud Foundry immediately restarts any instances that exceed the memory limit. If an instance repeatedly exceeds the memory limit in a short period of time, Cloud Foundry delays restarting the instance.

- **Start Command:** This is the command that Cloud Foundry uses to start each instance of your app. This start command varies by app framework.
- **Subdomain (host) and Domain:** The route, which is the combination of subdomain and domain, must be globally unique. This is true whether you specify a portion of the route or allow Cloud Foundry to use defaults.
- **Services:** Apps can bind to services such as databases, messaging, and key-value stores. Apps are deployed into app spaces. An app can only bind to a service that has an existing instance in the target app space.

## Define Deployment Options

You can define deployment options on the command line, in a manifest file, or both together. See [Deploying with Application Manifests](#) to learn how app settings change from push to push, and how command-line options, manifests, and commands like `cf scale` interact.

When you deploy an app while it is running, Cloud Foundry stops all instances of that app and then deploys. Users who try to run the app get a “404 not found” message while `cf push` runs. Stopping all instances is necessary to prevent two versions of your code from running at the same time. A worst-case example would be deploying an update that involved a database schema migration, because instances running the old code would not work and users could lose data.


Cloud Foundry uploads all app files except version control files and folders with names such as `.svn`, `.git`, and `_darcs`. To exclude other files from upload, specify them in a `.cfignore` file in the directory where you run the push command. For more information, see the [Ignore Unnecessary Files When Pushing](#) section of the [Considerations for Designing and Running an Application in the Cloud](#) topic.

For more information about the manifest file, see the [Deploying with Application Manifests](#) topic.

## Configure Pre-Runtime Hooks

 **Note:** The Java buildpack does not support pre-runtime hooks.


To configure pre-runtime hooks, create a file named `.profile` and place it in the root of your app directory. If the directory includes a `.profile` script, then Cloud Foundry executes it immediately before each instance of your app starts. Because the `.profile` script executes after the buildpack, the script has access to the language runtime environment created by the buildpack.

 **Note:** Your app root directory may also include a `.profile.d` directory that contains bash scripts that perform initialization tasks for the buildpack. Developers should not edit these scripts unless they are using a [custom buildpack](#).

You can use the `.profile` script to perform app-specific initialization tasks, such as setting custom environment variables. Environment variables are key-value pairs defined at the operating system level. These key-value pairs provide a way to configure the apps running on a system. For example, any app can access the `LANG` environment variable to determine which language to use for error messages and instructions, collating sequences, and date formats.

To set an environment variable, add the appropriate bash commands to your `.profile` file. See the example below.

```
Set the default LANG for your apps
export LANG=en_US.UTF-8
```

 **Note:** If you are using a PHP buildpack version prior to v4.3.18, the buildpack does not execute your PHP app's `.profile` script. Your PHP app will host the `.profile` script's contents. This means that any PHP app staged using the affected PHP buildpack versions can leak credentials placed in the `.profile` script.

## Step 5: Push the App

Run the following command to deploy an app without a manifest:

```
cf push APP-NAME
```

If you provide the app name in a manifest, you can reduce the command to `cf push`. See [Deploying with Application Manifests](#).

Because all you have provided is the name of your app, `cf push` sets the number of instances, amount of memory, and other attributes of your app to the default values. You can also use command-line options to specify these and additional attributes.

The following transcript illustrates how Cloud Foundry assigns default values to app when given a `cf push` command.

 **Note:** When deploying your own apps, avoid generic names like `my-app`. Cloud Foundry uses the app name to compose the route to the app, and deployment fails unless the app has a globally unique route.

```
$ cf push my-app
Creating app my-app in org example-org / space development as a.user@shared-domain.example.com...
OK

Creating route my-app.shared-domain.example.com...
OK

Binding my-app.shared-domain.example.com to my-app...
OK

Uploading my-app...
Uploading app: 560.1K, 9 files
OK

Starting app my-app in org example-org / space development as a.user@shared-domain.example.com...
-----> Downloaded app package (552K)
OK
-----> Using Ruby version: ruby-1.9.3
-----> Installing dependencies using Bundler version 1.3.2
Running: bundle install --without development:test --path
vendor/bundle --binstubs vendor/bundle/bin --deployment
Installing rack (1.5.1)
Installing rack-protection (1.3.2)
Installing tilt (1.3.3)
Installing sinatra (1.3.4)
Using bundler (1.3.2)
Updating files in vendor/cache
Your bundle is complete! It was installed into ./vendor/bundle
Cleaning up the bundler cache.
-----> Uploading droplet (23M)

1 of 1 instances running

App started

Showing health and status for app my-app in org example-org / space development as a.user@shared-domain.example.com...
OK

requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: my-app.shared-domain.example.com

state since cpu memory disk
#0 running 2014-01-24 05:07:18 PM 0.0% 18.5M of 1G 52.5M of 1G
```

## Step 6: (Optional) Configure Service Connections

If you bound a service to the app that you deployed, you might need to configure your app with the service URL and credentials. For more information, see the specific documentation for your app framework:

- [Ruby](#)
- [Node.js](#)
- [Spring](#)
- [Grails](#)

## Step 7: Troubleshoot Deployment Problems

If your app does not start on Cloud Foundry, first ensure that your app can run locally.

You can troubleshoot your app in the cloud using the cf CLI. See [Troubleshoot Application Deployment and Health](#).



## Deploying with Application Manifests

Page last updated:

You use the Cloud Foundry Command Line Interface tool (cf CLI) `cf push` command to deploy apps. `cf push` deploys apps with a default number of instances, disk space limit, and memory limit. You can override the default values by invoking `cf push` with flags and values, or by specifying key-value pairs in a manifest file.

Manifests provide consistency and reproducibility, and can help you automate deploying apps.

### How cf push Finds the Manifest

By default, the `cf push` command deploys an application using a `manifest.yml` file in the current working directory.

For example:

```
$ cf push
Using manifest file /path-to-current-working-directory/manifest.yml
```

If you have created your manifest in a different location, use `cf push -f PATH-TO-MANIFEST`. Replace `PATH-TO-MANIFEST` with the path to your manifest.

You can include the name of your manifest file in `PATH-TO-MANIFEST`.

For example:

```
$ cf push -f ./different-directory-1/different-directory-2/alternate_manifest.yml
Using manifest file ./different-directory-1/different-directory-2/alternate_manifest.yml
```

If you provide a path with no filename, the `cf push` command requires a file named `manifest.yml`.

For example:

```
$ cf push -f ./different-directory-1/different-directory-2/
Using manifest file ./different-directory-1/different-directory-2/manifest.yml
```

### Example Manifest

Although you can deploy apps without a manifest, manifests provide consistency and reproducibility. This can be useful when you want your apps to be portable between different clouds.


Manifests are written in YAML. The manifest below illustrates some YAML conventions, as follows:

- The manifest begins with three dashes.
- The `applications` block begins with a heading followed by a colon.
- The application `name` is preceded by a single dash and one space.
- Subsequent lines in the block are indented two spaces to align with `name`.

```

applications:
- name: my-app
 memory: 512M
 instances: 2
```

A minimal manifest requires only an application `name`. To create a valid minimal manifest, remove the `memory` and `instances` properties from this example.

 **Note:** If your app name begins with the dash character (`-`), you cannot interact with the app using the cf CLI. This is because the cf CLI interprets the dash as a flag.


## Always Provide an Application Name to `cf push`

`cf push` requires an application name, which you provide either in a manifest or at the command line.

As described in [How `cf push` Finds the Manifest](#) above, the command `cf push` locates the `manifest.yml` in the current working directory by default, or in the path provided by the `-f` option.

If you do not use a manifest, the minimal `cf push` command looks like this:


```
$ cf push my-app
```

 **Note:** When you provide an application name at the command line, `cf push` uses that application name whether or not there is a different application name in the manifest. If the manifest describes multiple applications, you can push a single application by providing its name at the command line; the `cf` CLI does not push the others. Use these behaviors for testing.

## How `cf push` Finds the Application

By default, `cf push` recursively pushes the contents of the current working directory. Alternatively, you can provide a path using either a manifest or a command line option.

- If the path is to a directory, `cf push` recursively pushes the contents of that directory instead of the current working directory.
- If the path is to a file, `cf push` pushes only that file.

 **Note:** If you want to push more than a single file, but not the entire contents of a directory, consider using a `.cfignore` file to tell `cf push` what to exclude.

## Precedence Between Manifests, Command Line Options, and Most Recent Values

When you push an application for the first time, Cloud Foundry applies default values to any attributes that you do not set in a manifest or `cf push` command line options.

- For example, `cf push my-app` with no manifest might deploy one instance of the app with one gigabyte of memory. In this case the default values for instances and memory are “1” and “1G”, respectively.

Between one push and another, attribute values can change in other ways.

- For example, the `cf scale` command changes the number of instances.

The attribute values on the server at any one time represent the cumulative result of all settings applied up to that point: defaults, attributes in the manifest, `cf push` command line options, and commands like `cf scale`. There is no special name for this resulting set of values on the server. You can think of them as the most recent values.


`cf push` follows rules of precedence when setting attribute values:

- Manifests override most recent values, including defaults.
- Command line options override manifests.

In general, you can think of manifests as just another input to `cf push`, to be combined with command line options and most recent values.

## Optional Attributes

This section explains how to describe optional application attributes in manifests. Each of these attributes can also be specified by a command line option. Command line options override the manifest.

 **Note:** The route component attributes `domain`, `domains`, `host`, `hosts`, and `no-hostname` have been deprecated in favor of the `routes` attribute. For more information, see [Deprecated App Manifest Features](#).

## buildpacks

You can refer to a buildpack by name in a manifest or a command line option. The `cf buildpacks` command lists the buildpacks that you can use.

See below for information on referencing buildpacks in a manifest. The command line option that overrides this attribute is `-b`.

- **Custom buildpacks:** If your application requires a custom buildpack, you can use the `buildpacks` attribute to specify it in a number of ways:
  - By name: `MY-BUILDPACK`.
  - By GitHub URL: `https://github.com/cloudfoundry/java-buildpack.git`.
  - By GitHub URL with a branch or tag: `https://github.com/cloudfoundry/java-buildpack.git#v3.3.0` for the `v3.3.0` tag.


```


...
buildpacks:
- buildpack_URL
```

- **Multiple buildpacks:** If you are using multiple buildpacks, you can provide an additional `-b` flag or add an additional value to your manifest:

```

...
buildpacks:
- buildpack_URL
- buildpack_URL
```

 **Note:** This feature does not work with [Deprecated App Manifest Features](#).

 **Note:** You must specify multiple buildpacks in the correct order: the buildpack will use the app start command given by the final buildpack. See [the multi-buildpack repository](#) for more information.

Also see [Pushing an Application with Multiple Buildpacks](#) for more information.

## command

Some languages and frameworks require that you provide a custom command to start an application. Refer to the [buildpack](#) documentation to determine if you need to provide a custom start command.

You can provide the custom start command in your application manifest or on the command line. See [Starting, Restarting, and Restaging Applications](#) for more information about how Cloud Foundry determines its default start command.

To specify the custom start command in your application manifest, add it in the `command: START-COMMAND` format as the following example shows:

```

...
command: bundle exec rake VERBOSE=true
```


The start command you specify becomes the default for your application. To return to using the original default start command set by your buildpack, you must explicitly set the attribute to `null` as follows:

```

...
command: null
```

On the command line, use the `-c` option to specify the custom start command as the following example shows:

```
$ cf push my-app -c "bundle exec rake VERBOSE=true"
```

 **Note:** The `-c` option with a value of 'null' forces `cf push` to use the buildpack start command. See [Forcing cf push to use the Buildpack Start Command](#) for more information.

If you override the start command for a Buildpack application, Linux uses `bash -c YOUR-COMMAND` to invoke your application. If you override the start command for a Docker application, Linux uses `sh -c YOUR-COMMAND` to invoke your application. Because of this, if you override a start command, you should prefix `exec` to the final command in your custom composite start command.

An app needs to catch [termination signals](#) and clean itself up appropriately. Because of the way that shells manage process trees, the use of custom composite shell commands, particularly those that create child processes using `&`, `&&`, `||`, etc., can prevent your app from receiving signals that are sent to the top level bash process.

To resolve this issue, you can use `exec` to replace the bash process with your own process. For example:

- `bin/rake cf:on_first_instance db:migrate && bin/rails server -p $PORT -e $RAILS_ENV` The process tree is bash -> ruby, so on graceful shutdown only the bash process receives the TERM signal, not the ruby process.
- `bin/rake cf:on_first_instance db:migrate && exec bin/rails server -p $PORT -e $RAILS_ENV` Because of the `exec` prefix included on the final command, the ruby process invoked by rails takes over the bash process managing the execution of the composite command. The process tree is only ruby, so the ruby web server receives the TERM signal and can shutdown gracefully for 10 seconds.

In more complex situations, like making a custom buildpack, you may want to use bash `trap`, `wait`, and backgrounded processes to manage your process tree and shut down apps gracefully. In most situations, however, a well-placed `exec` should be sufficient.

## disk\_quota

Use the `disk_quota` attribute to allocate the disk space for your app instance. This attribute requires a unit of measurement: `M`, `MB`, `G`, or `GB`, in upper case or lower case.

```

...
disk_quota: 1024M
```

The command line option that overrides this attribute is `-k`.

## docker

If your application is contained in a Docker image, then you may use the `docker` attribute to specify it and an optional Docker username.


This attribute is a combination of `push` options that include `--docker-image` and `--docker-username`.

```

...
docker:
 image: docker-image-repository/docker-image-name
 username: docker-user-name
```

The command line option `--docker-image` or `-o` overrides `docker.image`. The command line option `--docker-username` overrides `docker.username`.

The manifest attribute `docker.username` is optional. If it is used, then the password must be provided in the environment variable `CF_DOCKER_PASSWORD`. Additionally, if a Docker username is specified, then a Docker image must also be specified.

 **Note:** Using the `docker` attribute in conjunction with the `buildpack` or `path` attributes will result in an error.

## health-check-http-endpoint

Use the `health-check-http-endpoint` attribute to customize the endpoint for the `http` health check type. If you do not provide a `health-check-http-endpoint` attribute, it uses endpoint `/`.

```

...
health-check-type: http
health-check-http-endpoint: /health
```

## health-check-type

Use the `health-check-type` attribute to set the `health_check_type` flag to either `port`, `process` or `http`. If you do not provide a `health-check-type` attribute, it defaults to `port`.

```

...
health-check-type: port
```

The command line option that overrides this attribute is `-u`.

The value of `none` is deprecated in favor of `process`.

## memory

Use the `memory` attribute to specify the memory limit for all instances of an app. This attribute requires a unit of measurement: `M`, `MB`, `G`, or `GB`, in upper case or lower case. For example:

```

...
memory: 1024M
```

The default memory limit is 1G. You might want to specify a smaller limit to conserve quota space if you know that your app instances do not require 1G of memory.

The command line option that overrides this attribute is `-m`.

## no-route

By default, `cf push` assigns a route to every app. But, some apps process data while running in the background and should not be assigned routes.

You can use the `no-route` attribute with a value of `true` to prevent a route from being created for your app.

```

...
no-route: true
```

The command line option that overrides this attribute is `--no-route`.

In the Diego architecture, `no-route` skips creating and binding a route for the app, but does not specify which type of health check to perform. If your app does not listen on a port because it is a worker or a scheduler app, then it does not satisfy the port-based health check and Cloud Foundry marks it as crashed. To prevent this, disable the port-based health check with `cf set-health-check APP_NAME process`.

To remove a route from an existing app, perform the following steps:

1. Remove the route using the `cf unmap-route` command.
2. Push the app again with the `no-route: true` attribute in the manifest or the `--no-route` command line option.

For more information, see [Describing Multiple Applications with One Manifest](#) below.

## path

You can use the `path` attribute to tell Cloud Foundry the directory location where it can find your application.

The directory specified as the `path`, either as an attribute or as a parameter on the command line, becomes the location where the buildpack `Detect` script executes.

The command line option that overrides this attribute is `-p`.

```

...
path: /path/to/application/bits
```

For more information, see [How cf push Finds the Application](#).

## random-route

If you push your app without specifying any route-related CLI options or app manifest flags, the cf CLI attempts to generate a route based on the app name, which can cause collisions.

You can use the `random-route` attribute to generate a unique route and avoid name collisions.

When you use `random-route`, the cf CLI generates an HTTP route with a random host (if `host` is not set) or a TCP route with an unused port number.

See the following example use cases:

- You deploy the same app to multiple spaces for testing purposes. In this situation, you can use `random-route` to randomize routes declared with the route attribute in the app manifest.
- You use an app manifest for a classroom training exercise in which multiple users deploy the same app to the same space.

The command line option that overrides this attribute is `--random-route`.

```

...
random-route: true
```

## routes

Use the `routes` attribute to provide multiple HTTP and TCP routes. Each route for this app is created if it does not already exist.

This attribute is a combination of `push` options that include `--hostname`, `-d`, and `--route-path`.

```

...
routes:
- route: example.com
- route: www.example.com/foo
- route: tcp-example.com:1234
```

### Manifest Attributes

The `routes` attribute cannot be used in conjunction with the following attributes: `host`, `hosts`, `domain`, `domains`, and `no-hostname`. An error will result.

### Push Flag Options

This attribute has unique interactions with different command line options.

| Push Flag Option            | Resulting Behaviour                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--no-route</code>     | All declared routes are ignored.                                                                                                                         |
| <code>-d</code>             | Overrides DOMAIN part of all declared HTTP and TCP routes.                                                                                               |
| <code>--hostname, -n</code> | Sets or overrides HOSTNAME in all HTTP routes.<br>It has no impact on TCP routes.                                                                        |
| <code>--route-path</code>   | Sets or overrides the PATH in all HTTP routes.<br>It has no impact on TCP routes.                                                                        |
| <code>--random-route</code> | Sets or overrides the HOSTNAME in all HTTP routes.<br>Sets or overrides the PORT in all TCP routes.<br>The PORT and HOSTNAME will be randomly generated. |

## stack

Use the `stack` attribute to specify which stack to deploy your application to.

To see a list of available stacks, run `cf stacks` from the cf CLI.

```

...
stack: cflinuxfs2
```

The command line option that overrides this attribute is `-s`.

## timeout

The `timeout` attribute defines the number of seconds that Cloud Foundry allocates for starting your application. It is related to the `health-check-type` attribute.

For example:

```

...
timeout: 80
```

## Environment Variables

The `env` block consists of a heading, then one or more environment variable/value pairs.

For example:

```

...
env:
 RAILS_ENV: production
 RACK_ENV: production
```

`cf push` deploys the application to a container on the server. The variables belong to the container environment.

While the application is running, you can modify environment variables.

- View all variables: `cf env my-app`
- Set an individual variable: `cf set-env my-app my-variable_name my-variable_value`
- Unset an individual variable: `cf unset-env my-app my-variable_name my-variable_value`

Environment variables interact with manifests in the following ways:

- When you deploy an application for the first time, Cloud Foundry reads the variables described in the environment block of the manifest and adds them to the environment of the container where the application is staged, and the environment of the container where the application is deployed.
- When you stop and then restart an application, its environment variables persist.

## Services

Applications can bind to services such as databases, messaging, and key-value stores.

Applications are deployed into App Spaces. An application can only bind to services instances that exist in the target App Space before the application is deployed.

The `services` block consists of a heading, then one or more service instance names.

Whoever creates the service chooses the service instance names. These names can convey logical information, as in `backend_queue`, describe the nature of the service, as in `mysql_5.x`, or do neither, as in the example below.

```

...
services:
- instance_ABC
- instance_XYZ
```

Binding to a service instance is a special case of setting an environment variable, namely `VCAP_SERVICES`. See the [Bind a Service](#) section of the *Delivering Service Credentials to an Application* topic.

## Describing Multiple Applications with One Manifest

You can deploy multiple applications with one `cf push` command by describing the apps in a single manifest.

Suppose you want to deploy two applications called respectively spark and flame, and you want Cloud Foundry to create and start spark before flame. You accomplish this by listing spark first in the manifest.

In this situation there are two sets of bits that you want to push. Let's say that they are `spark.rb` in the spark directory and `flame.rb` in the flame directory. One level up, the `fireplace` directory contains the spark and the flame directories along with the `manifest.yml` file. Your plan is to run the cf CLI from the `fireplace` directory, where you know it can find the manifest.

Now that you have changed the directory structure and manifest location, `cf push` can no longer find your applications by its default behavior of looking in the current working directory. How can you ensure that `cf push` finds the bits you want to push?

The answer is to add a path line to each application description to lead `cf push` to the correct bits. Assume that `cf push` is run from the `fireplace` directory.

For `spark`:

```

...
path: ./spark/
```

For `flame`:

```

...
path: ./flame/
```

The manifest now consists of two applications blocks.

```

this manifest deploys two applications
apps are in flame and spark directories
flame and spark are in fireplace
cf push should be run from fireplace
applications:
- name: spark
 memory: 1G
 instances: 2
 host: flint-99
 domain: shared-domain.example.com
 path: ./spark/
 services:
 - mysql-flint-99
- name: flame
 memory: 1G
 instances: 2
 host: burnin-77
 domain: shared-domain.example.com
 path: ./flame/
 services:
 - redis-burnin-77
```

Follow these general rules when using a multiple-application manifest:

- Name and completely describe your applications in the manifest.
- Use a `no-route` line in the description of any application that provides background services to another application.
- Do not provide an application name with `cf push`.




- Do not use any command line options with `cf push`.

There are only two narrow exceptions:

- If your manifest is not named `manifest.yml` or not in the current working directory, use the `-f` command line option.
- If you want to push a single application rather than all of the applications described in the manifest, provide the desired application name by running `cf push my-app`.

## Minimizing Duplication

 **Note:** Top-level attributes have been deprecated in favor of YAML anchors. For more information, see [Deprecated App Manifest Features](#).

In manifests where multiple applications share settings or services, you may see duplicated content. While the manifests still work, duplication increases the risk of typographical errors, which cause deployments to fail.

You can declare shared configuration using a YAML anchor, which the manifest refers to in app declarations by using an alias.

```

defaults: &defaults
 buildpack: staticfile_buildpack
 memory: 1G

applications:
- name: bigapp
 <<: *defaults
- name: smallapp
 <<: *defaults
 memory: 256M
```

This manifest pushes two apps, smallapp and bigapp, with the staticfile buildpack but with 256M memory for smallapp and 1G for bigapp.

## Variable Substitution

Variable substitution replaces [Inheritance](#), which has been deprecated.

Value substitution allow app developers to create app manifests with values shared across all applicable environments in combination with references to environment-specific differences defined in separate files. In addition, using variable substitution enables developers to store sensitive data in a separate file that the app manifest would reference, making the security sensitive data easier to manage and keep secure.

To utilize this feature, your app manifest requires an explicit declaration that the app or app configuration requires additional data. Use template variables in parentheses in your app manifest in place of fixed values.

For example:

```

applications:
- name: test-app
 instances: ((instances))
 memory: ((memory))
 buildpacks: go_buildpack
 env:
 GOPACKAGENAME: go_calls_ruby
 command: go_calls_ruby
```

The variable substitution file should have corresponding attribute values:

```
instances: 2
memory: 1G
```

The cf CLI replaces the variables in the app manifest with the specified values and proceeds with the push process as usual.

For example:

```
$ cf push foo-app -f ~/workspace/var_manifest.yml --vars-file ~/workspace/vars.yml
Pushing from manifest to org My-Org / space lessing as jdoe@pivotal.io...
Using manifest file /Users/jdoe/workspace/var_manifest.yml
Getting app info...
Creating app with these attributes...
+ name: foo-app
 path: /Users/jdoe/workspace/cf-acceptance-tests/assets/dora
+ instances: 2
+ memory: 1G
 routes:
+ foo-app.cfapps.io
...
```

Template variables can also be used as partial values. Starting with the following manifest.yml:

```

applications:
- name: ((app-name))
 instances: ((instances))
 env:
 ((env-key)): ((env-val))
 routes:
 - route: ((host)).env.com
```

and a secrets.yml variable file:

```

app-name: test-app
instances: 2
env-key: HIDDEN
env-val: HIDDEN
host: test
```

When you do a push invoking both files above, the partial value for `routes` in the manifest.yml is replaced by `host` in the variables.yml file.

```
$ cf push -f manifest.yml --vars-file secrets.yml
Pushing from manifest to org system / space maspace as admin...
Using manifest file manifest.yml
Getting app info...
Creating app with these attributes...
+ name: test-app
 path: /home/pivotal/go/src/github.com/cloudfoundry/cf-acceptance-tests/assets/dora
+ instances: 2
 env:
+ HIDDEN
 routes:
+ test.env.com
Creating app test-app...
```

## Deprecated App Manifest Features

These app manifest features have been deprecated in favor of other options, as described below.

**⚠ warning:** Running `cf push app -f manifest.yml` fails if your manifest uses any of these deprecated features along with the feature that replaces it.

## YAML Anchors Replace Top-Level Attributes

Previously, you could declare top-level attributes, also known as global attributes. For example, you could move an attribute above the `applications` block, where it need appear only once.

The following example illustrates how this was used to manage duplicated settings.

```

all applications use these settings and services
domain: shared-domain.example.com
memory: 1G
instances: 1
```

```
services:
- clockwork-mysql
applications:
- name: springtock
 host: tock09876
 path: ./spring-music/build/libs/spring-music.war
- name: springtick
 host: tick09875
 path: ./spring-music/build/libs/spring-music.war
```

Now, you can use YAML aliases instead.

The following example illustrates how to declare shared configuration using a YAML anchor, which the manifest refers to in app declarations by using an alias.

```

defaults: &defaults
 buildpack: staticfile_buildpack
 memory: 1G

applications:
- name: bigapp
 <<: *defaults
- name: smallapp
 <<: *defaults
 memory: 256M
```

When pushing the app, make explicit the attributes in each app's declaration. To do this, assign the anchors and include the app-level attributes with YAML aliases in each app declaration.

## Attribute routes Replaces domain, domains, host, hosts, and no-hostname

Previously, you could specify routes by listing them all at once using the `routes` attribute, or by using their hosts and domains as shown below.

```

applications
- name: webapp
 host: www
 domains:
 - example.com
 - example.io
```

The following route component attributes have been deprecated:

- `domain`
- `domains`
- `host`
- `hosts`
- `no-hostname`

Now you can only specify routes by using the `routes` attribute:

```

applications
- name: webapp
 routes:
 - route: www.example.com/foo
 - route: tcp.example.com:1234
```

This app manifest feature has been deprecated, and a replacement option is under consideration.

## Inheritance

This feature has been deprecated, and has been replaced by [Variable Substitution](#).

With inheritance, child manifests inherited configurations from a parent manifest, and the child manifests could use inherited configurations as provided,

extend them, or override them.

## Deploy an App with Docker

Page last updated:

This topic describes how to use the [Cloud Foundry Command Line Interface \(cf CLI\)](#) to push an app with a new or updated Docker image. Cloud Foundry then uses the Docker image to create containers for the app.

See [Using Docker in Cloud Foundry](#) in the Cloud Foundry documentation for an explanation of how Docker works in Cloud Foundry.

## Requirements

To push apps with Docker, you need the following:

- A Cloud Foundry deployment that has Docker support enabled. To enable Docker support, see the [Enable Docker](#) section of *Using Docker in Cloud Foundry* in the Cloud Foundry documentation.
- A Docker image that meets the following requirements:
  - The Docker image must contain an `/etc/passwd` file with an entry for the `root` user. In addition, the home directory and the shell for that `root` user must be present in the image file system.
  - The total size of the Docker image file system layers must not exceed the disk quota for the app. The maximum disk allocation for apps is set by the Cloud Controller. The default maximum disk quota is 2048 MB per app.



**Note:** If the total size of the Docker image file system layers exceeds the disk quota, the app instances do not start.

- The location of the Docker image on [Docker Hub](#) or another Docker registry.
- A registry that supports the [Docker Registry HTTP API V2](#) and presents a valid certificate for HTTPS traffic.

## Requirement for cf ssh Support

If you want to log in to your app container using the `cf ssh` command, you must make a shell such as `sh` or `bash` available in the container.

The SSH server in the container looks for the following executables in absolute locations or the `PATH` environment variable:

- `/bin/bash`
- `/usr/local/bin/bash`
- `/bin/sh`
- `bash`
- `sh`

## Benefits of Specifying Tags

If you want your app container to be consistent after platform updates and code changes, specify a tag when you push your Docker image. Otherwise, the platform applies the `latest` tag without respecting changes to `PORT` or `ENTRYPOINT`.

If you push your Docker image without specifying a tag, you must run `cf restage` for the changes to take effect.

## Port Configuration

By default, apps listen for connections on the port specified in the `PORT` environment variable for the app. Cloud Foundry allocates this value dynamically.

When configuring a Docker image for Cloud Foundry, you can control the exposed port and the corresponding value of `PORT` by specifying the `EXPOSE` directive in the image Dockerfile. If you specify the `EXPOSE` directive, then the corresponding app pushed to Cloud Foundry listens on that exposed port. For example, if you set `EXPOSE` to `7070`, then the app listens for connections on port 7070.

If you do not specify a port in the `EXPOSE` directive, then the app listens on the value of the `PORT` environment variable as determined by Cloud Foundry.

If you set the `PORT` environment variable via an `ENV` directive in a Dockerfile, Cloud Foundry overrides the value with the system-determined value.

Cloud Foundry supports only one exposed port on the image.

## Start Command

By default, Docker uses the start command specified in the Docker image. You can override the start command either by using a command-line parameter or by specifying it in a manifest file.

For more information about command-line parameters for `docker start`, see [docker start](#) in the Docker Documentation.

## Push a Docker Image From Docker Hub

To deploy a Docker image from a Docker Hub repository, run `cf push APP-NAME --docker-image REPO/IMAGE:TAG`. Replace the placeholder values in the command as follows:

- `APP-NAME`: The name of the app being pushed
- `REPO`: The name of the repository where the image is stored
- `IMAGE`: The name of an image from Docker Hub
- `TAG`: (Optional, but recommended) The tag or version for the image

For example, the following command pushes the `my-image` image from Docker Hub to a Cloud Foundry app:

```
$ cf push my-app --docker-image cloudfoundry/my-image
```

## Push a Docker Image from a Private Registry

As an alternative to Docker Hub, you can use any Docker image registry that presents a valid certificate for HTTPS traffic, such as a company-internal Docker registry.

To deploy a Docker image using a specified Docker registry, run `cf push APP-NAME --docker-image MY-PRIVATE-REGISTRY.DOMAIN:PORT/REPO/IMAGE:TAG`.

Replace the placeholder values in the command as follows:

- `APP-NAME`: The name of the app being pushed
- `MY-PRIVATE-REGISTRY.DOMAIN`: The path to the Docker registry
- `PORT`: The port where the registry serves traffic
- `REPO`: The name of the repository where the image is stored
- `IMAGE`: The name of the image being pushed
- `TAG`: (Optional, but recommended) The tag or version for the image

For example, the following command pushes the `v2` version of the `my-image` image from the `my-repo` repository of the `internal-registry.example.com` registry on port `5000`:

```
$ cf push my-app --docker-image internal-registry.example.com:5000/my-repo/my-image:v2
```

## Push a Docker Image From a Registry with Authentication

Many Docker registries control access to Docker images by authenticating with a username and password. Follow the steps below to deploy a Docker image with registry authentication:

1. Make sure the `CF_DOCKER_PASSWORD` environment variable is set to the Docker registry user password.

2. Run the following command:

```
$ CF_DOCKER_PASSWORD=YOUR-PASSWORD cf push APP-NAME --docker-image REPO/IMAGE:TAG --docker-username USER
```

Replace the placeholder values in the command as follows:

- `YOUR-PASSWORD` : The password to use for authentication with the registry
- `APP-NAME` : The name of the app being pushed
- `REPO` : The repository where the image is stored:
  - For Docker Hub, this is just the repository name
  - For a private registry, this includes the registry address and port, as described in [Push a Docker Image from a Private Registry](#), in the format: `MY-PRIVATE-REGISTRY.DOMAIN:PORT/REPO`
- `IMAGE` : The name of the image being pushed
- `TAG` : (Optional, but recommended) The tag or version for the image
- `USER` : The username to use for authentication with the registry

## Push a Docker Image From Google Container Registry (GCR)

PCF supports pushing apps from images hosted on Google Container Registry (GCR) service. This feature requires that you use [json\\_key based authentication](#).

### Step 1: Authenticate with GCR

To authenticate with GCR using PCF, you must create a JSON key file and associate it with your project:

1. Create a GCP service account. See [Creating and Enabling Service Accounts for Instances](#).

```
$ gcloud iam service-accounts create MY-ACCOUNT --display-name "MY DISPLAY NAME"
```

2. Create a JSON key file and associate it with the service account:

```
$ gcloud iam service-accounts keys create key.json --iam-account=MY-ACCOUNT@MY-PROJECT-ID.iam.gserviceaccount.com
```

3. Set your project ID:

```
$ gcloud config set project MY-PROJECT-ID
```

4. Add the IAM policy binding for your project and service account:

```
gcloud projects add-iam-policy-binding MY-PROJECT --member serviceAccount:MY-ACCOUNT@MY-PROJECT-ID.iam.gserviceaccount.com --role roles/storage.objectViewer
```


### Step 2: Deploy the GCP Image


Run the following command to deploy your GCR image using the cf CLI:

```
CF_DOCKER_PASSWORD="$(cat key.json)" cf push APP-NAME --docker-image docker://MY-REGISTRY-URL/MY-PROJECT/MY-IMAGE-NAME --docker-username _json_key
```

Replace the placeholder values in the command as follows:

- `APP-NAME` : The name of the app being pushed
- `MY-REGISTRY-URL` : The URL of your registry
- `MY-PROJECT` : The name of your project
- `MY-IMAGE-NAME` : The name of your image

 **Note:** The `key.json` file must point to the file you created in the previous step.

 **Note:** For information about specifying `MY-REGISTRY-URL`, see [Pushing and Pulling Images](#) on the Google Cloud documentation.

## Docker Volume Support

You can use volume services with Docker apps. For more information about enabling volume support, see the [Using an External File System \(Volume Services\)](#) topic.



## Deploying a Large Application

Page last updated:


This topic describes constraints and recommended settings for deploying applications above 750 MB.

### Deployment Considerations and Limitations

The deployment process involves uploading, staging, and starting the app. See the [Deployment](#) section of the Application Container Lifecycle topic for more information about the default time limits for uploading, staging, and starting an app.


To deploy large apps to PAS, ensure the following:

- The total size of the files to upload for your app does not exceed the maximum app file size that an admin sets in **Ops Manager > PAS > Application Developer Controls**.
- Your network connection speed is sufficient to upload your app within the 15 minute limit. We recommend a minimum speed of 874 KB/s.

 **Note:** PAS provides an authorization token that is valid for a minimum of 20 minutes.

- You allocate enough memory for all instances of your app. Use either the `-m` flag with `cf push` or set an app memory value in your `manifest.yml` file.
- You allocate enough disk space for all instances of your app. Use either the `-k` flag with `cf push` or set a disk space allocation value in your `manifest.yml` file.
- If you use an app manifest file, `manifest.yml`, be sure to specify adequate values for your app for attributes such as app memory, app start timeout, and disk space allocation.  
For more information about using manifests, refer to the [Deploying with Application Manifests](#) topic.
- You push only the files that are necessary for your application.  
To meet this requirement, push only the directory for your application, and remove unneeded files or use the `.cfignore` file to [specify excluded files](#).
- You configure Cloud Foundry Command Line Interface (cf CLI) staging, startup, and timeout settings to override settings in the manifest, as necessary.
  - `CF_STAGING_TIMEOUT`: Controls the maximum time that the cf CLI waits for an app to stage after Cloud Foundry successfully uploads and packages the app. Value set in minutes.
  - `CF_STARTUP_TIMEOUT`: Controls the maximum time that the cf CLI waits for an app to start. Value set in minutes.
  - `cf push -t TIMEOUT`: Controls the maximum time that Cloud Foundry allows to elapse between starting an app and the first healthy response from the app. When you use this flag, the cf CLI ignores any app start timeout value set in the manifest. Value set in seconds.

For more information about using the cf CLI to deploy apps, refer to the [Push section](#) of the *Getting Started with the cf CLI* topic.

 **Note:** Changing the timeout setting for the cf CLI does not change the timeout limit for Cloud Foundry server-side jobs such as staging or starting applications. You must change server-side timeouts in the manifest. Because of the differences between the Cloud Foundry and cf CLI timeout values, your app might successfully start even though the cf CLI reports `App failed`. Run `cf apps APP_NAME` to review the actual status of your app.

### Default Settings and Limitations Summary Table

This table provides summary information of constraints and default settings to consider when you deploy a large app to PAS.

| Setting                          | Note                                                                            |
|----------------------------------|---------------------------------------------------------------------------------|
| App Package Size                 | Maximum: Set in <b>Ops Manager &gt; PAS &gt; Application Developer Controls</b> |
| Authorization Token Grace Period | Default: 20 minutes, minimum                                                    |
| <code>CF_STAGING_TIMEOUT</code>  | cf CLI environment variable<br>Default: 15 minutes                              |
| <code>CF_STARTUP_TIMEOUT</code>  | cf CLI environment variable<br>Default: 5 minutes                               |
| <code>cf push -t TIMEOUT</code>  | App start timeout maximum<br>Default: 60 seconds                                |
| Disk Space Allocation            | Default: 1024 MB                                                                |
| Internet Connection Speed        | Recommended Minimum: 874 KB/s                                                   |

| Internet Connection Speed | Recommended Minimum: 0.7 Mbps |
|---------------------------|-------------------------------|
|---------------------------|-------------------------------|

## Starting, Restarting, and Restaging Applications

Page last updated:

This topic describes how to start, restart, and restage applications in Cloud Foundry.

### Start Your Application

To start your application, run the following command from your application root directory:

```
$ cf push YOUR-APP
```

For more information about deploying applications, see the [Deploy an Application](#) topic.

Cloud Foundry determines the start command for your application from one of the three following sources:

- The `-c` command-line option in the Cloud Foundry Command Line Interface (cf CLI). See the following example:

```
$ cf push YOUR-APP -c "node YOUR-APP.js"
```

- The `command` attribute in the application manifest. See the following example:  
`command: node YOUR-APP.js`
- The buildpack, which provides a start command appropriate for a particular type of application.

The source that Cloud Foundry uses depends on factors explained below.

### How Cloud Foundry Determines its Default Start Command

The first time you deploy an application, `cf push` uses the buildpack start command by default. After that, `cf push` defaults to whatever start command was used for the previous push.

To override these defaults, provide the `-c` option, or the `command` attribute in the manifest. When you provide start commands both at the command line and in the manifest, `cf push` ignores the command in the manifest.

### Forcing Cloud Foundry To Use the Buildpack Start Command

To force Cloud Foundry to use the buildpack start command, specify a start command of `null`.

You can specify a null start command in one of two ways.

- Using the `-c` command-line option in the cf CLI:

```
$ cf push YOUR-APP -c "null"
```

- Using the `command` attribute in the application manifest:  
`command: null`

This can be helpful after you have deployed while providing a start command at the command line or the manifest. At this point, a command that you provided, rather than the buildpack start command, has become the default start command. In this situation, if you decide to deploy using the buildpack start command, the `null` command makes that easy.

### Start Commands When Migrating a Database

Start commands are used in special ways when you migrate a database as part of an application deployment. For more information, see [Services Overview](#).

## Restart Your Application

To restart your application, run the following command:

```
$ cf restart YOUR-APP
```

Restarting your application stops your application and restarts it with the already compiled droplet. A droplet is a tarball that includes:

- stack
- [buildpack](#) [↗](#)
- application source code

The Diego [cell](#) [↗](#) unpacks, compiles, and runs a droplet on a container.

Restart your application to refresh the application's environment after actions such as binding a new service to the application or setting an environment variable that only the application consumes. However, if your environment variable is consumed by the buildpack in addition to the application, then you must [restage](#) the application for the change to take effect.

## Restage Your Application

To restage your application, run the following command:

```
$ cf restage YOUR-APP
```


Restaging your application stops your application and restages it, by compiling a new droplet and starting it.

Restage your application if you have changed the environment in a way that affects your staging process, such as setting an environment variable that the buildpack consumes. The staging process has access to environment variables, so the environment can affect the contents of the droplet.

Restaging your application compiles a new droplet from your application without updating your application source. If you must update your application source, re-push your application by following the steps in the section [above](#).

## Pushing an App with Multiple Processes (Beta)

This topic describes how to push and manage apps with multiple processes.

 **Note:** This is a beta feature. Because the CLI may change, this feature is not recommended for use in scripts until it is generally available.

### About Processes


The CAPI v3 API supports using a single command to push apps that run multiple processes, such as a web app that has a UI process and a worker process. To push an app that creates multiple processes from the same codebase, you first define its processes in a Procfile. See [Push an App with Multiple Processes](#).

For more information about processes, see the [Processes](#) section of the CAPI v3 documentation.

## Push an App with Multiple Processes

You can push an app with multiple processes using a Procfile. Follow the procedure below.

1. Create a file named `Procfile` in the root of your app directory.

 **Note** For more information about Procfiles, see the [Procfiles](#) section of the CAPI v3 documentation.

2. Add each process and its start command to the Procfile. See the following example:

```
web: bundle exec rackup config.ru -p $PORT
worker: bundle exec rake worker:start
```

3. Run the `v3-push` command:

```
cf v3-push myapp
```

By default, the web process has a route and one instance. Other processes have zero instances by default.

### Scale a Process

To scale an app process, run the following command:

```
cf v3-scale APP-NAME --process PROCESS-NAME -i INSTANCE-COUNT
```

### View Processes

To view the processes running as part of an app, run `cf APP-NAME`. See the following example in which the app has a `web` and a `worker` process.

```
$ cf v3-app myapp
Showing health and status for app myapp in org test / space test as admin...
```

```
name: myapp
requested state: started
processes: web:1/1, worker:2/2
memory usage: 256M x 1, 256M x 2
routes: myapp.cloudfoundry.example.com
stack: cflinuxfs2
buildpacks: ruby
```

```
web:1/1
state since cpu memory disk
#0 running 2017-09-25 15:43:26 PM 0.2% 18.9M of 256M 84.4M of 1G
```

```
worker:2/2
state since cpu memory disk
#0 running 2017-09-25 15:49:46 PM 0.1% 5M of 256M 73M of 1G
#1 running 2017-09-25 15:49:46 PM 0.1% 5M of 256M 73M of 1G
```

## Running cf push Sub-Step Commands (Beta)

This topic describes how to run beta Cloud Foundry Command Line Interface (cf CLI) commands that provide granular control over the `cf push` process. These commands break down the `cf push` process into sub-steps that can run independently.

 **Note:** This is a beta feature. Because the CLI may change, this feature is not recommended for use in scripts until it is generally available.

### Overview

The cf CLI includes commands to provide granular control over app pushes. With these commands, you can choose to perform only some steps of the `cf push` process or perform specific actions between the steps normally executed as part of running `cf push`.

Here are some example use cases for the sub-step commands:

- Updating a third party system before staging an app
- Retrying failed stagings without incurring downtime
- Calling external services to report audit data during push
- Scanning a droplet before deploy
- Integrating with a change request system

To support these custom push workflows, Cloud Foundry divides apps into smaller building blocks. The following table describes these building blocks as *Resources* and lists the command associated with each one.

For information on using these commands, see the [Example Workflows](#) section below.

| Resource | Description                                                                                                                                                                | Command                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| App      | The top-level resource that represents an app and its configuration.<br>For more information, see <a href="#">Apps</a> .                                                   | <code>v3-create-app</code>     |
| Package  | The source code that makes up an app.<br>For more information, see <a href="#">Packages</a> .                                                                              | <code>v3-create-package</code> |
| Build    | The staging process. Creating a build combines a Package with a Buildpack and builds it into an executable resource.<br>For more information, see <a href="#">Builds</a> . | <code>v3-stage</code>          |
| Droplet  | An executable resource that results from a Build.<br>For more information, see <a href="#">Droplet</a> .                                                                   | <code>v3-set-droplet</code>    |

### Example Workflows

The following sections describe example workflows for working with the `cf push` sub-step commands.

#### Push an App Using Sub-Step Commands

This example workflow describes how to push an app using sub-step commands instead of `cf push`.

1. Create your app with the cf CLI:

```
cf v3-create-app MY-APP
```

2. From your app directory, create a package for your app.

```
cf v3-create-package MY-APP
```

3. Locate and copy the `package guid` from the output of the previous step. See the following example output:

```
Uploading and creating bits package for app MY-APP in org test / space test as admin...
package guid: 0dfca85a-8ed4-4f00-90d0-3ab08852dba8
OK
```

4. Stage the package you created:

```
cf v3-stage MY-APP --package-guid PACKAGE-GUID
```

5. Locate and copy the `droplet guid` from the output of the previous step. See the following example output:

```
Staging package for MY-APP in org test / space test as admin...
...
Package staged
droplet guid: f60d3464-415a-4202-9d40-26a70373a487
state: staged
created: Mon 25 Sep 16:37:45 PDT 2018
```

6. Assign the droplet to your app:

```
cf v3-set-droplet MY-APP -d DROPLET-GUID
```

7. Start your app:

```
cf v3-start MY-APP
```

## Roll Back to a Previous Droplet

This example workflow describes how to roll back to a previous droplet used by your app. You may want to use this, for example, if you update your app and it has a bug that causes it to crash.

1. List the droplets for your app:

```
cf v3-droplets MY-APP
```

2. From the output, locate and copy the second-to-last GUID. In the following example, this is `66524145-5502-40e6-b782-47fe68e13c49`.

```
Listing droplets of app MY-APP in org test / space test as admin...

guid state created
66524145-5502-40e6-b782-47fe68e13c49 staged Mon 25 Sep 16:37:34 PDT 2018
0677ad93-9f77-4aaa-9a6b-44da022dcd58 staged Mon 25 Sep 16:44:55 PDT 2018
```

3. Stop your app:

```
cf v3-stop MY-APP
```

4. Set the app to use the previous droplet:

```
cf v3-set-droplet MY-APP -d PREVIOUS-DROPLET-GUID
```

5. Start your app:

```
cf v3-start MY-APP
```



## Using Blue-Green Deployment to Reduce Downtime and Risk

Page last updated:

Blue-green deployment is a technique that reduces downtime and risk by running two identical production environments called Blue and Green.

At any time, only one of the environments is live, with the live environment serving all production traffic. For this example, Blue is currently live and Green is idle.

As you prepare a new version of your software, deployment and the final stage of testing takes place in the environment that *isn't* live: in this example, Green. Once you have deployed and fully tested the software in Green, you switch the router so all incoming requests now go to Green instead of Blue. Green is now live, and Blue is idle.

This technique can eliminate downtime due to application deployment. In addition, blue-green deployment reduces risk: if something unexpected happens with your new version on Green, you can immediately roll back to the last version by switching back to Blue.

**Note:** If your app uses a relational database, blue-green deployment can lead to discrepancies between your Green and Blue databases during an update. To maximize data integrity, configure a single database for backward and forward compatibility.

**Note:** You can adjust the route mapping pattern to display a static maintenance page during a maintenance window for time-consuming tasks, such as migrating a database. In this scenario, the router switches all incoming requests from Blue to Maintenance to Green.

## Blue-Green Deployment with Cloud Foundry Example

For this example, we'll start with a simple application: "demo-time." This app is a web page that displays the words "Blue time" and the date/time on the server.

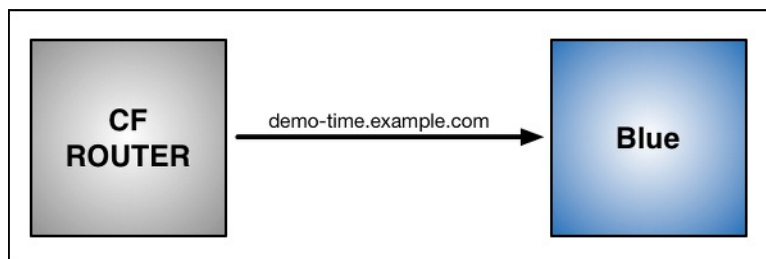
### Step 1: Push an App

Use the Cloud Foundry Command Line Interface (cf CLI) to push the application. Name the application "Blue" with the subdomain "demo-time."

```
$ cf push Blue -n demo-time
```

As shown in the graphic below:

- Blue is now running on Cloud Foundry.
- The CF Router sends all traffic for `demo-time.example.com` traffic to Blue.



### Step 2: Update App and Push

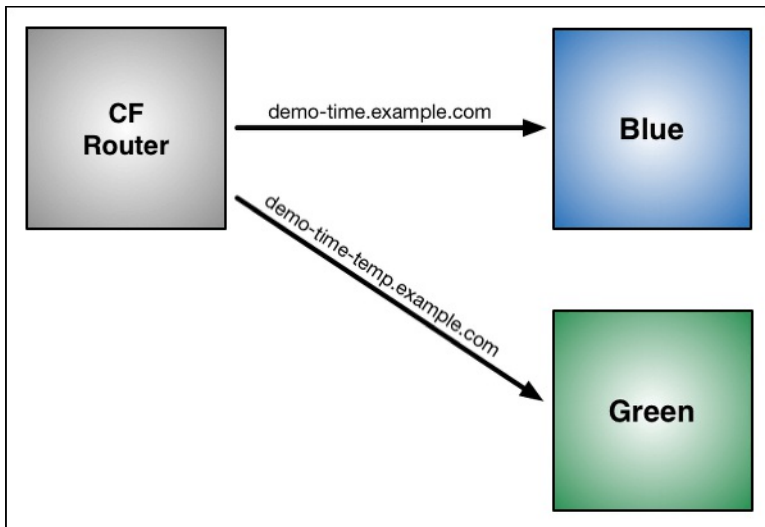
Now make a change to the application. First, replace the word "Blue" on the web page with "Green," then rebuild the source file for the application. Run `cf push` again, but use the name "Green" for the application and provide a different subdomain to create a temporary route:

```
$ cf push Green -n demo-time-temp
```

After this push:

- Two instances of our application are now running on Cloud Foundry: the original Blue and the updated Green.

- The CF Router continues sending all traffic for `demo-time.example.com` to Blue. The router now also sends any traffic for `demo-time-temp.example.com` to Green.



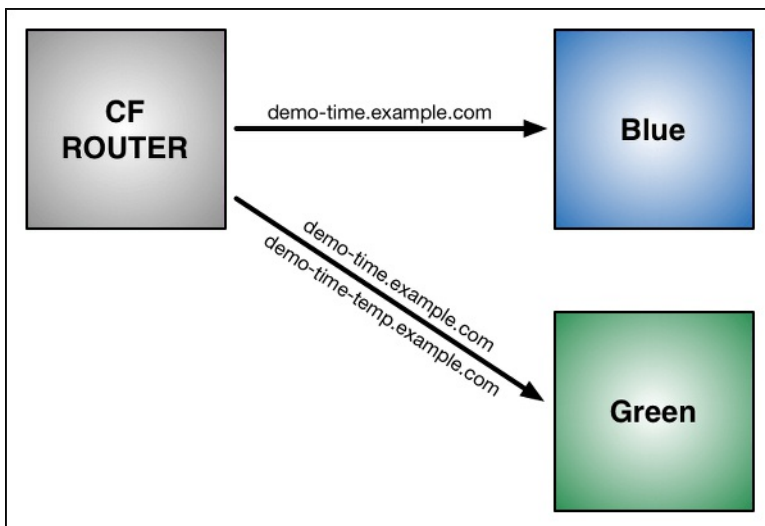
## Step 3: Map Original Route to Green

Now that both apps are up and running, switch the router so all incoming requests go to the Green app *and* the Blue app. Do this by mapping the original URL route (`demo-time.example.com`) to the Green application using the [cf map-route](#) command.

```
$ cf map-route Green example.com -n demo-time
Binding demo-time.example.com to Green... OK
```

After the `cf map-route` command :

- The CF Router continues sending traffic for `demo-time-temp.example.com` to Green.
- Within a few seconds, the CF Router begins load balancing traffic for `demo-time.example.com` between Blue and Green.



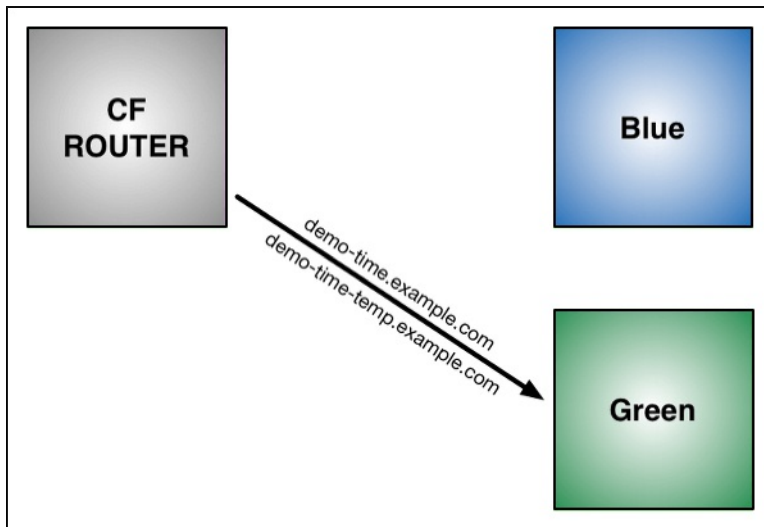
## Step 4: Unmap Route to Blue

Once you verify Green is running as expected, stop routing requests to Blue using the [cf unmap-route](#) command:

```
$ cf unmap-route Blue example.com -n demo-time
Unbinding demo-time.example.com from blue... OK
```

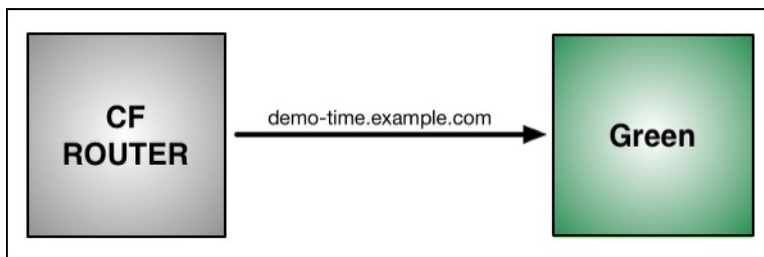
After `cf unmap-route` command:

- The CF Router stops sending traffic to Blue. Now all traffic for `demo-time.example.com` is sent to Green:



## Step 5: Remove Temporary Route to Green

You can now use `cf unmap-route` to remove the route `demo-time-temp.example.com` from Green. The route can be deleted using `cf delete-route` or reserved for later use. You can also decommission Blue, or keep it in case you need to roll back your changes.



## Implementation

Cloud Foundry community members have written a plugin to automate the blue-green deployment process:

- [BlueGreenDeploy](#) [↗](#): `cf-blue-green-deploy` is a plugin, written in Go, for the Cloud Foundry Command Line Interface (cf CLI) that automates a few steps involved in zero-downtime deploys.

## Troubleshooting Application Deployment and Health

Page last updated:

Refer to this topic for help diagnosing and resolving common issues when you deploy and run applications on Cloud Foundry.

### Common Issues

The following sections describe common issues you might encounter when attempting to deploy and run your application, and possible resolutions.

#### cf push Times Out

If your deployment times out during the upload or staging phase, you may receive one of the following error messages:

- `504 Gateway Timeout`
- `Error uploading application`
- `Timed out waiting for async job JOB-NAME to finish`

If this happens, do the following:

- **Check your network speed.** Depending on the size of your application, your `cf push` could be timing out because the upload is taking too long. We recommended an Internet connection speed of at least 768 KB/s (6 Mb/s) for uploads.
- **Make sure you are pushing only needed files.** By default, `cf push` will push all the contents of the current working directory. Make sure you are pushing only the directory for your application. If your application is too large, or if it has many small files, Cloud Foundry may time out during the upload. To reduce the number of files you are pushing, ensure that you push only the directory for your application, and remove unneeded files or use the `.cfignore` file to [specify excluded files](#).
- **Set the `CF_STAGING_TIMEOUT` and `CF_STARTUP_TIMEOUT` environment variables.** By default your app has 15 minutes to stage and 5 minutes to start. You can increase these times by setting `CF_STAGING_TIMEOUT` and `CF_STARTUP_TIMEOUT`. Type `cf push -h` at the command line for more information.
- **If your app contains a large number of files, try pushing the app repeatedly.** Each push uploads a few more files. Eventually, all files have uploaded and the push succeeds. This is less likely to work if your app has many small files.

#### App Too Large

If your application is too large, you may receive one of the following error messages on `cf push`:

- `413 Request Entity Too Large`
- `You have exceeded your organization's memory limit`

If this happens, do the following:

- **Make sure your org has enough memory for all instances of your app.** You will not be able to use more memory than is allocated for your organization. To view the memory quota for your org, use `cf org ORG_NAME`.  
Your total memory usage is the sum of the memory used by all applications in all spaces within the org. Each application's memory usage is the memory allocated to it multiplied by the number of instances. To view the memory usage of all the apps in a space, use `cf apps`.
- **Make sure your application is less than 1 GB.** By default, Cloud Foundry deploys all the contents of the current working directory. To reduce the number of files you are pushing, ensure that you push only the directory for your application, and remove unneeded files or use the `.cfignore` file to [specify excluded files](#). The following limits apply:
  - The app files to push cannot exceed 1 GB.
  - The droplet that results from compiling those files cannot exceed 1.5 GB. Droplets are typically a third larger than the pushed files.
  - The combined size of the app files, compiled droplet, and buildpack cache cannot total more than 4 GB of space during staging.

#### Unable to Detect a Supported Application Type

If Cloud Foundry cannot [identify an appropriate buildpack](#) for your app, you will see an error message that states

```
Unable to detect a supported application
type
```

You can view what buildpacks are available with the `cf buildpacks` command.

If you see a buildpack that you believe should support your app, refer to the [buildpack documentation](#) for details about how that buildpack detects applications it supports.

If you do not see a buildpack for your app, you may still be able to push your application with a [custom buildpack](#) using `cf push -b` with a path to your buildpack.

## App Deploy Fails

Even when the deploy fails, the app might exist on PAS. Run `cf apps` to review the apps in the currently targeted org and space. You might be able to correct the issue using the CLI or [Apps Manager](#), or you might have to delete the app and redeploy.

Common reasons deploying an app fails include the following:

- You did not successfully create and bind a needed service instance to the app, such as a PostgreSQL or MongoDB service instance. Refer to Step 3: Create and Bind a Service Instance for a RoR Application.
- You did not successfully create a unique URL for the app. Refer to the troubleshooting tip App Requires Unique URL.

## App Requires Unique URL

PAS requires that each app that you deploy has a unique URL. Otherwise, the new app URL collides with an existing app URL and PAS cannot successfully deploy the app. You can resolve this issue by running `cf push` with either of the following flags to create a unique URL:

- `-n` to assign a different HOST name for the app.
- `--random-route` to create a URL that includes the app name and random words. Using this option might create a long URL, depending on the number of words that the app name includes.

## App Fails to Start

After `cf push` stages the app and uploads the droplet, the app may fail to start, commonly with a pattern of starting and crashing similar to the following example:

```
-----> Uploading droplet (23M)
...
0 of 1 instances running, 1 starting
0 of 1 instances running, 1 down
...
0 of 1 instances running, 1 failing
FAILED
Start unsuccessful
```

If this happens, try the following:

- **Find the reason app is failing and modify your code.** Run `cf events APP-NAME` and `cf logs APP-NAME --recent` and look for messages similar to this:

```
2018-07-20T15:53:26.00-0700 app.crash app-name index: 2, reason: CRASHED, cell_id: d874ad05-d0ca-4c63-9f5a-0b1ddd90dd5d, instance: f406c53e-b1ca-4a0f-6140-dddd, e
```

These messages may identify a memory or port issue. If they do, take that as a starting point when you re-examine and fix your application code.

- **Make sure your application code uses the `PORT` environment variable.** Your application may be failing because it is listening on the wrong port. Instead of hard coding the port on which your application listens, use the `PORT` environment variable. For example, this Ruby snippet assigns the port value to the `listen_here` variable: `listen_here = ENV['PORT']`. For more examples specific to your application framework, see the appropriate [buildpacks documentation](#) for your app's language.
- **Make sure your app adheres to the principles of the [Twelve-Factor App](#) and [Prepare to Deploy an Application](#).** These texts explain how to prevent situations where your app builds locally but fails to build in the cloud.
- **Verify the timeout configuration of your app.** Application health checks use a timeout setting when an app starts up for the first time. See [Using Application Health Checks](#). If an application fails to start up due to health check timeout, you might see messages in the logs similar to the following:

```

2017-01-30T14:07:20.39-0800 [CELL/0] OUT Creating container
2017-01-30T14:07:20.65-0800 [CELL/0] OUT Successfully created container
2017-01-30T14:07:22.30-0800 [CELL/0] OUT Starting health monitoring of container
2017-01-30T14:08:23.52-0800 [CELL/0] ERR Timed out after 1m0s:
health check never passed.
2017-01-30T14:08:23.57-0800 [CELL/0] OUT Destroying container
2017-01-30T14:08:23.59-0800 [API/0] OUT Process has crashed with type: "web"
2017-01-30T14:08:23.59-0800 [CELL/0] OUT Creating container
2017-01-30T14:08:23.60-0800 [API/0] OUT App instance exited with guid 91086440-bac0-44f0-808f-a034a1ec2ed0
payload: {"instance"=>"", "index"=>0, "reason"=>"CRASHED",
"exit_description"=>"2 error(s) occurred:\n\n* 1 error(s)
occurred:\n\n* Exited with status 6\n* 2 error(s)
occurred:\n\n* cancelled\n* cancelled", "crash_count"=>1,
"crash_timestamp"=>1485814103565763172,
"version"=>"3e6e4232-7e19-4168-9583-1176833d2c71"}
2017-01-30T14:08:23.83-0800 [CELL/0] OUT Successfully destroyed container
2017-01-30T14:08:23.84-0800 [CELL/0] OUT Successfully created container
2017-01-30T14:08:25.41-0800 [CELL/0] OUT Starting health monitoring of container

```

## App consumes too much memory, then crashes

An app that `cf push` has uploaded and started can crash later if it uses too much memory.

**Make sure your app is not consuming more memory than it should.** When you ran `cf push` and `cf scale`, that configured a limit on the amount of memory your app should use. Check your app's actual memory usage. If it exceeds the limit, modify the app to use less memory.

## Routing Conflict

PAS allows multiple apps, or versions of the same app, to be mapped to the same route. This feature enables Blue-Green deployment. For more information see [Using Blue-Green Deployment to Reduce Downtime and Risk](#).

Routing multiple apps to the same route may cause undesirable behavior in some situations by routing incoming requests randomly to one of the apps on the shared route.

If you suspect a routing conflict, run `cf routes` to check the routes in your installation.

If two apps share a route outside of a Blue-Green deploy strategy, choose one app to re-assign to a different route and follow the procedure below:

1. Run `cf unmap-route YOUR-APP-NAME OLD-ROUTE` to remove the existing route from that app.
2. Run `cf map-route YOUR-APP-NAME NEW-ROUTE` to map the app to a new, unique route.

## Gather Diagnostic Information

Use the techniques in this section to gather diagnostic information and troubleshoot app deployment issues.

## Examine Environment Variables

`cf push` deploys your application to a container on the server. The environment variables in the container govern your application.

You can set environment variables in a manifest created before you deploy. See [Deploying with Application Manifests](#).

You can also set an environment variable with a `cf set-env` command followed by a `cf push` command. You must run `cf push` for the variable to take effect in the container environment.

Use the `cf env` command to view the environment variables that you have set using the `cf set-env` command and the variables in the container environment:

```
$ cf env my-app
Getting env variables for app my-app in org My-Org / space development as admin...
OK
```

System-Provided:

```
{
 "VCAP_SERVICES": {
 "p-mysql-n/a": [
 {
 "credentials": {
 "uri": "postgres://lrra:e6B-X@p-mysqlprovider.example.com:5432/lrra"
 },
 "label": "p-mysql-n/a",
 "name": "p-mysql",
 "syslog_drain_url": "",
 "tags": ["postgres", "postgresql", "relational"]
 }
]
 }
}
```


User-Provided:

```
my-env-var: 100
my-drain: http://drain.example.com
```

## View Logs

To view app logs streamed in real-time, use the `cf logs APP-NAME` command.

To aggregate your app logs to view log history, bind your app to a syslog drain service. For more information, see [Streaming Application Logs to Log Management Services](#).

 **Note:** The Diego architecture does not support the `cf files` command.

## Trace Cloud Controller REST API Calls

If a command fails or produces unexpected results, re-run it with HTTP tracing enabled to view requests and responses between the Cloud Foundry Command Line Interface (cf CLI) and the Cloud Controller REST API.


For example:

- Re-run `cf push` with `-v`:  
`cf push APP-NAME -v`
- Re-run `cf push` while appending API request diagnostics to a log file:  
`CF_TRACE=PATH-TO-TRACE.LOG cf push APP-NAME`

These examples enable HTTP tracing for a single command only. To enable it for an entire shell session, set the variable first:

```
export
CF_TRACE=true
```

```
export CF_TRACE=PATH-TO-TRACE.LOG
```

 **Note:** `CF_TRACE` is a local environment variable that modifies the behavior of the cf CLI. Do not confuse `CF_TRACE` with the [variables in the container environment](#) where your apps run.

## Analyze Zipkin Trace IDs

When the Zipkin feature is enabled in Cloud Foundry, the Gorouter adds or forwards Zipkin trace IDs and span IDs to HTTP headers. For more information about what the Gorouter provides in the HTTP header, see the [HTTP Headers](#) section of the *HTTP Routing* topic.

After adding Zipkin HTTP headers to app logs, developers can use `cf logs myapp` to correlate the trace and span ids logged by the Gorouter with the trace


ids logged by their app. To correlate trace ids for a request through multiple apps, each app must forward appropriate values for the headers with requests to other applications.

## Use Troubleshooting Commands


You can investigate app deployment and health using the cf CLI.

Some cf CLI commands may return connection credentials. Remove credentials and other sensitive information from command output before you post the output a public forum.

- `cf apps` : Returns a list of the applications deployed to the current space with deployment options, including the name, current state, number of instances, memory and disk allocations, and URLs of each application.
- `cf app APP-NAME` : Returns the health and status of each instance of a specific application in the current space, including instance ID number, current state, how long it has been running, and how much CPU, memory, and disk it is using.

 **Note:** CPU values returned by `cf app` show the total usage of each app instance on all CPU cores on a host VM, where each core contributes 100%. For example, the CPU of a single-threaded app instance on a Diego cell with one core cannot exceed 100%, and four instances sharing the cell cannot exceed an average CPU of 25%. A multi-threaded app instance running alone on a cell with eight cores can draw up to 800% CPU.

- `cf env APP-NAME` : Returns environment variables set using `cf set-env` and variables existing in the container environment.
- `cf events APP-NAME` : Returns information about application crashes, including error codes. Shows that an app instance exited. For more detail, look in the application logs. See <https://github.com/cloudfoundry/errors> for a list of Cloud Foundry errors.
- `cf logs APP-NAME --recent` : Dumps recent logs. See [Viewing Logs in the Command Line Interface](#).
- `cf logs APP-NAME` : Returns a real-time stream of the application STDOUT and STDERR. Use **Ctrl-C** (^C) to exit the real-time stream.
- `cf files APP-NAME` : Lists the files in an application directory. Given a path to a file, outputs the contents of that file. Given a path to a subdirectory, lists the files within. Use this to [explore](#) individual logs.

 **Note:** Your application should direct its logs to STDOUT and STDERR. The `cf logs` command also returns messages from any [log4j](#) facility that you configure to send logs to STDOUT.

## Access Apps with SSH

If you need to troubleshoot an instance of an app, you can gain SSH access to the app with the SSH proxy and daemon. See the [Application SSH Overview](#) topic for more information.

## Send Requests to App Instance

To obtain debug data without SSH, you can make HTTP requests to a specific instance of an app by using the `X-CF-APP-INSTANCE` HTTP header. See the [App Instance Routing](#) section of the *HTTP Routing* topic for more information.



## SSH for Apps and Services

The following list provides information about configuring and using SSH for apps and services:

- [App SSH Overview](#)
- [Accessing Apps with SSH](#)
- [Accessing Services with SSH](#)

## Application SSH Overview

Page last updated:

This topic introduces SSH configuration for applications in your Pivotal Application Service deployment.

If you need to troubleshoot an instance of an app, you can gain SSH access to the app using the SSH proxy and daemon.

For example, one of your app instances may be unresponsive, or the log output from the app may be inconsistent or incomplete. You can SSH into the individual VM that runs the problem instance to troubleshoot.

## SSH Access Control Hierarchy

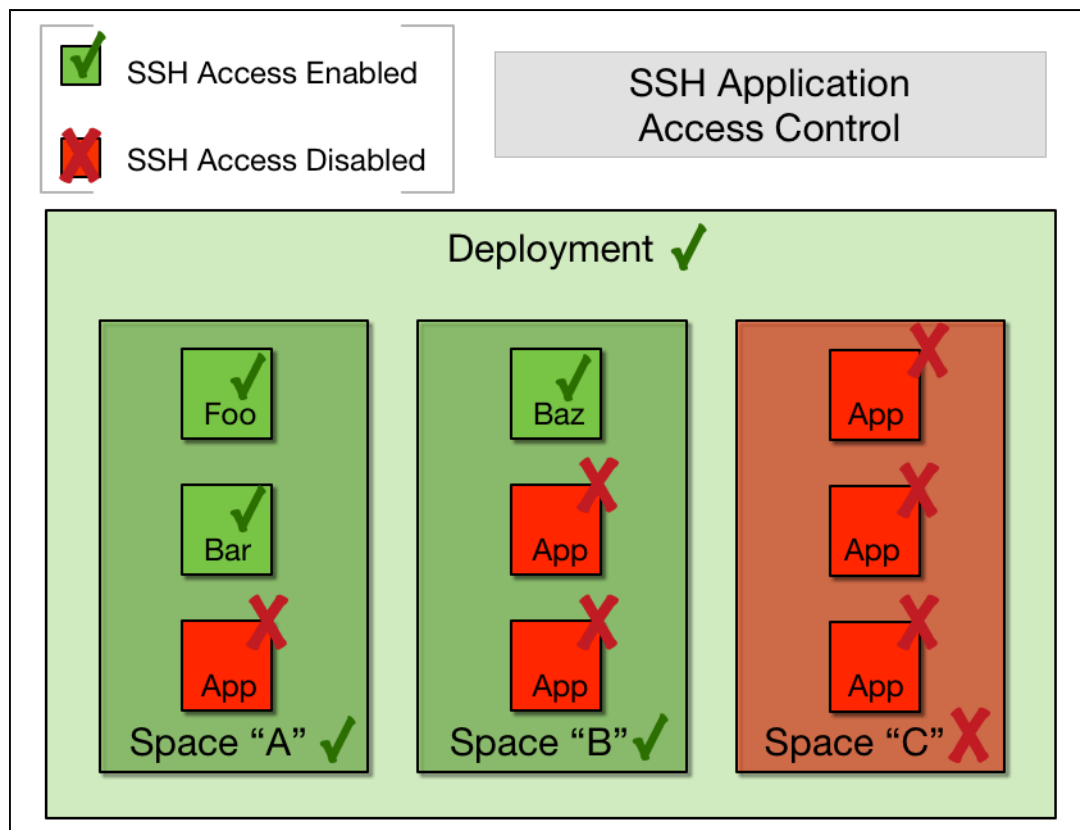
Operators, space managers, and space developers can configure SSH access for PAS, spaces, and apps as described in this table:

| User Role       | Scope of SSH Permissions Control | How They Define SSH Permissions                                                                                                                 |
|-----------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Operator        | Entire deployment                | Configure the deployment to allow or prohibit SSH access (one-time). For more information, see <a href="#">Configuring SSH Access for PCF</a> . |
| Space Manager   | Space                            | cf CLI <a href="#">allow-space-ssh</a> and <a href="#">disallow-space-ssh</a> commands                                                          |
| Space Developer | Application                      | cf CLI <a href="#">enable-ssh</a> and <a href="#">disable-ssh</a> commands                                                                      |

An application is SSH-accessible only if operators, space managers, and space developers all grant SSH access at their respective levels. For example, the image below shows a deployment where:

- An operator allowed SSH access at the deployment level.
- A space manager allowed SSH access for applications running in spaces “A” and “B” but not “C.”
- A space developer enabled SSH access for applications that include “Foo,” “Bar,” and “Baz.”

As a result, apps “Foo,” “Bar,” and “Baz” accept SSH requests.



## SSH Access for Apps and Spaces

Space managers and space developers can configure SSH access from the command line. The Cloud Foundry Command Line Interface (cf CLI) also includes commands to return the value of the SSH access setting. See the [Accessing Apps with Diego SSH](#) topic to use and configure SSH at both the application level and the space level.

## Configuring SSH Access for Pivotal Application Service

Pivotal Cloud Foundry deployments control SSH access to apps at the PAS level. Additionally, Cloud Foundry supports load balancing of SSH sessions with your load balancer. The [Configuring SSH Access](#) topic describes how to set SSH access for your deployment.

## About SSH Access

The SSH system components include the SSH proxy and daemon, and the system also supports authentication, and load balancing of incoming SSH traffic. The [Understanding SSH](#) topic provides a conceptual overview.

## Accessing Apps with SSH

Page last updated:

*This page assumes you are using cf CLI v6.13.0 or later.*

The Cloud Foundry Command Line Interface (cf CLI) lets you securely log into remote host virtual machines (VMs) running Pivotal Application Service application instances. This topic describes the commands that enable SSH access to applications, and enable, disable, and check permissions for such access.

The cf CLI looks up the `app_ssh_oauth_client` identifier in the Cloud Controller `/v2/info` endpoint, and uses this identifier to query the UAA server for an SSH authorization code. On the target VM side, the SSH proxy contacts the Cloud Controller through the `app_ssh_endpoint` listed in `/v2/info` to confirm permission for SSH access.

## Application SSH Commands

| cf CLI Command                                                                                                                     | Purpose                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cf enable-ssh</code><br><code>cf disable-ssh</code><br><code>cf allow-space-ssh</code><br><code>cf disallow-space-ssh</code> | <a href="#">Enable and Disable SSH Access</a>                                                                                                          |
| <code>cf ssh-enabled</code><br><code>cf space-ssh-allowed</code>                                                                   | <a href="#">Check SSH Access Permissions</a>                                                                                                           |
| <code>cf ssh</code>                                                                                                                | <a href="#">Securely log into an application container</a>                                                                                             |
| <code>cf ssh-code</code>                                                                                                           | <a href="#">Enable secure log in to an application container using non-CF SSH tools like <code>ssh</code>, <code>scp</code>, and <code>sftp</code></a> |

## Enabling and Disabling SSH Access

A cloud operator can deploy Pivotal Application Service to either allow or prohibit Application SSH across the entire deployment. For more information, see [Configuring SSH Access for PCF](#).

Within a deployment that permits SSH access to applications, Space Developers can enable or disable SSH access to individual applications, and Space Managers can enable or disable SSH access to all apps running within a space.

You must restart your application after enabling SSH access.

## Configuring SSH Access at the Application Level

[cf enable-ssh](#) enables SSH access to all instances of an app:

```
$ cf enable-ssh MY-AWESOME-APP
```

[cf disable-ssh](#) disables SSH access to all instances of an app:

```
$ cf disable-ssh MY-AWESOME-APP
```

## Configuring SSH Access at the Space Level

[cf allow-space-ssh](#) allows SSH access into all apps in a space:

```
$ cf allow-space-ssh SPACE-NAME
```

[cf disallow-space-ssh](#) disallows SSH access into all apps in a space:

```
$ cf disallow-space-ssh SPACE-NAME
```

## Checking SSH Permissions

[cf ssh-enabled](#) checks whether an app is accessible with SSH:

```
$ cf ssh-enabled MY-AWESOME-APP
ssh support is disabled for 'MY-AWESOME-APP'
```

[cf space-ssh-allowed](#) checks whether all apps running within a space are accessible with SSH:

```
$ cf space-ssh-allowed SPACE-NAME
ssh support is enabled in space 'SPACE-NAME'
```

## Logging Into an Application Container with cf SSH

If SSH access is allowed at the deployment, space, and application level, you can run the `cf ssh APP-NAME` command to start an interactive SSH session with a VM hosting an application. By default, the command accesses the container running the first instance of the application, the instance with index 0.

```
$ cf ssh MY-AWESOME-APP
```

When logged into a VM hosting an app, you can use tools like the Cloud Foundry Diego Operator Toolkit (cfdot) to run app status diagnostics. For more information, see [How to use CF Diego Operator Toolkit](#).

## Common cf SSH Flags

You can tailor [cf ssh](#) commands with the following flags, most of which mimic flags for the Unix or Linux `ssh` command. Run the `cf ssh --help` command for more details.

- The `-i` flag targets a specific instance of an application. To log into the VM container hosting the third instance, `index=2`, of MY-AWESOME-APP, run:

```
$ cf ssh MY-AWESOME-APP -i 2
```

- The `-L` flag enables local port forwarding, binding an output port on your machine to an input port on the application VM. Pass in a local port, and your application VM port and port number, all colon delimited. You can prepend your local network interface, or use the default `localhost`.

```
$ cf ssh MY-AWESOME-APP -L [LOCAL-NETWORK-INTERFACE:]LOCAL-PORT:REMOTE-HOST-NAME:REMOTE-HOST-PORT
```

- The `-N` flag skips returning a command prompt on the remote machine. This sets up local port forwarding if you do not need to execute commands on the host VM.
- The `--request-pseudo-tty` and `--force-pseudo-tty` flags let you run an SSH session in pseudo-tty mode rather than generate terminal line output.

## SSH Session Environment

If you want the environment of your interactive SSH session to match the environment of your buildpack-based app, with the same environment variables and working directory, run the following commands after starting the session:

```
/tmp/lifecycle/shell
```

After running the above command, the value of the `VCAP_APPLICATION` environment variable differs slightly from its value in the environment of the app process, as it will not have the `host`, `instance_id`, `instance_index`, or `port` fields set. These fields are available in other environment variables, as described in the [VCAP\\_APPLICATION](#) documentation.

## Application SSH Access without cf CLI

In addition to `cf ssh`, you can use other SSH clients such as `ssh`, `scp`, or `sftp` to access your application, if you have SSH permissions.

Follow the steps below to securely connect to an application instance by logging in with a specially-formed username that passes information to the SSH proxy running on the host VM. For the password, use a one-time SSH authorization code generated by [cf ssh-code](#).

1. Run `cf app MY-AWESOME-APP --guid` and record the GUID of your target app.

```
$ cf app MY-AWESOME-APP --guid
abcdefab-1234-5678-abcd-1234abcd1234
```

2. Query the `/v2/info` endpoint of the Cloud Controller in your deployment. Record the domain name and port of the `app_ssh_endpoint` field, and the `app_ssh_host_key_fingerprint` field. You will compare the `app_ssh_host_key_fingerprint` with the fingerprint returned by the SSH proxy on your target VM.

```
$ cf curl /v2/info
{
 ...
 "app_ssh_endpoint": "ssh.MY-DOMAIN.com:2222",
 "app_ssh_host_key_fingerprint": "a6:14:c0:ea:42:07:b2:f7:53:2c:0b:60:e0:00:21:6c",
 ...
}
```

3. Run `cf ssh-code` to obtain a one-time authorization code that substitutes for an SSH password. You can run `cf ssh-code | pbcopy` to automatically copy the code to the clipboard.

```
$ cf ssh-code
E1x89n
```

4. Run your `ssh` or other command to connect to the application instance. For the username, use a string of the form `cf:APP-GUID/APP-INSTANCE-INDEX@SSH-ENDPOINT`, where `APP-GUID` and `SSH-ENDPOINT` come from the previous steps. For the port number, use the `SSH-PORT` recorded above. `APP-INSTANCE-INDEX` is the index of the instance you want to access.

With the above example, you `ssh` into the container hosting the first instance of your app by running the following command:

```
$ ssh -p 2222 cf:abcdefab-1234-5678-abcd-1234abcd1234/0@ssh.MY-DOMAIN.com
```

Or you can use `scp` to transfer files by running one of the following commands:

```
scp -P 2222 -o User=cf:abcdefab-1234-5678-abcd-1234abcd1234/0 ssh.MY-DOMAIN.com:REMOTE-FILE-TO-RETRIEVE LOCAL-FILE-DESTINATION
scp -P 2222 -o User=cf:abcdefab-1234-5678-abcd-1234abcd1234/0 LOCAL-FILE-TO-COPY ssh.MY-DOMAIN.com:REMOTE-FILE-DESTINATION
```

5. When the SSH proxy reports its RSA fingerprint, confirm that it matches the `app_ssh_host_key_fingerprint` recorded above. When prompted for a password, paste in the authorization code returned by `cf ssh-code`.

```
$ ssh -p 2222 cf:abcdefab-1234-5678-abcd-1234abcd1234/0@ssh.MY-DOMAIN.com
The authenticity of host '[ssh.MY-DOMAIN.com]:2222 ([203.0.113.5]:2222)' can't be established.
RSA key fingerprint is a6:14:c0:ea:42:07:b2:f7:53:2c:0b:60:e0:00:21:6c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[ssh.MY-DOMAIN.com]:2222 [203.0.113.5]:2222' (RSA) to the list of known hosts.
cf:d0a2e11d-e6ca-4120-b32d-140@ssh.ketchup.cf-app.com's password:
vcap@ce4f5164kws:~$
```

You have now securely connected to the application instance.

## SSH Proxy Security Configuration

The SSH proxy has the following SSH security configuration by default:

| Security Parameter | Values                                     |
|--------------------|--------------------------------------------|
|                    | <code>chacha20-poly1305@openssh.com</code> |
|                    | <code>aes128-gcm@openssh.com</code>        |

|               |                                                                   |
|---------------|-------------------------------------------------------------------|
| Ciphers       | <div>aes256-ctr</div> <div>aes192-ctr</div> <div>aes128-ctr</div> |
| MACs          | <div>hmac-sha2-256-etm@openssh.com</div> <div>hmac-sha2-256</div> |
| Key Exchanges | <div>curve25519-sha256@libssh.org</div>                           |

The `cf ssh` command is compatible with this security configuration. If you use a different SSH client to access applications over SSH, you should ensure that you configure your client to be compatible with these ciphers, MACs, and key exchanges. For more information about other SSH clients, see the [Application SSH Access without cf CLI](#) section of this topic.

## Proxy to Container Authentication

A second layer of SSH security runs within each container. When the SSH proxy attempts to handshake with the SSH daemon inside the target container, it uses the following fields associated with the `diego-ssh` key in its route to the application instance. This inner layer works invisibly and requires no user action, but is described here to complete the SSH security picture.

### CONTAINER\_PORT (required)

`container_port` indicates which port inside the container the SSH daemon is listening on. The proxy attempts to connect to host side mapping of this port after authenticating the client.

### HOST\_FINGERPRINT (optional)

When present, `host_fingerprint` declares the expected fingerprint of the SSH daemon's host public key. When the fingerprint of the actual target's host key does not match the expected fingerprint, the connection is terminated. The fingerprint should only contain the hex string generated by `ssh-keygen -l`.

### USER (optional)

`user` declares the user ID to use during authentication with the container's SSH daemon. While this is not a required part of the routing data, it is required for password authentication and may be required for public key authentication.

### PASSWORD (optional)

`password` declares the password to use during password authentication with the container's ssh daemon.

### PRIVATE\_KEY (optional)

`private_key` declares the private key to use when authenticating with the container's SSH daemon. If present, the key must be a PEM encoded RSA or DSA public key.

### Example Application Process

```
{
 "process_guid": "ssh-process-guid",
 "domain": "ssh-experiments",
 "rootfs": "preloaded:cflinuxfs2",
 "instances": 1,
 "start_timeout": 30,
 "setup": {
 "download": {
 "artifact": "diego-sshd",
 "from": "http://file-server.service.cf.internal.example.com:8080/v1/static/diego-sshd/diego-sshd.tgz",
 "to": "/tmp",
 "cache_key": "diego-sshd"
 }
 },
 "action": {
 "run": {
 "path": "/tmp/diego-sshd",
 "args": [
 "-address=0.0.0.0:2222",
 "-authorizedKey=ssh-rsa ..."
],
 "env": [],
 "resource_limits": {}
 }
 },
 "ports": [2222],
 "routes": {
 "diego-ssh": {
 "container_port": 2222,
 "private_key": "PEM encoded PKCS#1 private key"
 }
 }
}
```

## Daemon discovery

To be accessible via the SSH proxy, containers must host an SSH daemon, expose it via a mapped port, and advertise the port in a `diego-ssh` route. If a proxy cannot find the target process or a route, user authentication fails.

```
"routes": {
 "diego-ssh": { "container_port": 2222 }
}
```

The Diego system generates the appropriate process definitions for Pivotal Application Service applications which reflect the policies that are in effect.




## Accessing Services with SSH

Page last updated:

This page assumes you are using Cloud Foundry Command Line Interface (cf CLI) v6.15.0 or later.

This topic describes how to gain direct command line access to your deployed service instance. For example, you may need access to your database to execute raw SQL commands to edit the schema, import and export data, or debug application data issues.


To establish direct command line access to a service, you deploy a host app and use its SSH and port forwarding features to communicate with the service instance through the app container. The technique outlined below works with TCP services such as MySQL or Redis.

 **Note:** The procedure in this topic requires use of a service key, and not all services support service keys. Some services support credentials through [application binding](#) only.

## Create a Service Instance

1. In your terminal window, log in to your deployment with `cf login`.
2. List the marketplace services installed as product tiles on your Pivotal Cloud Foundry (PCF) Ops Manager. See the [Adding and Deleting Products](#) topic if you need to add the service as a tile. In this example, we create a p-mysql service instance.

```
$ cf marketplace
p-mysql 100mb MySQL databases on demand
```

3. Create your service instance. As part of the [create-service](#)  command, indicate the service name, the service plan, and the name you choose for your service instance.

```
$ cf create-service p-mysql 100mb MY-DB
```

## Push Your Host App

To push an app that will act as the host for the SSH tunnel, push any app that will successfully deploy to Pivotal Application Service.


 **Note:** Your app must be prepared before you push it. See the [Deploy an Application](#) topic for details on preparing apps for deployment.

1. Push your app.

```
$ cf push YOUR-HOST-APP
```


2. Enable SSH for your app.

```
$ cf enable-ssh YOUR-HOST-APP
```

 **Note:** To enable SSH access to your app, SSH access must also be enabled for both the space that contains the app and Pivotal Application Service. See the [Application SSH Overview](#) topic for more details.

## Create Your Service Key

To establish SSH access to your service instance, you must create a service key that contains critical information for configuring your SSH tunnel.

1. Create a service key for your service instance using the [cf create-service-key](#)  command.

```
$ cf create-service-key MY-DB EXTERNAL-ACCESS-KEY
```

2. Retrieve your new service key using the [cf service-key](#) command.

```
$ cf service-key MY-DB EXTERNAL-ACCESS-KEY
Getting key EXTERNAL-ACCESS-KEY for service instance MY-DB as user@example.com

{
 "hostname": "us-cdbr-iron-east-01.p-mysql.net",
 "jdbcUrl": "jdbc:mysql://us-cdbr-iron-east-03.p-mysql.net/ad_b2fca6t49704585d?user=b5136e448be920u0026password=231f435o05",
 "name": "ad_b2fca6t49704585d",
 "password": "231f435o05",
 "port": "3306",
 "uri": "mysql://b5136e448be920:231f435o05@us-cdbr-iron-east-03.p-mysql.net:3306/ad_b2fca6t49704585d?reconnect=true",
 "username": "b5136e448be920"
}
```

## Configure Your SSH Tunnel

Configure an SSH tunnel to your service instance using [cf ssh](#). Tailor the example command below with information from your service key.

```
$ cf ssh -L 63306:us-cdbr-iron-east-01.p-mysql.net:3306 YOUR-HOST-APP
```

- Use any available local port for port forwarding. For example, `63306`.
- Replace `us-cdbr-iron-east-01.p-mysql.net` with the address provided under `hostname` in the service key retrieved above.
- Replace `3306` with the port provided under `port` above.
- Replace `YOUR-HOST-APP` with the name of your host app.

After you enter the command, open another terminal window and perform the steps below in [Access Your Service Instance](#).

## Access Your Service Instance

To establish direct command-line access to your service instance, use the relevant command line tool for that service. This example uses the MySQL command line client to access the p-mysql service instance.

```
$ mysql -u b5136e448be920 -h 0 -p -D ad_b2fca6t49704585d -P 63306
```

- Replace `b5136e448be920` with the username provided under `username` in your service key.
- `-h 0` instructs `mysql` to connect to your local machine.
- `-p` instructs `mysql` to prompt for a password. When prompted, use the password provided under `password` in your service key.
- Replace `ad_b2fca6t49704585d` with the database name provided under `name` in your service key.
- `-P 63306` instructs `mysql` to connect on port `63306`.

## Routes and Domains

The following list provides information about configuring routes and domains:

- [Configuring Routes and Domains](#)

## Routes and Domains

Page last updated:

This topic describes how routes and domains work in Pivotal Application Service, and how developers and administrators configure routes and domains for their applications using the Cloud Foundry Command Line Interface (cf CLI).

For more information about routing capabilities in PAS, see the [HTTP Routing](#) topic.

## Routes

The PAS Gorouter routes requests to applications by associating an app with an address, known as a route. We call this association a **mapping**. Use the cf CLI [cf map-route](#) command to associate an app and route.

The routing tier compares each request with a list of all the routes mapped to apps and attempts to find the best match. For example, the Gorouter would make the following matches for the two routes `myapp.shared-domain.example.com` and `myapp.shared-domain.example.com/products`:


| Request                                                          | Matched Route                                         |
|------------------------------------------------------------------|-------------------------------------------------------|
| <code>http://myapp.shared-domain.example.com</code>              | <code>myapp.shared-domain.example.com</code>          |
| <code>http://myapp.shared-domain.example.com/contact</code>      | <code>myapp.shared-domain.example.com</code>          |
| <code>http://myapp.shared-domain.example.com/products</code>     | <code>myapp.shared-domain.example.com/products</code> |
| <code>http://myapp.shared-domain.example.com/products/123</code> | <code>myapp.shared-domain.example.com/products</code> |
| <code>http://products.shared-domain.example.com</code>           | No match; 404                                         |

The Gorouter does not use a route to match requests until the route is mapped to an app. In the above example, `products.shared-domain.example.com` may have been created as a route in Cloud Foundry, but until it is mapped to an app, requests for the route receive a `404`.


The routing tier knows the location of instances for apps mapped to routes. Once the routing tier determines a route as the best match for a request, it makes a load-balancing calculation using a round-robin algorithm, and forwards the request to an instance of the mapped app.

Developers can map many apps to a single route, resulting in load-balanced requests for the route across all instances of all mapped apps. This approach enables the blue/green zero-downtime deployment strategy. Developers can also map an individual app to multiple routes, enabling access to the app from many URLs. The number of routes that can be mapped to each app is approximately 1000 (128 KB).

Routes belong to a space, and developers can only map apps to a route in the same space.

 **Note:** Routes are globally unique. Developers in one space cannot create a route with the same URL as developers in another space, regardless of which orgs control these spaces.

## HTTP vs. TCP Routes

 **Note:** By default, PAS only supports routing of HTTP requests to applications.

Routes are considered HTTP if they are created from HTTP domains, and TCP if they are created from TCP domains. See [HTTP vs. TCP Shared Domains](#).


HTTP routes include a domain, an optional hostname, and an optional context path. `shared-domain.example.com`, `myapp.shared-domain.example.com`, and `myapp.shared-domain.example.com/products` are all examples of HTTP routes. Applications should listen to the `localhost` port defined by the `$PORT` environment variable, which is `8080` on Diego. As an example, requests to `myapp.shared-domain.example.com` would be routed to the application container at `localhost:8080`.

- Requests to HTTP routes must be sent to ports 80 or 443.
- Ports cannot be reserved for HTTP routes.


TCP routes include a domain and a route port. A route port is the port clients make requests to. This is not the same port as what an application pushed to Cloud Foundry listens on. `tcp.shared-domain.example.com:60000` is an example of a TCP route. Just as for HTTP routes, applications should listen to the `localhost` port defined by the `$PORT` environment variable, which is `8080` on Diego. As an example, requests to `tcp.shared-domain.example.com:60000` would be routed to the application container at `localhost:8080`.

- Once a port is reserved for a route, it cannot be reserved for another route.
- Hostname and path are not supported for TCP routes.

## Internal Routes


 **Note:** This feature is currently experimental.

Applications can communicate without leaving the platform on the container network using internal routes. You can create an internal route using the [cf map-route](#) command with an [internal domain](#).

By default, apps cannot communicate with each other on the container network. To allow apps to communicate with each other you must create a network policy. For more information, see [add-network-policy](#)  in the *Cloud Foundry CLI Reference Guide*.


## Create a Route

When a developer creates a route using the cf CLI, PAS determines whether the route is an HTTP or a TCP route based on the domain. To create a HTTP route, a developer must choose an HTTP domain. To create a TCP route, a developer must choose a TCP domain.

Domains in PAS provide a namespace from which to create routes. To list available domains for a targeted organization, use the [cf domains](#)  command. For more information about domains, see the [Domains](#) section.

The following sections describe how developers can create HTTP and TCP routes for different use cases.

### Create an HTTP Route with Hostname

In PAS, a hostname is the label that indicates a subdomain of the domain associated with the route. Given a domain `shared-domain.example.com`, a developer can create the route `myapp.shared-domain.example.com` in space `my-space` by specifying the hostname `myapp` with the [cf create-route](#)  command as shown in this example:

```
$ cf create-route my-space shared-domain.example.com --hostname myapp
Creating route myapp.shared-domain.example.com for org my-org / space my-space as username@example.com...
OK
```

This command instructs PAS to only route requests to apps mapped to this route for the following URLs:

- `http://myapp.shared-domain.example.com`
- `https://myapp.shared-domain.example.com`
- Any path under either of the above URLs, such as `http://myapp.shared-domain.example.com/bar`

### Create an HTTP Route without Hostname

This approach creates a route with the same address as the domain itself and is permitted for private domains only. For more information, see the [Private Domains](#) section.

A developer can create a route in space `my-space` from the domain `private-domain.example.com` with no hostname with the [cf create-route](#)  command:

```
$ cf create-route my-space private-domain.example.com
Creating route private-domain.example.com for org my-org / space my-space as username@example.com...
OK
```

If DNS has been configured correctly, this command instructs PAS to route requests to apps mapped to this route from the following URLs:

- `http://private-domain.example.com`
- `https://private-domain.example.com`
- Any path under either of the above URLs, such as `http://private-domain.example.com/foo`

If there are no other routes for the domain, requests to any subdomain, such as `http://foo.private-domain.example.com`, will fail.

A developer can also create routes for subdomains with no hostnames. The following command creates a route in space `my-space` from the subdomain `foo.private-domain.example.com`:

```
$ cf create-route my-space foo.private-domain.example.com
Creating route foo.private-domain.example.com for org my-org / space my-space as username@example.com...
OK
```

Assuming DNS has been configured for this subdomain, this command instructs PAS to route requests to apps mapped to this route from the following URLs:

- `http://foo.private-domain.example.com`
- `https://foo.private-domain.example.com`
- Any path under either of the above URLs, such as `http://foo.private-domain.example.com/foo`

## Create an HTTP Route with Wildcard Hostname

An application mapped to a wildcard route acts as a fallback app for route requests if the requested route does not exist. To create a wildcard route, use an asterisk for the hostname.

A developer can create a wildcard route in space `my-space` from the domain `foo.shared-domain.example.com` with the following command:

```
$ cf create-route my-space foo.shared-domain.example.com --hostname '*'
Creating route *.foo.shared-domain.example.com for org my-org / space my-space as username@example.com...
OK
```

If a client sends a request to `http://app.foo.shared-domain.example.com` by accident, attempting to reach `myapp.foo.shared-domain.example.com`, PAS routes the request to the app mapped to the route `*.foo.shared-domain.example.com`.

## Create an HTTP Route with a Path

Developers can use paths to route requests for the same hostname and domain to different apps.

A developer can create three routes using the same hostname and domain in the space `my-space` with the following commands:

```
$ cf create-route my-space shared-domain.example.com --hostname store --path products
Creating route store.shared-domain.example.com/products for org my-org / space my-space as username@example.com...
OK

$ cf create-route my-space shared-domain.example.com --hostname store --path orders
Creating route store.shared-domain.example.com/orders for org my-org / space my-space as username@example.com...
OK


$ cf create-route my-space shared-domain.example.com --hostname store
Creating route store.shared-domain.example.com for org my-org / space my-space as username@example.com...
OK
```

The developer can then map the new routes to different apps by following the steps in the [Map a Route to Your Application](#) section below.

If the developer maps the first route with path `products` to the `products` app, the second route with path `orders` to the `orders` app, and the last route to the `storefront` app. After this, the following occurs:

- PAS routes requests to `http://store.shared-domain.example.com/products` to the `products` app.
- PAS routes requests to `http://store.shared-domain.example.com/orders` to the `orders` app.
- PAS routes requests to `http://store.shared-domain.example.com` to the `storefront` app.

PAS attempts to match routes with a path first, and then attempts to match host and domain.

 **Note:** Routes with the same domain and hostname but different paths can only be created in the same space. Private domains do not have this limitation.

 **Note:** PAS does not route requests for context paths to the root context of an application. Applications must serve requests on the context path.

## Create a TCP Route with a Port

A developer can create a TCP route for `tcp.shared-domain.example.com` on an arbitrary port with the following command. If the clients of the app can accommodate addressing an arbitrary port, then developers should use the `--random-port` to instruct PAS to pick a port for your route.


```
$ cf create-route my-space tcp.shared-domain.example.com --random-port
Creating route tcp.shared-domain.example.com for org my-org / space my-space as user@example.com...
OK
Route tcp.shared-domain.example.com:60034 has been created
```

In this example, PAS routes requests to `tcp.shared-domain.example.com:60034` to apps mapped to this route.

To request a specific port, a developer can use the `--port` flag, so long as the port is not reserved for another space. The following command creates a TCP route for `tcp.shared-domain.example.com` on port 60035:

```
$ cf create-route my-space tcp.shared-domain.example.com --port 60035
Creating route tcp.shared-domain.example.com:60035 for org my-org / space my-space as user@example.com...
OK
```

## List Routes


Developers can list routes for the current space with the [cf routes](#)  command. A route is uniquely identified by the combination of hostname, domain, port, and path.

```
$ cf routes
Getting routes as user@private-domain.example.com ...

space host domain port path type apps
my-space myapp shared-domain.example.com myapp
my-space myapp private-domain.example.com myapp
my-space store shared-domain.example.com /products products
my-space store shared-domain.example.com /orders orders
my-space store shared-domain.example.com storefront
my-space shared-domain.example.com 60000 tcp tcp-app
```

Developers can only see routes in spaces where they are members.


## Check Routes


Developers cannot create a route that is already taken. To check whether a route is available, developers can use the [cf check-route](#)  command.

The following command checks whether a route with the hostname `store` and the domain `shared-domain.example.com` and the path `/products` exists:


```
$ cf check-route store shared-domain.example.com --path /products
Checking for route...
OK
Route store.shared-domain.example.com/products does exist
```

## Map a Route to Your Application

For an app to receive requests to a route, developers must map the route to the app with the [cf map-route](#)  command. If the route does not already exist, this command creates it.

 **Note:** Any app that is not routed to port `80` or port `443` must be explicitly mapped using the `cf map-route` command. Otherwise, the route is automatically mapped to port `443`.

Developers can create and reserve routes for later use by following the steps in the [Manually Map a Route](#) section. Or they can map routes to their app immediately as part of a push by following the steps in the [Map a Route with Application Push](#) section.

 **Note:** Changes to route mappings are executed asynchronously. On startup, an application will be accessible at its route within a few seconds. Similarly, upon mapping a new route to a running app, the app will be accessible at this route within a few seconds of the CLI exiting successfully.

## Manually Map a Route

Given the following routes and applications:

| Route                                    | Application |
|------------------------------------------|-------------|
| store.shared-domain.example.com/products | products    |
| store.shared-domain.example.com/orders   | orders      |
| store.shared-domain.example.com          | storefront  |
| tcp.shared-domain.example.com:60000      | tcp-app     |

The following commands map the above routes to their respective apps. Developers use hostname, domain, and path to uniquely identify a route to map their apps to.

```
$ cf map-route products shared-domain.example.com --hostname store --path products
$ cf map-route orders shared-domain.example.com --hostname store --path orders
$ cf map-route storefront shared-domain.example.com --hostname store
$ cf map-route tcp-app tcp.shared-domain.example.com --port 60000
```

The following command maps the wildcard route `*.foo.shared-domain.example.com` to the app `myfallbackapp`.

```
$ cf map-route myfallbackapp foo.shared-domain.example.com --hostname '*'
```

## Map a Route with Application Push

Developers can map a route to their app with the `cf push` command.

If a domain or hostname is not specified, then a route will be created using the app name and the default shared domain (see [Shared Domains](#)). The following command pushes the app `myapp`, creating the route `myapp.shared-domain.example.com` from the default shared domain `shared-domain.example.com`. If the route has not already been created in another space this command also maps it to the app.

```
$ cf push myapp
```

To customize the route during `push`, specify the domain using the `-d` flag and the hostname with the `--hostname` flag. The following command creates the `foo.private-domain.example.com` route for `myapp`:

```
$ cf push myapp -d private-domain.example.com --hostname foo
```

To map a TCP route during `push`, specify a TCP domain and request a random port using `--random-route`. To specify a port, push the app without a route, then create and map the route manually by following the steps in the [Create a TCP Route with a Port](#) section.

```
$ cf push tcp-app -d tcp.shared-domain.example.com --random-route
```

## Map a Route Using Application Manifest

Developers can map a route to their app with a manifest by editing the `route` attribute to specify the host, domain, port and/or path components of the route. For more information, see the [Deploying with Application Manifests](#) topic.

## Map a Route to Multiple Apps

PAS allows multiple apps, or versions of the same app, to be mapped to the same route. This feature enables Blue-Green deployment. For more information see [Using Blue-Green Deployment to Reduce Downtime and Risk](#).

Routing multiple apps to the same route may cause undesirable behavior in some situations by routing incoming requests randomly to one of the apps on the shared route.

See the [Routing Conflict](#) section of the Troubleshooting Application Deployment and Health topic for more information about troubleshooting this problem.



## Map Multiple Routes to One App

You can have multiple routes to an app, but those routes cannot have different context paths.


The following routes are valid for a single app:

| Route 1                            | Route 2                                    |
|------------------------------------|--------------------------------------------|
| <code>myapp.example.com</code>     | <code>myapp.apps.cf.example.com</code>     |
| <code>myapp.example.com/foo</code> | <code>myapp.apps.cf.example.com/foo</code> |

The following routes are **not** valid for a single app:

| Route 1                                    | Route 2                                    |
|--------------------------------------------|--------------------------------------------|
| <code>myapp.example.com/foo</code>         | <code>myapp.apps.cf.example.com/bar</code> |
| <code>myapp.apps.cf.example.com/foo</code> | <code>myapp.example.com/bar</code>         |

## Map an Internal Route to an App

 **Note:** This feature is currently experimental.

You can map an internal route to any app. This internal route allows your app to communicate with other apps without leaving the platform. Once mapped, this route becomes available to all other apps on the platform.

This example creates a `foo.apps.internal` internal route for `myapp` :

```
$ cf map-route myapp apps.internal --hostname foo
```

## Unmap a Route

Developers can remove a route from an app using the `cf unmap-route` command. The route remains reserved for later use in the space where it was created until the route is deleted.

To unmap an HTTP route from an app, identify the route using the hostname, domain, and path:

```
$ cf unmap-route tcp-app private-domain.example.com --hostname myapp --path mypath
```

To unmap a TCP route from an app, identify the route using the domain and port:

```
$ cf unmap-route tcp-app tcp.shared-domain.example.com --port 60000
```

## Delete a Route

Developers can delete a route from a space using the `cf delete-route` command.

To delete a HTTP route, identify the route using the hostname, domain, and path:

```
$ cf delete-route private-domain.example.com --hostname myapp --path mypath
```

To delete a TCP route, identify the route using the domain and port.

```
$ cf delete-route tcp.private-domain.example.com --port 60000
```

## Routing Requests to a Specific App Instance

 **Note:** Usage of `X-CF-APP-INSTANCE` is supported only for Diego.

Users can route HTTP requests to a specific application instance using the header `X-CF-APP-INSTANCE`. The format of the header should be `X-CF-APP-INSTANCE: APP_GUID:APP_INDEX`.

`APP_GUID` is an internal identifier for your application. Use the `cf APP-NAME --guid` command to discover the `APP_GUID` for your application.

```
$ cf app myapp --guid
```

`APP_INDEX`, for example `0`, `1`, `2`, or `3`, is an identifier for a particular app instance. Use the CLI command `cf app APP-NAME` to get statistics on each instance of a particular app.


```
$ cf app myapp
```

The following example shows a request made to instance `9` of an application with GUID `5cdc7595-2e9b-4f62-8d5a-a86b92f2df0e` and mapped to route `myapp.private-domain.example.com`.

```
$ curl myapp.private-domain.example.com -H "X-Cf-App-Instance: 5cdc7595-2e9b-4f62-8d5a-a86b92f2df0e:9"
```

If the cf CLI cannot find the instance the format is incorrect, a `404` status code is returned.

## Domains

 **Note:** The term domain in this topic differs from its common use and is specific to Cloud Foundry. Likewise, shared domain and private domain refer to resources with specific meaning in Cloud Foundry. The use of domain name, root domain, and subdomain refers to DNS records.

Domains indicate to a developer that requests for any route created from the domain will be routed to PAS. This requires DNS to be configured out-of-band to resolve the domain name to the IP address of a load balancer configured to forward requests to the CF routers. For more information about configuring DNS, see the [DNS for Domains](#) section.

## List Domains for an Org

When creating a route, developers will select from domains available to them. Use the `cf domains` command to view a list of available domains for the targeted org:


```
$ cf domains
Getting domains in org my-org as user@example.com... OK
name status type
shared-domain.example.com shared
tcp.shared-domain.example.com shared tcp
private-domain.example.com owned
```

This example displays three available domains: a shared HTTP domain `shared-domain.example.com`, a shared TCP domain `tcp.shared-domain.example.com`, and a private domain `private-domain.example.com`. See [Shared Domains](#) and [Private Domains](#).

## HTTP vs. TCP Domains

HTTP domains indicate to a developer that only requests using the HTTP protocol will be routed to applications mapped to routes created from the domain. Routing for HTTP domains is layer 7 and offers features like custom hostnames, sticky sessions, and TLS termination.

TCP domains indicate to a developer that requests over any TCP protocol, including HTTP, will be routed to applications mapped to routes created from the domain. Routing for TCP domains is layer 4 and protocol agnostic, so many features available to HTTP routing are not available for TCP routing. TCP domains are defined as being associated with the TCP Router Group. The TCP Router Group defines the range of ports available to be reserved with TCP Routes. Currently, only Shared Domains can be TCP.

 **Note:** By default, PAS only supports routing of HTTP requests to applications.

## Shared Domains

Admins manage shared domains, which are available to users in all orgs of a PAS deployment. An admin can offer multiple shared domains to users. For example, an admin may offer developers the choice of creating routes for their apps from `shared-domain.example.com` and `cf.some-company.com`.

There is not technically a default shared domain. If a developer pushes an app without specifying a domain (see [Map a Route with Application Push](#)), a route will be created for it from the first shared domain created in the system. All other operations involving route require the domain be specified (see [Routes](#)).

Shared domains are HTTP by default, but can be configured to be TCP when associated with the TCP Router Group.

### Create a Shared Domain

Admins can create an HTTP shared domain with the `cf create-shared-domain` command:

```
$ cf create-shared-domain shared-domain.example.com
```

To create a TCP shared domain, first discover the name of the TCP Router Group.

```
$ cf router-groups
Getting router groups as admin ...
name type
default-tcp tcp
```

Then create the shared domain using the `--router-group` option to associate the domain with the TCP router group.


```
$ cf create-shared-domain tcp.shared-domain.example.com --router-group default-tcp
```

### Delete a Shared Domain


Admins can delete a shared domain from PAS with the `cf delete-shared-domain` command:

```
$ cf delete-shared-domain example.com
```

## Internal Domain

 **Note:** This feature is currently experimental.

The internal domain is a special type of shared domain used for app communication internal to the platform. When you enable service discovery, the internal domain `apps.internal` becomes provided for your use.

 **Note:** The internal domain *apps.internal* cannot be deleted. At this time, no other internal domains can be created.

## Private Domains

Org managers can add private domains, or custom domains, and give members of the org permission to create routes for privately registered domain names. Private domains can be shared with other orgs, enabling users of those orgs to create routes from the domain.

Private domains can be HTTP or HTTPS only. TCP Routing is supported for shared domains only.

### Create a Private Domain

Org managers can create a private domain with the following command:

```
$ cf create-domain my-org private-domain.example.com
```

Org managers can create a private domain for a subdomain with the following command:

```
$ cf create-domain my-org foo.private-domain.example.com
```

## Sharing a Private Domain with One or More Orgs

Org managers can grant or revoke access to a private domain to other orgs if they have permissions for these orgs with the following commands:

```
$ cf share-private-domain test-org private-domain.example.com
```

```
$ cf unshare-private-domain test-org private-domain.example.com
```

## Delete a Private Domain

Org managers can delete a domain from PAS with the `cf delete-domain` command:

```
$ cf delete-domain private-domain.example.com
```

## Requirements for Parent and Child Domains

In the domain `myapp.shared-domain.example.com`, `shared-domain.example.com` is the parent domain of subdomain `myapp`. Note the following requirements for domains:

- You can only create a private domain that is parent to a private subdomain.
- You can create a shared domain that is parent to either a shared or a private subdomain.

The domain `foo.myapp.shared-domain.example.com` is the child subdomain of `myapp.shared-domain.example.com`. Note the following requirements for subdomains:

- You can create a private subdomain for a private parent domain only if the domains belong to the same org.
- You can create a private subdomain for a shared parent domain.
- You can only create a shared subdomain for a shared parent domain.
- You cannot create a shared subdomain for a private parent domain.

## DNS for Domains

To create customized access to your apps, you can map specific or wildcard custom domains to PAS by using your DNS provider.

### Mapping Domains to Your Custom Domain

To associate a registered domain name with a domain on PAS, configure a CNAME record with your DNS provider, pointing at any shared domain offered in PAS.

### Mapping a Single Domain to Your Custom Domain


To map a single domain to a custom domain to PAS, configure a CNAME record with your DNS provider.

The following table provides some example CNAME record mappings.

| Record Set in Custom Domain | Type  | Target in PAS                   |
|-----------------------------|-------|---------------------------------|
| myapp.yourcustomdomain.com. | CNAME | myapp.shared-domain.example.com |

`www.yourcustomdomain.com.` | CNAME | `myapp.shared-domain.example.com`

After you create the CNAME mapping, your DNS provider routes your custom domain to `myapp.shared-domain.example.com`.

 **Note:** Refer to your DNS provider documentation to determine whether the trailing `.` is required.

## Mapping Multiple Subdomains to Your Custom Domain

Use a wildcard CNAME record to point all of the subdomains in your custom domain to `shared-domain.example.com`.

Each separately configured subdomain has priority over the wildcard configuration.

The following table provides some example wildcard CNAME record mappings.


| Record Set in Custom Domain          | Type  | Target in PAS                                  |
|--------------------------------------|-------|------------------------------------------------|
| <code>*.yourcustomdomain.com.</code> | CNAME | <code>*.shared-domain.example.com</code>       |
| <code>*.yourcustomdomain.com.</code> | CNAME | <code>*.myapp.shared-domain.example.com</code> |

If you use a wildcard as the subdomain name, then your DNS provider can route from `*.YOURCUSTOMDOMAIN` to any of the following:

- `*.shared-domain.example.com`
- `foo.myapp.shared-domain.example.com`
- `bar.foo.myapp.shared-domain.example.com`

## Configuring DNS for Your Registered Root Domain


To use your root domain (for example, `example.com`) for apps on PAS you can either use custom DNS record types like ALIAS and ANAME, if your DNS provider offers them, or subdomain redirection.

 **Note:** Root domains are also called zone apex domains.

If your DNS provider supports using an ALIAS or ANAME record, configure your root domain with your DNS provider to point at a shared domain in PAS.

| Record         | Name                    | Target                                   | Note                                                                                                                      |
|----------------|-------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| ALIAS or ANAME | empty or <code>@</code> | <code>private-domain.example.com.</code> | Refer to your DNS provider documentation to determine whether to use an empty or <code>@</code> value for the Name entry. |

If your DNS provider does not support ANAME or ALIAS records you can use subdomain redirection, also known as domain forwarding, to redirect requests for your root domain to a subdomain configured as a CNAME.


 **Note:** If you use domain forwarding, SSL requests to the root domain may fail if the SSL certificate only matches the subdomain. For more information about SSL certificates, see [Configuring Trusted System Certificates for Applications](#).

Configure the root domain to point at a subdomain such as `www`, and configure the subdomain as a CNAME record pointing at a shared domain in PAS.

| Record         | Name                                    | Target                                       | Note                                                                                         |
|----------------|-----------------------------------------|----------------------------------------------|----------------------------------------------------------------------------------------------|
| URL or Forward | <code>private-domain.example.com</code> | <code>www.private-domain.example.com</code>  | This method results in a <code>301 permanent redirect</code> to the subdomain you configure. |
| CNAME          | <code>www</code>                        | <code>myapp.shared-domain.example.com</code> |                                                                                              |

## Managing Services

The following list provides information about managing service instances:

- [Services Overview](#) 
- [Managing Service Instances](#)
- [Sharing Service Instances](#)
- [Delivering Service Credentials to an App](#)
- [Managing Service Keys](#)
- [Configuring Play Framework Service Connections](#)
- [Using an External File System \(Volume Services\)](#)
- [User-Provided Service Instances](#)

## Managing Service Instances with the cf CLI

Page last updated:

This topic describes lifecycle operations for service instances, including creating, updating, and deleting. For an overview of services, and documentation about other service management operations, see [Services Overview](#). If you are interested in building services for Cloud Foundry and making them available to end users, see the [Custom Services](#) documentation.

To run the commands in this topic, you must first install the Cloud Foundry Command Line Interface (cf CLI). See the [Cloud Foundry Command Line Interface](#) topics for more information.

### List Marketplace Services

After targeting and logging into Cloud Foundry, run the `cf marketplace` cf CLI command to view the services available to your targeted organization.

Available services may differ between organizations and between Cloud Foundry marketplaces.

```
$ cf marketplace
Getting services from marketplace in org my-org / space test as user@example.com...
OK

service plans description
p-mysql 100mb, 1gb A DBaaS
p-riakcs developer An S3-compatible object store
```

### Creating Service Instances

You can create a service instance with the following command: `cf create-service SERVICE PLAN SERVICE_INSTANCE`

Use the information in the list below to replace `SERVICE`, `PLAN`, and `SERVICE_INSTANCE` with appropriate values.

- `SERVICE`: The name of the service you want to create an instance of.
- `PLAN`: The name of a plan that meets your needs. Service providers use **plans** to offer varying levels of resources or features for the same service.
- `SERVICE_INSTANCE`: The name you provide for your service instance. You use this name to refer to your service instance with other commands. Service instance names can include alpha-numeric characters, hyphens, and underscores, and you can rename the service instance at any time.

```
$ cf create-service rabbitmq small-plan my-rabbitmq

Creating service my-rabbitmq in org console / space development as user@example.com...
OK
```

**User Provided Service Instances** provide a way for developers to bind applications with services that are not available in their Cloud Foundry marketplace. For more information, see the [User Provided Service Instances](#) topic.

### Arbitrary Parameters

*Arbitrary parameters require cf CLI v6.12.1+*

Some services support providing additional configuration parameters with the provision request. Pass these parameters in a valid JSON object containing service-specific configuration parameters, provided either in-line or in a file. For a list of supported configuration parameters, see the documentation for the particular service offering.

Example providing service-specific configuration parameters in-line:

```
$ cf create-service my-db-service small-plan my-db -c '{"storage_gb":4}'

Creating service my-db in org console / space development as user@example.com...
OK
```

Example providing service-specific configuration parameters in a file:

```
$ cf create-service my-db-service small-plan my-db -c /tmp/config.json

Creating service my-db in org console / space development as user@example.com...
OK
```

## Instance Tags

*Instance tags require cf CLI v6.12.1+*

Some services provide a list of tags that Cloud Foundry delivers in the [VCAP\\_SERVICES Environment Variable](#). These tags provide developers with a more generic way for applications to parse `VCAP_SERVICES` for credentials. Developers may provide their own tags when creating a service instance by including the `-t` flag followed by a comma-separated list of tags.

Example providing a comma-separated list of tags:

```
$ cf create-service my-db-service small-plan my-db -t "prod, workers"

Creating service my-db in org console / space development as user@example.com...
OK
```

## List Service Instances

Run the `cf services` command to list the service instances in your targeted space. The output from running this command includes any bound apps and the state of the last requested operation for the service instance.

```
$ cf services
Getting services in org my-org / space test as user@example.com...
OK

name service plan bound apps last operation
mybucket p-riacks developer myapp create succeeded
mydb p-mysql 100mb create succeeded
```

## Get Details for a Particular Service Instance

Details include dashboard urls, if applicable, and operation start and last updated timestamps.

```
$ cf service mydb

Service instance: mydb
Service: p-mysql
Plan: 100mb
Description: MySQL databases on demand
Documentation url:
Dashboard: https://p-mysql.example.com/manage/instances/abed-ef12-3456

Last Operation
Status: create succeeded
Message:
Started: 2015-05-08T22:59:07Z
Updated: 2015-05-18T22:01:26Z
```

## Bind a Service Instance

Depending on the service, you can bind service instances to applications and/or routes.

Not all services support binding, as some services deliver value to users directly without integration with Cloud Foundry, such as SaaS applications.




## Bind a Service Instance to an Application

Depending on the service, binding a service instance to your application may deliver credentials for the service instance to the application. See the [Delivering Service Credentials to an Application](#) topic for more information. Binding a service instance to an application may also trigger application logs to be streamed to the service instance. For more information, see [Streaming Application Logs to Log Management Services](#).

```
$ cf bind-service my-app mydb
Binding service mydb to my-app in org my-org / space test as user@example.com...
OK
TIP: Use 'cf push' to ensure your env variable changes take effect

$ cf restart my-app
```

 **Note:** You must restart or in some cases re-push your application for changes to be applied to the `VCAP_SERVICES` environment variable and for the application to recognize these changes.

### Binding with Application Manifest

As an alternative to binding a service instance to an application after pushing an application, you can use the application manifest to bind the service instance during push. As of cf CLI v6.12.1, [Arbitrary Parameters](#) are not supported in application manifests. Using the manifest to bind service instances to routes is also not supported.

The following excerpt from an application manifest binds a service instance called `test-mysql-01` to the application on push.

```
services:
- test-mysql-01
```

The following excerpt from the `cf push` command and response demonstrates that the cf CLI reads the manifest and binds the service instance to an app called `test-msg-app`.

```
$ cf push
Using manifest file /Users/Bob/test-apps/test-msg-app/manifest.yml
...

Binding service test-mysql-01 to test-msg-app in org My-Org / space development as user@example.com
OK
```

For more information about application manifests, see [Deploying with Application Manifests](#).

## Bind a Service Instance to a Route

Binding a service instance to a route will cause application requests and responses to be proxied through the service instance, where it may be used to transform or intermediate requests. For more information, see [Manage Application Requests with Route Services](#).

```
$ cf bind-route-service shared-domain.example.com --hostname my-app my-service-instance
Binding route my-app.shared-domain.example.com to service instance my-service-instance in org my-org / space test as user@example.com...
OK
```

Restaging your application is not required.

## Arbitrary Parameters

*Arbitrary parameters require cf CLI v6.12.1+*

Some services support additional configuration parameters with the bind request. These parameters are passed in a valid JSON object containing service-specific configuration parameters, provided either in-line or in a file. For a list of supported configuration parameters, see documentation for the particular service offering.

```
$ cf bind-service rails-sample my-db -c '{"role":"read-only"}'
```

```
Binding service my-db to app rails-sample in org console / space development as user@example.com...
OK
```

```
$ cf bind-service rails-sample my-db -c /tmp/config.json
```

```
Binding service my-db to app rails-sample in org console / space development as user@example.com... OK
```


## Unbind a Service Instance

### Unbind a Service Instance from an Application

Unbinding a service instance from an application removes the credentials created for your application from the [VCAP\\_SERVICES](#) environment variable.


```
$ cf unbind-service my-app mydb
```

```
Unbinding app my-app from service mydb in org my-org / space test as user@example.com...
OK
```

 **Note:** You must restart or in some cases re-push your application for changes to be applied to the [VCAP\\_SERVICES](#) environment variable and for the application to recognize these changes.

### Unbind a Service Instance from a Route

Unbinding a service instance from a route will result in requests and responses no longer being proxied through the service instance. For more information, see [Manage Application Requests with Route Services](#).

 **Note:** If your bound service instance is providing security features, like authorization, unbinding the service instance may leave your application vulnerable.

```
$ cf unbind-route-service shared-domain.example.com --hostname my-app my-service-instance
```

```
Unbinding may leave apps mapped to route my-app.shared-domain.example.com vulnerable; e.g. if service instance my-service-instance provides authentication. Do you want to proceed?> y
```

```
Unbinding route my-app.shared-domain.example.com from service instance my-service-instance n org my-org / space test as user@example.com...
OK
```

Restaging your application is not required.

## Rename a Service Instance

You can change the name given to a service instance. Keep in mind that upon restarting any bound applications, the name of the instance will change in the [VCAP\\_SERVICES](#) environment variable. If your application depends on the instance name for discovering credentials, changing the name could break your application's use of the service instance.

```
$ cf rename-service mydb mydb1
```

```
Renaming service mydb to mydb1 in org my-org / space test as user@example.com...
OK
```

## Update a Service Instance

### Upgrade/Downgrade Service Plan

*Changing a plan requires cf CLI v6.7+ and cf-release v192+*

By updating the service plan for an instance, users can effectively upgrade and downgrade their service instance to other service plans. Though the platform and CLI now support this feature, services must expressly implement support for it so not all services will. Further, a service might support updating between some plans but not others. For instance, a service might support updating a plan where only a logical change is required, but not where data migration is necessary. In either case, users can expect to see a meaningful error when plan update is not supported.

```
$ cf update-service mydb -p new-plan
Updating service instance mydb as user@example.com...
OK
```

## Arbitrary Parameters

*Arbitrary parameters require cf CLI v6.12.1+*

Some services support additional configuration parameters with the update request. These parameters are passed in a valid JSON object containing service-specific configuration parameters, provided either in-line or in a file. For a list of supported configuration parameters, see documentation for the particular service offering.

```
$ cf update-service mydb -c '{"storage_gb":4}'
Updating service instance mydb as me@example.com...
```

```
$ cf update-service mydb -c /tmp/config.json
Updating service instance mydb as user@example.com...
```

## Instance Tags

*Instance tags require cf CLI v6.12.1+*

Some services provide a list of tags that Cloud Foundry delivers in the [VCAP\\_SERVICES Environment Variable](#). These tags provide developers with a more generic way for applications to parse `VCAP_SERVICES` for credentials. Developers may provide their own tags when creating a service instance by including a comma-separated list of tags with the `-t` flag.

```
$ cf update-service my-db -t "staging, web"
Updating service my-db in org console / space development as user@example.com...
OK
```

## Delete a Service Instance

Deleting a service instance deprovisions the service instance and deletes all data associated with the service instance.

```
$ cf delete-service mydb

Are you sure you want to delete the service mydb ? y
Deleting service mydb in org my-org / space test as user@example.com...
OK
```

## Sharing Service Instances (Beta)

**⚠ warning:** Service instance sharing is a beta feature and may be removed at any time without notice. Use at your own risk.

This topic explains how to use service instance sharing.

### About Service Instance Sharing

Sharing a service instance between spaces allows apps in different spaces to share databases, messaging queues, and other types of services. This eliminates the need for development teams to use service keys and user-provided services to bind their apps to the same service instance that was provisioned using the `cf create-service` command. Sharing service instances improves security, auditing, and provides a more intuitive user experience.

- Service instances can be shared into multiple spaces and across orgs.
- Developers and administrators can share service instances between spaces in which they have the Space Developer role.
- Developers who have a service instance shared with them can only bind and unbind apps to that service instance. They cannot update, rename, or delete it.
- Developers who have a service instance shared with them can view the values of any configuration parameters that were used to provision or update the service instance.

For example, if two development teams have apps in their own spaces, and both of those apps want to send messages to each other using a messaging queue, you can do the following:

1. The development team in space A can create a new instance of a messaging queue service, bind it to their app, and share that service instance into space B.
2. A developer in space B can then bind their app to the same service instance, and the two apps can begin publishing and receiving messages from one another.

### Enabling Service Instance Sharing in Cloud Foundry

To enable service instance sharing, you must enable the `service_instance_sharing` flag.

```
$ cf enable-feature-flag service_instance_sharing
```

### Sharing a Service Instance

You can share a service instance from one space to another if you have the Space Developer role in both spaces.

To share a service instance to another space, run the following beta Cloud Foundry Command Line Interface (cf CLI) command:

```
$ cf share-service SERVICE-INSTANCE -s OTHER-SPACE [-o OTHER-ORG]
```

- You cannot share a service instance into a space where a service instance with the same name already exists.
- To share a service instance into a space, the space must have access to the service and service plan of the service instance that you are sharing. Run the `cf enable-service-access` command to set this access.
- If you no longer have access to the service or service plan used to create your service instance, you cannot share that service instance.

### Unsharing a Service Instance

**⚠ warning:** Unsharing a service instance automatically deletes all bindings to apps in the spaces it was shared into. This may cause apps to fail. Before unsharing a service instance, run the `cf service SERVICE-INSTANCE` command to see how many bindings exist in the spaces the service instance is shared into.

You can unshare a service instance if you have the Space Developer role in the space where this service instance was shared from.

Developers cannot delete or rename a service instance until it is unshared from all spaces.

To unshare a service instance, run the following beta cf CLI command:

```
$ cf unshare-service SERVICE-INSTANCE -s OTHER-SPACE [-o OTHER-ORG] [-f]
```

The optional `-f` flag forces unsharing without confirmation.

## Security Considerations

- [Service keys](#) cannot be created from a space that a service instance has been shared into. This ensures that developers in the space where a service instance has been shared from have visibility into where and how many times the service instance is used.
- Sharing service instances does not automatically update app security groups (ASGs). The network policies defined in your ASGs may need to be updated to ensure that apps using shared service instances can access the underlying service.
- Access to a service must be enabled using the `cf enable-service-access` command for a service instance to be shared into a space.
- Not all services are enabled for sharing instances functionality. Contact the service vendor directly if you are unable to share instances of their service. If you are a service author, see [Enabling Service Instance Sharing](#).

## Disabling Service Instance Sharing in Cloud Foundry

To disable service instance sharing, run the following command:

```
$ cf disable-feature-flag service_instance_sharing
```


This only prevents new shares from being created. To remove existing shares, see [Deleting All Shares](#).

## Deleting All Shares

The script below finds all service instances that are shared, and for each space that the service instance is shared into, all service bindings to that service instance are deleted, and all shares are deleted.

If a service binding is not successfully deleted, the script continues trying to unshare subsequent service instances.

To use this script, you must be logged in as an administrator and have jq installed.

 **Note:** This script has been tested on macOS Sierra 10.12.4 and Ubuntu 14.04.5. Use the script at your own risk.

```
#!/usr/bin/env bash

set -u
set -e

refresh auth token
cf oauth-token >/dev/null

for instance_guid in $(cf curl /v3/service_instances | jq -r '.resources[].guid'); do
 for space_guid in $(cf curl /v2/service_instances/$instance_guid/shared_to | jq -r '.resources[].space_guid'); do
 echo "Unsharing service instance $instance_guid from space $space_guid"

 set +e
 cf curl -X DELETE "/v3/service_instances/$instance_guid/relationships/shared_spaces/$space_guid"
 set -e
 done
done
```



## Delivering Service Credentials to an Application

Page last updated:

This topic describes binding applications to service instances for the purpose of generating credentials and delivering them to applications. For an overview of services, and documentation on other service management operations, see [Using Services](#). If you are interested in building services for Cloud Foundry and making them available to end users, see the [Custom Services](#) documentation.


### Bind a Service Instance

Binding a service instance to your application triggers credentials to be provisioned for the service instance and delivered to the application runtime in the `VCAP_SERVICES` environment variable. For details on consuming these credentials with your application, see [Using Bound Service Instances](#).

Not all services support binding, as some services deliver value to users directly without integration with an application. In many cases binding credentials are unique to an application, and another app bound to the same service instance would receive different credentials; however this depends on the service.

```
$ cf bind-service my-app mydb
Binding service mydb to my-app in org my-org / space test as me@example.com...
OK
TIP: Use 'cf push' to ensure your env variable changes take effect

$ cf restart my-app
```

 **Note:** You must restart or in some cases re-push your application for changes to be applied to the `VCAP_SERVICES` environment variable and for the application to recognize these changes.

### Arbitrary Parameters

*Arbitrary parameters require Cloud Foundry Command Line Interface (cf CLI) v6.12.1 or later.*

Some services support additional configuration parameters with the bind request. These parameters are passed in a valid JSON object containing service-specific configuration parameters, provided either in-line or in a file. For a list of supported configuration parameters, see documentation for the particular service offering.

```
$ cf bind-service rails-sample my-db -c '{"role":"read-only"}'

Binding service my-db to app rails-sample in org console / space development as user@example.com...
OK
```

```
$ cf bind-service rails-sample my-db -c /tmp/config.json

Binding service my-db to app rails-sample in org console / space development as user@example.com... OK
```

### Binding with Application Manifest

As an alternative to binding a service instance after pushing an application, you can use the application manifest to bind the service instance during push. As of cf CLI v6.12.1, [Arbitrary Parameters](#) are not supported in application manifests.

The following excerpt from an application manifest would bind a service instance called `test-mysql-01` to the application on push.

```
services:
- test-mysql-01
```

The following excerpt from the `cf push` command and response demonstrates that the cf CLI reads the manifest and binds the service instance to an app called `test-msg-app`.

```
$ cf push
Using manifest file /Users/Bob/test-apps/test-msg-app/manifest.yml

...

Binding service test-mysql-01 to test-msg-app in org My-Org / space development as Bob@shared-domain.example.com
OK
```

For more information about application manifests, see [Deploying with Application Manifests](#).

## Named Service Bindings

Service offering and service instance names vary across environments. App authors can discover the service instances their apps require, without having to know environment-specific service names. Developers can specify a service binding name to be included in [VCAP\\_SERVICES](#).

To specify the service binding name, provide the `--binding-name` flag when binding an app to a service instance:

```
$ cf bind-service my-app my-service --binding-name postgres-database
OK
```

The provided name will be available in the `name` and `binding_name` properties in the [VCAP\\_SERVICES](#) environment variable:

```
"VCAP_SERVICES": {
 "service-name": [
 {
 "name": "postgres-database",
 "binding_name": "postgres-database",
 ...
 }
]
}
```

## Using Bound Service Instances

Once you have a service instance created and bound to your application, you need to configure the application to dynamically fetch the credentials for your service instance. The [VCAP\\_SERVICES](#) environment variable contains credentials and additional metadata for all bound service instances. There are two methods developers can leverage to have their applications consume binding credentials.

- **Parse the JSON yourself:** See the documentation for [VCAP\\_SERVICES](#). Helper libraries are available for some frameworks.
- **Auto-configuration:** Some buildpacks create a service connection for you by creating additional environment variables, updating config files, or passing system parameters to the JVM.

For details on consuming credentials specific to your development framework, refer to the Service Binding section in the documentation for [your framework's buildpack](#).

## Update Service Credentials

To update your service credentials, perform the following steps:

1. [Unbind the service instance](#) using the credentials you are updating with the following command:

```
$ cf unbind-service YOUR-APP YOUR-SERVICE-INSTANCE
```

2. [Bind the service instance](#) with the following command. This adds your credentials to the [VCAP\\_SERVICES](#) environment variable.

```
$ cf bind-service YOUR-APP YOUR-SERVICE-INSTANCE
```


3. Restart or re-push the application bound to the service instance so that the application recognizes your environment variable updates.



## Unbind a Service Instance

Unbinding a service removes the credentials created for your application from the [VCAP\\_SERVICES](#) environment variable.

```
$ cf unbind-service my-app mydb
Unbinding app my-app from service mydb in org my-org / space test as me@example.com...
OK
```


 **Note:** You must restart or in some cases re-push your application for changes to be applied to the [VCAP\\_SERVICES](#) environment variable and for the application to recognize these changes.

## Managing Service Keys

Page last updated:

This topic describes managing service instance credentials with service keys.

Service keys generate credentials for manually configuring consumers of marketplace services. Once you configure them for your service, local clients, apps in other spaces, or entities outside your deployment can access your service with these keys.

 **Note:** Some service brokers do not support service keys. If you want to build a service broker that supports service keys, see [Services](#). If you want to use a service broker that does not support service keys, see [Delivering Service Credentials to an Application](#).

## Create a Service Key

To generate credentials for a service instance, use the `cf create-service-key` command:

```
$ cf create-service-key MY-SERVICE MY-KEY
Creating service key MY-KEY for service instance MY-SERVICE as me@example.com...
OK
```

Use the `-c` flag to provide service-specific configuration parameters in a valid JSON object, either in-line or in a file.

To provide the JSON object in-line, use the following format:

```
$ cf create-service-key MY-SERVICE MY-KEY -c '{"read-only":true}'
Creating service key MY-KEY for service instance MY-SERVICE as me@example.com...
OK
```

To provide the JSON object as a file, give the absolute or relative path to your JSON file:

```
$ cf create-service-key MY-SERVICE MY-KEY -c PATH-TO-JSON-FILE
Creating service key MY-KEY for service instance MY-SERVICE as me@example.com...
OK
```

## List Service Keys for a Service Instance

To list service keys for a service instance, use the `cf service-keys` command:

```
$ cf service-keys MY-SERVICE
Getting service keys for service instance MY-SERVICE as me@example.com...

name
mykey1
mykey2
```

## Get Credentials for a Service Key

To retrieve credentials for a service key, use the `cf service-key` command:

```
$ cf service-key MY-SERVICE MY-KEY
Getting key MY-KEY for service instance MY-SERVICE as me@example.com...

{
 uri: foo://user2:pass2@example.com/mydb,
 servicename: mydb
}
```

Use the `--guid` flag to display the API GUID for the service key:

```
$ cf service-key --guid MY-SERVICE MY-KEY
Getting key MY-KEY for service instance MY-SERVICE as me@example.com...

e3696fcb-7a8f-437f-8692-436558e45c7b

OK
```

## Configure Credentials for a Service Key

Once these credentials are obtained, you can use a local CLI or utility to connect to the service instance, configure an application running outside the platform to connect to the service instance, or create a user-provided service instance so that applications in another space can connect to the service instance. How you configure these credentials will depend on what local client, app, or entity is used to access your service instance.

For more information on configuring credentials with a user-provided service instance, see [User-Provided Service Instances](#).

## Delete a Service Key

To delete a service key, use the `cf delete-service-key` command:

```
$ cf delete-service-key MY-SERVICE MY-KEY

Are you sure you want to delete the service key MY-KEY ? y
Deleting service key MY-KEY for service instance MY-SERVICE as me@example.com...

OK
```

Add option `-f` to force deletion without confirmation.

```
$ cf delete-service-key -f MY-SERVICE MY-KEY

Deleting service key MY-KEY for service instance MY-SERVICE as me@example.com...

OK
```

## Configuring Play Framework Service Connections

Page last updated:


Cloud Foundry provides support for connecting a Play Framework application to services such as MySQL, and Postgres. In many cases, a Play Framework application running on Cloud Foundry can automatically detect and configure connections to services.

### Auto-Configuration

By default, Cloud Foundry will detect service connections in a Play Framework application and configure them to use the credentials provided in the Cloud Foundry environment. Auto-configuration will only happen if there is a single service of any of the supported types - MySQL or Postgres.

## Using an External File System (Volume Services)

This topic describes how Pivotal Cloud Foundry (PCF) app developers can read and write to a mounted file system from their apps. In PCF, a volume service provides a volume so your app can read or write to a reliable, non-ephemeral file system.

 **Note:** The NFS volume service is available for Linux cells only. This service is not available for Windows cells.

### Prerequisite

Before you can use a volume service with your app, your Cloud Foundry administrator must add a volume service to your deployment. See the [Enabling NFS Volume Services](#) topic for more information.

You can run the Cloud Foundry Command Line Interface (cf CLI) `cf marketplace` command to determine if any volume services are available. See the following example output of the NFS volume service:

```
$ cf marketplace
service plans description
nfs Existing Service for connecting to NFS volumes
```


If no volume service that fits your requirements exists, contact your Cloud Foundry administrator.

## Mount an External Filesystem

The sections below describe how to mount an external filesystem to your app.

### Create and Bind a Service Instance

To use a volume service deployed by your Cloud Foundry administrator, you must first create an instance of the specific volume service that you need. Follow the instructions below to create this service instance.


 **Note:** For NFS-specific instructions and information, see [NFS Volume Service](#).

- In a terminal window, run `cf create-service SERVICE-NAME PLAN SERVICE-INSTANCE -c SHARE-JSON` to create a service instance. Replace the following with the specified values:
  - `SERVICE`: The name of the volume service that you want to use.
  - `PLAN`: The name of the service plan. Service plans are a way for providers to offer varying levels of resources or features for the same service.
  - `SERVICE-INSTANCE`: A name you provide for your service instance. Use any series of alpha-numeric characters, hyphens, and underscores. You can rename the instance at any time.
  - `SHARE-JSON` (NFS Only): If you create an instance of the NFS volume service, you must supply an extra parameter, `share`, by using the `-c` flag with a JSON string, in-line or in a file. This parameter forwards information to the broker about the NFS server and share required for the service.

The following example shows creating an instance of the “Existing” NFS service plan, passing an in-line JSON string:

```
$ cf create-service nfs Existing nfs_service_instance -c '{"share": "10.10.10.10/export/myshare"}'
```

- Run `cf bind-service YOUR-APP SERVICE-NAME -c GID-AND-UID-JSON MOUNT-PATH READ-ONLY-TRUE` to bind your service instance to an app. Replace the following with the specified values:
  - `YOUR-APP`: The name of the PCF app for which you want to use the volume service.
  - `SERVICE-NAME`: The name of the volume service instance you created in the previous step.
  - `GID-AND-UID-JSON` (NFS only): If you bind an instance of the NFS volume service, you must supply two extra parameters, `gid` and `uid`. You can specify these parameters with the `-c` flag and a JSON string, in-line or from a file. This parameter specifies the `gid` and `uid` to use when mounting the share to the app.
  - `MOUNT-PATH` (Optional): To mount the volume to a particular path within your app rather than the default path, you supply the `mount` parameter. Choose a path with a root-level folder that already exists in the container, such as `/home`, `/usr`, or `/var`.

 **Note:** Do not specify a `MOUNT-PATH` within the `/app` directory. For more information, see [Mount Path Limitation](#).

- `READ-ONLY-TRUE` (Optional): When you issue the `cf bind-service` command, Volume Services mounts a read-write file system by default. You can specify a read-only mount by adding `"readonly":true` to the bind configuration JSON string.

The following example shows binding `my-app` to the `nfs_service_instance` and specifying a read-only volume to be mounted to `/var/volume1`, passing an in-line JSON string:

```
$ cf bind-service my-app nfs_service_instance -c '{"uid":"1000","gid":"1000","mount":"/var/volume1","readonly":true}'
```

If you use an LDAP server, you must specify `username` and `password` instead of a UID and GID in this command. For example:

```
$ cf bind-service my-app nfs_service_instance -c '{"username":"user1000","password":"secret","mount":"/var/volume1","readonly":true}'
```

3. Run `cf restage YOUR-APP` to complete the service binding by restaging your app. Replace `YOUR-APP` with the name of your app.

```
$ cf restage my-app
```

## Access the Volume Service from your App

To access the volume service from your app, you must know which file path to use in your code. You can view the file path in the details of the service binding, which are available from the `VCAP_SERVICES` environment variable. Follow the steps below.

1. Run `cf env YOUR-APP` to view environment variables for your app. Replace `YOUR-APP` with the name of your app.

```
$ cf env my-app
"VCAP_SERVICES": {
 "nfs": [
 {
 "credentials": {},
 "label": "nfs",
 "name": "nfs_service_instance",
 "plan": "Existing",
 "provider": null,
 "syslog_drain_url": null,
 "tags": [
 "nfs"
],
 "volume_mounts": [
 {
 "container_dir": "/var/vcap/data/153e3c4b-1151-4cf7-b311-948dd77fce64",
 "device_type": "shared",
 "mode": "rw"
 }
]
 }
]
}
```

2. Use the properties under `volume_mounts` for any information your app needs. Refer to the following table:

| Property                   | Description                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>container_dir</code> | String containing the path to the mounted volume that you bound to your app.                                                                                                                            |
| <code>device_type</code>   | The NFS volume release. This currently only supports <code>shared</code> devices. A <code>shared</code> device represents a distributed file system that can mount on all app instances simultaneously. |
| <code>mode</code>          | String that informs what type of access your app has to NFS, either read-only, <code>ro</code> , or read and write, <code>rw</code> .                                                                   |

## Bind with an App Manifest

You can also bind volume services using an app manifest as described in the [Services](#) section of the *Deploying with App Manifests* topic. However, app manifests do not support bind configuration. If you want to bind a volume service using an app manifest, you must specify bind configuration when you create the service instance. The releases that support this are `nfs-volume` v1.3.1 and later and `smb-volume` v1.0.0 and later.

## Mount Path Limitation

Do not specify a `MOUNT-PATH` within the `/app` directory, which is where PAS unpacks the droplet. If you specify a mount inside the `/app` directory, the app may fail to start and parts of the app droplet may be written to the remote file share. This is because PAS mounts the volume before moving your compiled app into the droplet.

If your app requires the shared volume to be placed within the `/app` directory, do the following:

1. Specify a mount volume in a location outside of the `/app` directory.
2. Create a symbolic link at app startup time, prior to launching the app. For example:

```
cf push my-app -c "ln -s /var/volume1 /app/volume1 && $HOME/boot.sh"
```

## NFS Volume Service

This section describes how to use the NFS volume service.

### Create an NFS Volume Service

Cloud Foundry offers two NFS volume services:

- `nfs`: This volume service is implemented with libfuse. It only supports NFSv3 and has some performance constraints.
- `nfs-experimental`: This volume service provides better performance.
  - For read-only mounts, the driver enables attribute caching. This results in fewer attribute RPCs and better performance.
  - It skips `mapfs` mounting and performs a normal kernel mount of the NFS file system without the overhead associated with FUSE mounts when you omit `uid` and `gid` or `username` and `password` in bind configuration.

Both services offer a single plan called `Existing`.

To create an NFS volume service, follow the procedure below that corresponds to your use case.


#### Create with `nfs` Service

You can create a NFS volume service with NFSv3 using the `Existing` plan of the `nfs` service. Run the following command:

```
$ cf create-service nfs Existing SERVICE-INSTANCE-NAME -c '{"share":"SERVER/SHARE"}'
```

Where:

- `SERVICE-INSTANCE-NAME` is a name you provide for this NFS volume service instance.
- `SERVER/SHARE` is the NFS address of your server and share.

 **Note:** Ensure you omit the `:` that usually follows the server name in the address.

You can run the `cf services` command to confirm that your newly-created NFS volume service displays in the output.

#### Create with `nfs-experimental` Service:


You can create a NFS volume service with NFSv3 or NFSv4 using the `Existing` plan of the `nfs-experimental` service. Run the following command:

```
$ cf create-service nfs-experimental Existing SERVICE-INSTANCE-NAME -c '{"share":"SERVER/SHARE"}'
```

Where:

- `SERVICE-INSTANCE-NAME` is a name you provide for this NFS volume service instance.

- `SERVER/SHARE` is the NFS address of your server and share.

 **Note:** Ensure you omit the `:` that usually follows the server name in the address.

You can run the `cf services` command to confirm that your newly-created NFS volume service displays in the output.

## Deploy and Bind a Sample App

This section describes how to deploy a sample app and bind it to the NFS volume service.

1. Clone the github repo and push the `pora` test app:

- a. `cd ~/workspace`
- b. `git clone https://github.com/cloudfoundry/persi-acceptance-tests.git`
- c. `cd ~/workspace/persi-acceptance-tests/assets/pora`
- d. `cf push pora --no-start`

2. To bind the service to your app, run the following command:

```
$ cf bind-service pora SERVICE-INSTANCE-NAME -c '{"uid":"UID","gid":"GID"}'
```

Where:

- `SERVICE-INSTANCE-NAME`: The name of the volume service instance you created previously.
- `UID` and `GID`: The `gid` and `uid` to use when mounting the share to the app. The NFS driver uses these values in the following ways:
  - When sending traffic to the NFS server, the NFS driver translates the app user id and group id to the `UID` and `GID` values.
  - When returning attributes from the NFS server, the NFS driver translates the `UID` and `GID` back to the running user uid and default gid.

This allows you to interact with your NFS server as a specific user while allowing Cloud Foundry to run your application as an arbitrary user.

- **Optional parameters:**
  - `mount`: Use this option to specify the path at which volumes mount to the app container. The default is an arbitrarily-named folder in `/var/vcap/data`. You may need to modify this value if your app has specific requirements. For example:
 

```
cf bind-service pora myVolume -c '{"uid":"0","gid":"0","mount":"/var/path"}'
```
  - `readonly`: When you issue the `cf bind-service` command, Volume Services mounts a read-write file system by default. You can specify a read-only mount by adding `"readonly":true` to the bind configuration JSON string.

3. Start the app:

```
$ cf start pora
```

4. Use the following `curl` command to confirm the app is running. The command returns an instance index for your app.

```
$ curl http://pora.YOUR-CF-DOMAIN.com
```

5. Use the following `curl` command to confirm the app can access the shared volume. The command writes a file to the share and then reads it back out again.

```
$ curl http://pora.YOUR-CF-DOMAIN.com/write
```

## Additional Information

This section provides additional information about using the NFS Volume Service.

### Binding with LDAP Credentials

If your Cloud Foundry deployment has LDAP enabled, you can bind using LDAP credentials.



To bind an app to your volume using LDAP credentials, specify `username` and `password` instead of `uid` and `gid`. See the following example:

```
$ cf bind-service pora myVolume -c '{"username":"USERNAME","password":"PASSWORD"}
```



**Note:** If your LDAP server password changes, you must re-bind your app to the service and restage. If you do not, your app will fail during restart or scaling. This is because user credentials are stored as part of the service binding and checked whenever an app is placed on a cell.

## Specifying Bind Parameters During Service Instance Creation

As of `nfs-volume-release` v1.3.1, you can specify bind parameters in advance, when you create a service instance. Use this option if you bind the service to your app in an app manifest, where bind configuration is not supported.

## File Locking with `flock()` and `lockf()` / `fcntl()`


For apps that use file locking through unix system calls such as `flock()` and `fcntl()` or script commands such as `flock`, NFS volume service does not enforce the locking across Diego cells. This is because the file locking capability of the underlying `fuse-nfs` executable is not implemented. Locking is therefore limited to local locks between precesses on the same VM.

If you have a requirement for file locking, describe your use case in the following Github issue for consideration by the Diego Persistence team: [lock not propagated between instances](#).

## User-Provided Service Instances

Page last updated:

This topic describes how to create and update user-provided service instances.

 **Note:** The procedures in this topic use the Cloud Foundry Command Line Interface (cf CLI). You can also create user-provided service instances in Apps Manager from the Marketplace. To update existing user-provided service instances, navigate to the service instance page and select the **Configuration** tab.

### Overview

User-provided service instances enable developers to use services that are not available in the marketplace with their applications running on Cloud Foundry.

User-provided service instances can be used to deliver service credentials to an application, and/or to trigger streaming of application logs to a syslog compatible consumer. These two functions can be used alone or at the same time.

Once created, user-provided service instances behave like service instances created through the marketplace; see [Managing Service Instances](#) and [Application Binding](#) for details on listing, renaming, deleting, binding, and unbinding.

## Create a User-Provided Service Instance

The alias for [cf create-user-provided-service](#) is `cf cups`.

### Deliver Service Credentials to an Application

Suppose a developer obtains a URL, port, username, and password for communicating with an Oracle database managed outside of Cloud Foundry. The developer could manually create custom environment variables to configure their application with these credentials (of course you would never hard code these credentials in your application!).

User-provided service instances enable developers to configure their applications with these using the familiar [Application Binding](#) operation and the same application runtime environment variable used by Cloud Foundry to automatically deliver credentials for marketplace services ([VCAP\\_SERVICES](#)).

```
cf cups SERVICE_INSTANCE -p '{"username":"admin","password":"pa55woRD"}'
```

To create a service instance in interactive mode, use the `-p` option with a comma-separated list of parameter names. The Cloud Foundry Command Line Interface (cf CLI) prompts you for each parameter value.

```
$ cf cups my-user-provided-route-service -p "host, port"

host> rdb.local

port> 5432

Creating user provided service my-user-provided-route-service in org my-org / space my-space as user@example.com...
OK
```

Once the user-provided service instance is created, to deliver the credentials to one or more applications see [Application Binding](#).

### Stream Application Logs to a Service

User-provided service instances enable developers to stream applications logs to a syslog compatible aggregation or analytics service that isn't available in the marketplace. For more information about the syslog protocol see [RFC 5424](#) and [RFC 6587](#).

Create the user-provided service instance, specifying the URL of the service with the `-l` option.

```
cf cups SERVICE_INSTANCE -l syslog://example.log-aggregator.com
```

To stream application logs to the service, bind the user-provided service instance to your app.

## Proxy Application Requests to a Route Service

User-provided service instances enable developers to proxy application requests to [route services](#) for preprocessing. To create a user-provided service instance for a route service, specify the url for the route service using the `-r` option.

```
$ cf create-user-provided-service my-user-provided-route-service -r https://my-route-service.example.com
Creating user provided service my-user-provided-route-service in org my-org / space my-space as user@example.com...
OK
```

 **Note:** When creating the user-provided service, the route service url specified must be https.

To proxy requests to the user-provided route service, you must bind the service instance to the route. For more information, see [Manage Application Requests with Route Services](#).

## Update a User-provided Service Instance

You can use [cf update-user-provided-service](#) to update the attributes of an instance of a user-provided service. New credentials overwrite old credentials, and parameters not provided are deleted.

The alias for `update-user-provided-service` is `uups`.

Streaming index

---

title: Streaming App Logs

## owner:

The following list provides information about streaming app logs:

- [Streaming App Logs to Log Management Services](#)
- [Service-Specific Instructions for Streaming App Logs](#)
- [Streaming App Logs to Splunk](#)
- [Streaming App Logs with Fluentd](#)
- [Streaming App Logs to Azure OMS Log Analytics](#)

## Streaming Application Logs to Log Management Services

Page last updated:

This topic describes how to drain logs from Cloud Foundry to a third-party log management service.

Cloud Foundry aggregates logs for all instances of your applications as well as for requests made to your applications through internal components of Cloud Foundry. For example, when the Cloud Foundry Router forwards a request to an application, the Router records that event in the log stream for that app. Run the following command to access the log stream for an app in the terminal:

```
$ cf logs YOUR-APP-NAME
```

If you want to persist more than the limited amount of logging information that Cloud Foundry can buffer, drain these logs to a log management service.

For more information about the systems responsible for log aggregation and streaming in Cloud Foundry, see [Application Logging in Cloud Foundry](#).

## Using Services from the Cloud Foundry Marketplace

Your Cloud Foundry marketplace may offer one or more log management services. To use one of these services, create an instance of the service and bind it to your application with the following commands:

```
$ cf create-service SERVICE PLAN SERVICE-INSTANCE
$ cf bind-service YOUR-APP YOUR-LOG-STORE
```

For more information about service instance lifecycle management, see the [Managing Service Instances](#) topic.



**Note:** Not all marketplace services support syslog drains. Some services implement an integration with Cloud Foundry that enables automated streaming of application syslogs. If you are interested in building services for Cloud Foundry and making them available to end users, see the [Custom Services](#) [documentation](#).

## Using Services Not Available in Your Marketplace

If a compatible log management service is not available in your Cloud Foundry marketplace, you can use [user-provided service instances](#) to stream application logs to a service of your choice.

You can install and use the [CF Drain CLI Plugin](#) to create and manage user-provided syslog drains from the CF command-line interface (cf CLI).

You may need to prepare your log management service to receive app logs from Cloud Foundry. For specific instructions for several popular services, see [Service-Specific Instructions for Streaming Application Logs](#). If you cannot find instructions for your service, follow the generic instructions below.

### Step 1: Configure the Log Management Service

Complete the following steps to set up a communication channel between the log management service and your Cloud Foundry deployment:

1. Obtain the external IP addresses that your Cloud Foundry administrator assigns to outbound traffic.
2. Provide these IP addresses to the log management service. The specific steps to configure a third-party log management service depend on the service.
3. Whitelist these IP addresses to ensure unrestricted log routing to your log management service.
4. Record the syslog URL provided by the third-party service. Third-party services typically provide a syslog URL to use as an endpoint for incoming log data. You use this syslog URL in Step 2: Create a User-provided Service Instance.

Cloud Foundry uses the syslog URL to route messages to the service. The syslog URL has a scheme of `syslog`, `syslog-tls`, or `https`, and can include a port number. For example:

```
syslog://logs.example.com:1234
```

**Note:** PAS does not support using `syslog-tls` or `https` with self-signed certificates. If you are running your own syslog server and want to use `syslog-tls` or `https`, you must have an SSL certificate signed by a well-known certificate authority.

## Step 2: Create and Bind a User-Provided Service Instance

You can create a syslog drain service and bind apps to it using either generic Cloud Foundry Command Line Interface (cf CLI) commands, or drain-specific commands enabled by the CF Drain plugin for the cf CLI.

Each option is described below.

### With the CF Drain CLI Plugin

1. If the CF Drain CLI Plugin is not installed on your local workstation, follow the [Installing Plugin](#) instructions in the plugin source repository.
2. Decide whether to bind the drain to a single app or all apps in a space, and run the corresponding command:

- **Single app:**

```
cf drain APP-NAME SYSLOG-DRAIN-URL
```

Where:

- `APP-NAME` is name of the app to stream logs from
- `SYSLOG-DRAIN-URL` is the syslog URL from [Step 1: Configure the Log Management Service](#)

- **All apps in a space:**

```
cf drain-space --drain-name DRAIN-NAME --drain-url SYSLOG-DRAIN-URL --username USERNAME
```

Where:

- `DRAIN-NAME` is the name of the app to stream logs from.
- `SYSLOG-DRAIN-URL`: The syslog URL from [Step 1: Configure the Log Management Service](#).
- `USERNAME`: Username to use when pushing the app. If you do not specify a username, you must have admin permissions because the plugin will create a user.

After a short delay, logs begin to flow automatically.

Refer to the [Usage](#) section of the CF Drain plugin source repository for CF Drain commands, and [Managing Service Instances with the CLI](#) for general CF service commands.

### With General cf CLI Service Commands

**Note:** To bind a drain to all apps in a space with a single command, you must use the CF Drain CLI Plugin as described in the previous section.

1. To create the service instance, run `cf create-user-provided-service` (or `cf cups`) with the `-l` flag, filling in values as follows:

- DRAIN-NAME: A name to use for your syslog drain service instance
- SYSLOG-DRAIN-URL: The syslog URL from [Step 1: Configure the Log Management Service](#).

```
$ cf create-user-provided-service DRAIN-NAME -l SYSLOG-URL
```

See [User-Provided Service Instances](#) for more information.

2. To bind an app to the service instance, do one of the following:

- Run `cf push` with a manifest. The services block in the manifest must specify the service instance that you want to bind.
- Run `cf bind-service`

```
$ cf bind-service YOUR-APP-NAME DRAIN-NAME
```

After a short delay, logs begin to flow automatically.

Refer to [Managing Service Instances with the CLI](#) for more information.

## Step 3: Verify Logs Are Draining

To verify that logs are draining correctly to a third-party log management service:

1. Take actions that produce log messages, such as making requests of your app.
2. Compare the logs displayed in the CLI against those displayed by the log management service.

For example, if your application serves web pages, you can send HTTP requests to the application. In Cloud Foundry, these generate Router log messages, which you can view in the CLI. Your third-party log management service should display corresponding messages.

 **Note:** For security reasons, Cloud Foundry applications do not respond to `ping`. You cannot use `ping` to generate log entries.

## CF Drain CLI Plugin

The CF Drain CLI plugin extends the cf CLI by adding simple commands for user-provided syslog drains. Also, you can use the plugin to bind all apps in a space to a syslog drain. This option includes app, space, and org names in the drain. It also binds any new apps pushed to the space.

**Installation:** To install the CF Drain CLI plugin see the [Installing Plugin](#) instructions in the plugin source repository.

**Commands:** The plugin adds commands for creating, deleting, and listing syslog drains, and for binding apps to the drains. See the [Usage](#) section of the plugin source repository for details.

## Service-Specific Instructions for Streaming Application Logs

Page last updated:

This topic provides instructions for configuring some third-party log management services.

Once you have configured a service, refer to the [Third-Party Log Management Services](#) topic for instructions on binding your application to the service.

### Logit.io

From your Logit.io dashboard:

1. Identify the Logit ELK stack you want to use.
2. Click Logstash **Configuration**.
3. Note your Logstash **Endpoint**.
4. Note your TCP-SSL, TCP, or UDP **Port** (not the syslog port).
5. Create the log drain service in Cloud Foundry.

```
$ cf cups logit-ssl-drain -l syslog-tls://ENDPOINT:PORT
```

or

```
$ cf cups logit-drain -l syslog://ENDPOINT:PORT
```

6. Bind the service to an app.

```
$ cf bind-service YOUR-CF-APP-NAME logit-ssl-drain
```

or

```
$ cf bind-service YOUR-CF-APP-NAME logit-drain
```

7. Restage or push the app using one of the following commands:

```
$ cf restage YOUR-CF-APP-NAME
```

```
$ cf push YOUR-CF-APP-NAME
```

After a short delay, logs begin to appear in Kibana.

### Papertrail

From your Papertrail account:

1. Click **Add System**.



2. Click the **Other** link.



## Setup Systems

Your systems will log to **logs2.papertrailapp.com:14608**.

» Other situations: [Port 514](#) | [Other](#)

3. Select **I use Cloud Foundry**, enter a name, and click **Save**.

**Choose your situation:**

☐ **A My syslogd only uses the default port**  
GNU syslogd and some embedded devices will only log to port 514. A few old Linux distro versions use GNU syslogd (mostly CentOS and Gentoo).

☒ **B I use Cloud Foundry**  
Register each app separately. Use Heroku? [Here's how.](#)

☐ **C My system's hostname changes**  
In rare cases, one system may change hostnames frequently. For example, a roaming laptop which sets its hostname based on DHCP (and roams across networks).

We'll provide an app-specific syslog drain and step-by-step setup for [Cloud Foundry](#)®.

Let's create a destination for this app.

---

**What should we call it?**

  
Alphanumeric. Does not need to match app name.

**Save** →

4. Record the URL with port that is displayed after creating the system.

CloudFoundry will log to **logs.papertrailapp.com:36129**.

5. Create the log drain service in Cloud Foundry.

```
$ cf cups my-logs -l syslog-tls://logs.papertrailapp.com:PORT
```

6. Bind the service to an app.

```
$ cf bind-service APPLICATION-NAME my-logs
```

7. Restage the app.

```
$ cf restage APPLICATION-NAME
```

After a short delay, logs begin to flow automatically.

8. Once Papertrail starts receiving log entries, the view automatically updates to the logs viewing page.

```

All Systems ▾ Dashboard Events Account Help ▾ Me ▾
Skipping auto-reconfiguration.
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: Mar 05, 2014 18:57:36 PM
org.cloudfoundry.reconfiguration.AbstractServiceConfigurer configure
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: INFO: No beans of type org.springframework.data.mongodb.MongoDbFactory found
in application context. Skipping auto-reconfiguration.
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: Mar 05, 2014 18:57:36 PM
org.cloudfoundry.reconfiguration.AbstractServiceConfigurer configure
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: INFO: No beans of type
org.springframework.data.redis.connection.RedisConnectionFactory found in application context. Skipping auto-reconfiguration.
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: Mar 05, 2014 18:57:36 PM
org.cloudfoundry.reconfiguration.AbstractServiceConfigurer configure
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: INFO: Class org.springframework.amqp.rabbit.connection.ConnectionFactory not
in classpath. Skipping auto-reconfiguration for it
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,688 INFO RequestMappingHandlerMapping:181 - Mapped "
([/albums/{id}], methods=[DELETE], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public void
org.cloudfoundry.samples.music.web.controllers.AlbumController.deleteById(java.lang.String)
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,681 INFO RequestMappingHandlerMapping:181 - Mapped "
([/albums/{id}], methods=[GET], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public org.cloudfoundry.samples.music.domain.Album
org.cloudfoundry.samples.music.web.controllers.AlbumController.getById(java.lang.String)
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,681 INFO RequestMappingHandlerMapping:181 - Mapped "
([/albums], methods=[GET], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public
java.lang.Iterable org.cloudfoundry.samples.music.domain.Album org.cloudfoundry.samples.music.web.controllers.AlbumController.albums()
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,682 INFO RequestMappingHandlerMapping:181 - Mapped "
([/albums], methods=[PUT], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public org.cloudfoundry.samples.music.domain.Album
org.cloudfoundry.samples.music.web.controllers.AlbumController.add(org.cloudfoundry.samples.music.domain.Album)
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,682 INFO RequestMappingHandlerMapping:181 - Mapped "
([/albums], methods=[POST], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public org.cloudfoundry.samples.music.domain.Album
org.cloudfoundry.samples.music.web.controllers.AlbumController.update(org.cloudfoundry.samples.music.domain.Album)
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,684 INFO RequestMappingHandlerMapping:181 - Mapped "
([/info], methods=[], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public org.cloudfoundry.samples.music.domain.ApplicationInfo
org.cloudfoundry.samples.music.web.controllers.InfoController.info()
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,684 INFO RequestMappingHandlerMapping:181 - Mapped "
([/service], methods=[], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public
java.util.List org.springframework.cloud.service.ServiceInfo org.cloudfoundry.samples.music.web.controllers.InfoController.showServiceInfo()
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,684 INFO RequestMappingHandlerMapping:181 - Mapped "([/env], methods=
[], params=[], headers=[], consumes=[], produces=[], custom=[])" onto public java.util.Map java.lang.String, java.lang.String
org.cloudfoundry.samples.music.web.controllers.InfoController.showEnvFromEnv()
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,704 INFO SimpleHandlerMapping:382 - Root mapping to handler of
type [class org.springframework.web.servlet.mvc.ParameterizableViewMethodController]
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,726 INFO SimpleHandlerMapping:315 - Mapped URL path [/assets/**]
onto handler of type [class org.springframework.web.servlet.resource.ResourceHttpRequestHandler]
Mar 05 14:57:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:36,731 INFO SimpleHandlerMapping:315 - Mapped URL path [/**] onto
handler of type [class org.springframework.web.servlet.resource.DefaultServletHttpRequestHandler]
Mar 05 14:57:37 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: 22:57:37,048 INFO DispatcherServlet:400 - FrameworkServlet 'appServlet':
Initialization completed in 589 ms
Mar 05 14:57:37 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: Mar 05, 2014 18:57:37 PM org.apache.coyote.AbstractProtocol start
Mar 05 14:57:37 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: INFO: Starting ProtocolHandler ["http-bio-62939"]
Mar 05 14:57:37 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: Mar 05, 2014 18:57:37 PM org.apache.catalina.startup.Catalina start
Mar 05 14:57:37 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/App/1: INFO: Server startup in 11278 ms
Mar 05 14:59:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/AP1: Tried to stop app that never received a start event
Mar 05 14:59:36 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/AP1: Indexed app with guid 4a4dc908-c093-40bb-8718-186f147f3e73 ("instances=0-1")
Mar 05 14:59:37 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/DIA: Stopping app instance (index 1) with guid 4a4dc908-c093-40bb-8718-186f147f3e73
Mar 05 14:59:37 CloudFoundry 4a4dc908-c093-40bb-8718-186f147f3e73/DIA: Stopped app instance (index 1) with guid 4a4dc908-c093-40bb-8718-186f147f3e73
Example: "access denied" (1.2.3.4 OR redis) - sshd Search Contrast
https://papertrailapp.com/groups/151803/events/tiermed-on-id-378903602458826118a-prog-umb3A4a4dc908-c093-40bb-8718-186f147f3e7327%18App%27%18D

```

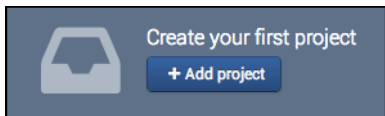
## Splunk

See [Streaming Application Logs to Splunk](#) for details.

## Splunk Storm

From your Splunk Storm account:

1. Click **Add project**.



2. Enter the project details.

Add project

Project name

Project time zone

(UTC-0600) America/Chicago

The Storm interface will use this time zone. If data you send to this project does not have a time zone already, it will be assigned this time zone by default.
[Learn More](#)

Cancel
Continue

3. Create a new **input** for **Network data**.

Network data
[Learn more](#)

- Sends directly from your servers
- Accepts syslog, syslog-ng, rsyslog, snare, netcat, etc.
- Works with Heroku drain

Select

- Manually enter the external IP addresses your Cloud Foundry administrator assigns to outbound traffic.

### Add network data

Storm can receive data from any network port. For example, Storm can accept remote data from [syslog](#), [rsyslog](#), [syslog-ng](#), [snare](#), [netcat](#) or any other application that transmits via TCP or UDP. [Learn more](#)

Authorize your IP address ▾

Automatically

Manually

- Note the host and port provided for TCP input.

### Authorized network inputs

Storm can receive data from any network port. For example, Storm can accept remote data from [syslog](#), [rsyslog](#), [syslog-ng](#), [snare](#), [netcat](#) or any other application that transmits via TCP or UDP.

1. Authorize your IP address  
[Authorize automatically](#)  
Authorize all IP addresses sending data to this project within the next 15 min.  
[Authorize manually](#)  
Specify the IP address

2. Send data to these ports for this project only  

TCP

tcp.k22g-wt6r.data.splunkstorm.com:15486

UDP

udp.k22g-wt6r.data.splunkstorm.com:15486

- Create the log drain service in Cloud Foundry using the displayed TCP host and port.

```
$ cf cups my-logs -l syslog://HOST:PORT
```

- Bind the service to an app

```
$ cf bind-service APPLICATION-NAME my-logs
```

- Restage the app

```
$ cf restage APPLICATION-NAME
```

After a short delay, logs begin to flow automatically.

- Wait for some events to appear, then click **Data Summary**.

### What to Search

266 Events  
INDEXED

a minute ago  
EARLIEST EVENT

a few seconds ago  
LATEST EVENT

Data Summary

- Click the **loggregator** link to view all incoming log entries from Cloud Foundry.

### Data Summary

Hosts (1)


Sources (1)

Sourcetypes (1)

Filter

| Host ▾      | all   | Count ▾ | Last Update ▾         |
|-------------|-------|---------|-----------------------|
| loggregator | all ▾ | 26      | 3/7/14 3:26:01.000 PM |

## SumoLogic

 **Note:** SumoLogic uses HTTPS for communication. HTTPS is supported in Cloud Foundry v158 and later.

From your SumoLogic account:

- Click the **Add Collector** link.

## Manage Collectors and Sources

[Upgrade Collectors](#) [Add Collector](#) [Access Keys](#)

2. Choose **Hosted Collector** and fill in the details.

**Add Collector**

Select a type of collector:

**Installed Collector**

Select to install a Collector in your deployment.

**Hosted Collector**

Select to set up a Collector in the Sumo Logic Cloud.

**FAQs**

- ▶ What's the difference between an Installed and Hosted Collector?
- ▶ Where should I install an Installed Collector?
- ▶ How do I know if I need more than one Installed Collector?
- ▶ Where does my data go?

**Add Collector**

**Name \***

**Description**

**Category**

Unless overwritten by Source metadata, the Collector will set the Source category of all messages to this value.

[Save](#) | [Cancel](#)

3. In the new collector's row of the collectors view, click the **Add Source** link.

**Manage Collectors and Sources** [Upgrade Collectors](#) [Add Collector](#) [Access Keys](#)

Show: [All Collectors](#) | [Running Collectors](#) | [Stopped Collectors](#) Expand: [All](#) | [None](#) [G](#) [<](#) [>](#) Page: 1 of 1

| Name            | Type   | Status | Source Category | Sources | Last Hour | Messages                                                                   |
|-----------------|--------|--------|-----------------|---------|-----------|----------------------------------------------------------------------------|
| ▼ Cloud Foundry | Hosted |        |                 | 1       | None      | <a href="#">Add Source</a>   <a href="#">Edit</a>   <a href="#">Delete</a> |

4. Select **HTTP** source and fill in the details. Note that you'll be provided an HTTPS url

**Select a type of Source:**

**Amazon S3**

Collects logs from an Amazon S3 bucket.

**HTTP**

HTTP receiver that collects logs sent to a specific address.

**Name \***   
Maximum name length is 128 characters

**Description**

**Source Host**   
Host name for the system from which the log files are being collected, e.g. LDAP\_Server

**Source Category**   
Log category metadata to use later for querying, e.g. OS\_Security

▶ **Advanced**

▶ **Filters**

[Save](#) | [Cancel](#)

5. Once the source is created, a URL should be displayed. You can also view the URL by clicking the **Show URL** link beside the created source.

**Manage Collectors and Sources** [Upgrade Collectors](#) [Add Collector](#) [Access Keys](#)

Show: [All Collectors](#) | [Running Collectors](#) | [Stopped Collectors](#) Expand: [All](#) | [None](#) [G](#) [<](#) [>](#) Page: 1 of 1

| Name                 | Type   | Status | Source Category | Sources | Last Hour | Messages                                                                   |
|----------------------|--------|--------|-----------------|---------|-----------|----------------------------------------------------------------------------|
| ▼ Cloud Foundry      | Hosted |        |                 | 1       | None      | <a href="#">Add Source</a>   <a href="#">Edit</a>   <a href="#">Delete</a> |
| CloudFoundry<br>HTTP |        |        |                 |         |           | <a href="#">Show URL</a>   <a href="#">Edit</a>   <a href="#">Delete</a>   |

6. Create the log drain service in Cloud Foundry using the displayed URL.

```
$ cf cups my-logs -l HTTPS-SOURCE-URL
```

7. Bind the service to an app.

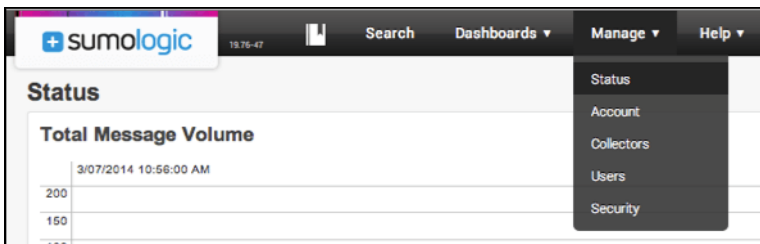
```
$ cf bind-service APPLICATION-NAME my-logs
```

8. Restage the app.

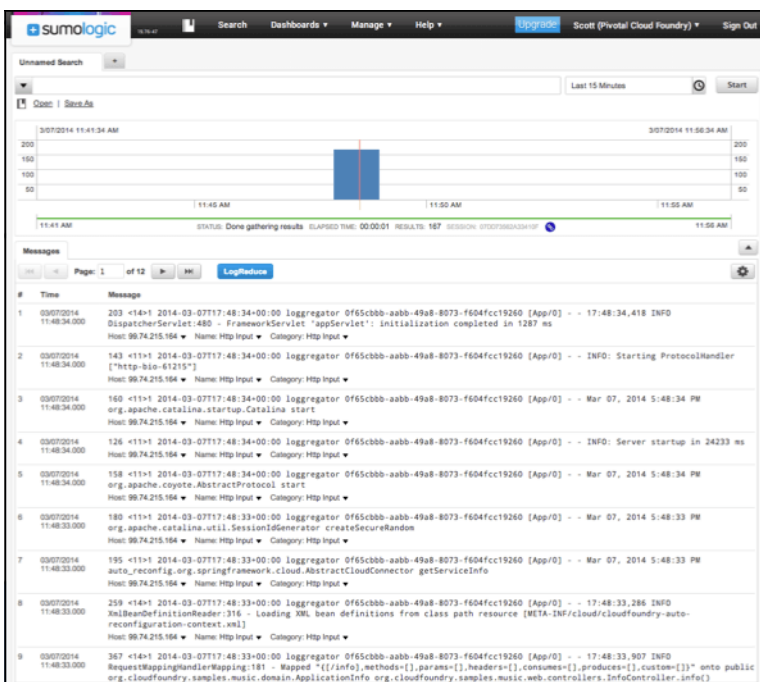
```
$ cf restage APPLICATION-NAME
```

After a short delay, logs begin to flow automatically.

9. In the SumoLogic dashboard, click **Manage**, then click **Status** to see a view of log messages received over time.



10. In the SumoLogic dashboard, click **Search**. Place the cursor in the search box, then press **Enter** to submit an empty search query.



## Logsense

**Note:** Logsense uses HTTPS for communication. HTTPS is supported in Cloud Foundry v158 and later.

From your Sematext account:

1. Click the [Create App / Logsense App](#) menu item. Enter a name and click **Add Application** to create the Logsense App.
2. Create the log drain service in Cloud Foundry using the displayed URL.

```
$ cf cups logsene-log-drain -l https://logsene-cf-receiver.sematext.com/YOUR_LOGSENE_TOKEN
```

3. Bind the log drain to an app. You could optionally bind multiple apps to one log drain.

```
$ cf bind-service YOUR-CF-APP-NAME logsene-log-drain
```

4. Restage the app.

```
$ cf restage APPLICATION-NAME
```

After a short delay, logs begin to flow automatically and appear in the [Logsene UI](#).

## Logentries is Not Supported

Cloud Foundry distributes log messages over multiple servers to handle load. Currently, we do not recommend using Logentries as it does not support multiple syslog sources.

## Streaming Application Logs to Splunk

Page last updated:

To integrate Cloud Foundry with Splunk Enterprise, complete the following process.

### 1. Create a Cloud Foundry Syslog Drain for Splunk

In Cloud Foundry, create a syslog drain user-provided service instance as described in [Using Third-Party Log Management Services](#).

Choose one or more applications whose logs you want to drain to Splunk through the service.

Bind each app to the service instance and restart the app.

Note the GUID for each app, the IP address of the Loggregator host, and the port number for the service. Locate the port number in the syslog URL. For example:

```
syslog://logs.example.com:1234
```

### 2. Prepare Splunk for Cloud Foundry

For detailed information about the following tasks, see the [Splunk documentation](#).

#### Install the RFC5424 Syslog Technology Add-On

The Cloud Foundry Loggregator component formats logs according to the Syslog Protocol defined in [RFC 5424](#). Splunk does not parse log fields according to this protocol. To allow Splunk to correctly parse RFC 5424 log fields, install the Splunk [RFC5424 Syslog Technical Add-On](#).

#### Patch the RFC5424 Syslog Technology Add-On

1. SSH into the Splunk VM
2. Replace `/opt/splunk/etc/apps/rfc5424/default/transforms.conf` with a new `transforms.conf` file that consists of the following text:

```
[rfc5424_host]
DEST_KEY = MetaData:Host
REGEX = <(d+)>d{1}s{1}\S+s{1}(\S+)
FORMAT = host::$1

[rfc5424_header]
REGEX = <(d+)>d{1}s{1}\S+s{1}\S+s{1}(\S+)s{1}(\S+)s{1}(\S+)
FORMAT = prival::$1 appname::$2 procid::$3 msgid::$4
MV_ADD = true
```

3. Restart Splunk

### Create a TCP Syslog Data Input

Create a TCP Syslog Data Input in Splunk, with the following settings:

- **TCP port** is the port number you assigned to your log drain service
- **Set sourcetype** is `Manual`
- **Source type** is `rfc5424_syslog` (type this value into text field)
- **Index** is the index you created for your log drain service

Your Cloud Foundry syslog drain service is now integrated with Splunk.

## 3. Verify that Integration was Successful

Use Splunk to execute a query of the form:

```
sourcetype=rfc5424_syslog index=~THE-INDEX-YOU-CREATED appname=APP-GUID
```

To view logs from all apps at once, you can omit the `appname` field.

Verify that results rows contain the three Cloud Foundry-specific fields:

- **appname**: The GUID for the Cloud Foundry application
- **host**: The IP address of the Loggregator host
- **procid**: The Cloud Foundry component emitting the log

If the Cloud Foundry-specific fields appear in the log search results, integration is successful.

If logs from an app are missing, make sure that the following are true:

- The app is bound to the service and was restarted after binding
- The service port number matches the TCP port number in Splunk



## Streaming Application Logs with Fluentd

Page last updated:

[Fluentd](#) is an open source log collector that allows you to implement unified logging layers. With Fluentd, you can stream application logs to different backends or services like Elasticsearch, HDFS and Amazon S3. This topic explains how to integrate Fluentd with Cloud Foundry applications.

### Step 1: Create a Cloud Foundry Syslog Drain for Fluentd

1. In Cloud Foundry, create a syslog drain user-provided service instance as described in [Using Third-Party Log Management Services](#).
2. Choose one or more applications whose logs you want to drain to Fluentd through the service.
3. Bind each app to the service instance, and restart the app.
4. Note the GUID for each app, the IP address of the Loggregator host, and the port number for the service.
5. Locate the port number in the syslog URL. For example:

```
syslog://logs.example.com:5140
```

### Step 2: Set up Fluentd for Cloud Foundry


This section assumes you have an active Fluentd instance running. If you do not have an active Fluentd instance, refer to the [Fluentd Documentation/Install](#) steps for more details.

Fluentd comes with native support for syslog protocol. To set up Fluentd for Cloud Foundry, configure the syslog input of Fluentd as follows.

1. In your main Fluentd configuration file, add the following `source` entry:

```
<source>
 @type syslog
 port 5140
 bind 0.0.0.0
 tag cf.app
 protocol_type udp
</source>
```

2. Restart the Fluentd service.

 **Note:** The Fluentd syslog input plugin supports `udp` and `tcp` options. Make sure to use the same transport that Cloud Foundry is using.

Fluentd will start listening for Syslog message on port 5140 and tagging the messages with `cf.app`, which can be used later for data routing. For more details about the full setup for the service, refer to the [Config File](#) article.

If your goal is to use an Elasticsearch or Amazon S3 backend, read the following guide: <http://www.fluentd.org/guides/recipes/elasticsearch-and-s3>

## Streaming Application Logs to Azure OMS Log Analytics (Beta)

Page last updated:

**⚠ warning:** The OMS Log Analytics Firehose Nozzle is currently intended for evaluation and test purposes only. Do not use this product in a production environment.

This topic explains how to integrate your Cloud Foundry (CF) apps with [OMS Log Analytics](#).

Operations Management Suite (OMS) Log Analytics is a monitoring service for Microsoft Azure. The OMS Log Analytics Firehose Nozzle is a CF component that forwards metrics from the Loggregator Firehose to OMS Log Analytics.

This topic assumes you are using the latest version of the Cloud Foundry Command Line Interface (cf CLI) and a working Pivotal Application Service deployment on Azure.

### Step 1: Create an OMS Workspace in Azure

See [Get started with Log Analytics](#) in the Microsoft Azure documentation to create an OMS workspace.

### Step 2: Deploy the Nozzle to Cloud Foundry

1. Run `cf login -a https://api.YOUR-DOMAIN -u YOUR-USERNAME --skip-ssl-validation`, replacing `YOUR-DOMAIN` with your domain and `YOUR-USERNAME` with your CF username, to authenticate to your CF instance. For example:

```
$ cf login -a https://api.example.com -u admin --skip-ssl-validation
```

2. Follow the steps below to create a new Cloud Foundry user and grant it access to the Loggregator Firehose using the UAA CLI (UAAC). For more information, see [Creating and Managing Users with the UAA CLI \(UAAC\)](#) and [Orgs, Spaces, Roles, and Permissions](#).

- a. Use `uaac target uaa.YOUR-DOMAIN` to target your UAA server:

```
$ uaac target uaa.example.com --skip-ssl-validation
```

- b. Run the following command to obtain an access token for the admin client:

```
$ uaac token client get admin
```

- c. Run `cf create-user USERNAME PASSWORD`, replacing `USERNAME` with a new username and `PASSWORD` with a password, to create a new user. For example:

```
$ cf create-user firehose-user firehose-password
```

- d. Run `uaac member add cloud_controller.admin USERNAME`, replacing `USERNAME` with the new username, to grant the new user admin permissions. For example:

```
$ uaac member add cloud_controller.admin firehose-user
```

- e. Run `uaac member add doppler.firehose USERNAME`, replacing `USERNAME` with the new username, to grant the new user permission to read logs from the Loggregator Firehose endpoint. For example:

```
$ uaac member add doppler.firehose firehose-user
```

3. Download the [OMS Log Analytics Firehose Nozzle BOSH release](#) from Github. Clone the repository and navigate to the `oms-log-analytics-firehose-nozzle` directory:

```
$ git clone https://github.com/Azure/oms-log-analytics-firehose-nozzle.git
$ cd oms-log-analytics-firehose-nozzle
```

4. Set the following environment variables in the [OMS Log Analytics Firehose Nozzle manifest](#):


| Environment Variable                                                                                            | Description                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>applications: - name: oms_nozzle ... env:   OMS_WORKSPACE: YOUR-WORKSPACE-ID   OMS_KEY: YOUR-OMS-KEY</pre> | Enter the ID and key value for your OMS workspace.                                                                                                                                                                                                                      |
| OMS_POST_TIMEOUT: 10s                                                                                           | (Optional) Set the HTTP post timeout for sending events to OMS Log Analytics. The default value is 10 seconds.                                                                                                                                                          |
| OMS_BATCH_TIME: 10s                                                                                             | (Optional) Set the interval for posting a batch to OMS. The default value is 10 seconds.<br><br>For more information, see the <a href="#">Configure Additional Logging</a> section below.                                                                               |
| OMS_MAX_MSG_NUM_PER_BATCH: 1000                                                                                 | (Optional) Set the maximum number of messages to include in an OMS batch. The default amount is 1000.<br><br>For more information, see the <a href="#">Configure Additional Logging</a> section below.                                                                  |
| <pre>FIREHOSE_USER: YOUR-FIREHOSE-USER FIREHOSE_USER_PASSWORD: YOUR-FIREHOSE-PASSWORD</pre>                     | Enter the username and password for the Firehose user you created in Step 2c.                                                                                                                                                                                           |
| API_ADDR: https://api.YOUR-DOMAIN                                                                               | Enter the URL of your API endpoint.                                                                                                                                                                                                                                     |
| DOPPLER_ADDR: wss://doppler.YOUR-DOMAIN:443                                                                     | Enter the URL of your Loggregator traffic controller endpoint.                                                                                                                                                                                                          |
| EVENT_FILTER: YOUR-LIST                                                                                         | (Optional) Enter the event types you want to filter out in a comma-separated list. The valid event types are <code>METRIC</code> , <code>LOG</code> , and <code>HTTP</code> .                                                                                           |
| IDLE_TIMEOUT: 60s                                                                                               | (Optional) Set the duration for the Firehose keepalive connection. The default time is 60 seconds.                                                                                                                                                                      |
| SKIP_SSL_VALIDATION: TRUE-OR-FALSE                                                                              | Set this value to <code>TRUE</code> to allow insecure connections to the UAA and the traffic controller. To block insecure connections to the UAA and traffic controller, set this value to <code>FALSE</code> .                                                        |
| LOG_LEVEL: INFO                                                                                                 | (Optional) Change this value to increase or decrease the amount of logs. Valid log levels in increasing order include <code>INFO</code> , <code>ERROR</code> , and <code>DEBUG</code> . The default value is <code>INFO</code> .                                        |
| LOG_EVENT_COUNT: TRUE-OR-FALSE                                                                                  | Set this value to <code>TRUE</code> to log the total count of events that the nozzle has sent, received, and lost. OMS logs this value as <code>CounterEvents</code> .<br><br>For more information, see the <a href="#">Configure Additional Logging</a> section below. |
| LOG_EVENT_COUNT_INTERVAL: 60s                                                                                   | (Optional) Set the time interval for logging the event count to OMS. The default interval is 60 seconds.<br><br>For more information, see the <a href="#">Configure Additional Logging</a> section below.                                                               |

5. Push the app:

```
$ cf push
```

## Step 3: View Logs in OMS Portal

Import the Cloud Foundry OMS view to your OMS Portal to view visualized logs and metrics. You can also create alert rules for specific events.


 **Note:** The OMS view of Cloud Foundry is not yet available in the OMS Solutions Gallery. You can add it manually to view your logs in OMS Portal.

## Import the OMS View

1. From the main OMS Overview page, navigate to **View Designer**.
2. Click **Import**.
3. Click **Browse**.
4. Select the **Cloud Foundry (Preview).omsview** file.
5. Save the view. The main OMS Overview page displays the **Tile**.
6. Click the **Tile** to view visualized metrics.

See the [OMS Log Analytics View Designer documentation](#)  for more information.

## Create Alert Rules

See [Overview of alerts in Microsoft Azure](#)  for more information about OMS Log Analytics alerts.

## Set Alert Queries

This section includes example queries that operators can set in the OMS Portal.

- The following query alerts the operator when the nozzle sends a `slowConsumerAlert` to OMS:

```
Type=CF_ValueMetric_CL Name_s=slowConsumerAlert
```

- The following query alerts the operator when Loggregator sends an `LGR` to indicate problems with the logging process:

```
Type=CF_LogMessage_CL SourceType_s=LGR MessageType_s=ERR
```

- The following query alerts the operator when the number of lost events reaches a certain threshold, specified in the OMS Portal:

```
Type=CF_CounterEvent_CL Job_s=nozzle Name_s=eventsLost
```

- The following query alerts the operator when the nozzle receives the `TruncatingBuffer.DroppedMessages` **CounterEvent**:


```
Type=CF_CounterEvent_CL Name_s="TruncatingBuffer.DroppedMessages"
```

## (Optional) Step 4: Configure Additional Logging

OMS Log Analytics Firehose Nozzle forwards metrics from the Loggregator Firehose to OMS with minimal processing, but the nozzle can push additional metrics to OMS.

## Log Sent, Received, and Lost Events

If you set the `LOG_EVENT_COUNT` environment variable to `TRUE` in the [manifest](#), the nozzle periodically sends the count of sent, received, and lost events to OMS. The value you set for the `LOG_EVENT_COUNT_INTERVAL` determines how frequently the nozzle sends the count.

 **Note:** The nozzle does not count **CounterEvents** themselves in the sent, received, or lost event count.

The nozzle sends the count as a **CounterEvent** with a **CounterKey** of one of the following:

|  |  |
|--|--|
|  |  |
|--|--|

| CounterEvent                | CounterKey                                                                                                        |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------|
| nozzle.stats.eventsReceived | The number of events the Firehose has received during the interval                                                |
| nozzle.stats.eventsSent     | The number of events the nozzle has successfully sent to OMS during the interval                                  |
| nozzle.stats.eventsLost     | The number of events the nozzle has tried to send to OMS during the interval, but failed to send after 4 attempts |

In most cases, the total count of `eventsSent` plus `eventsLost` is less than the total `eventsReceived` at the same time. The nozzle buffers some messages and posts them in a batch to OMS. Operators can adjust the buffer size by adjusting the `OMS_BATCH_TIME` and `OMS_MAX_MSG_NUM_PER_BATCH` environment variables in the [manifest](#).

## Log Slow Consumer Alerts

 **Note:** The nozzle does not count **ValueMetrics** in the sent, received, or lost event count.

Loggregator sends the nozzle a `slowConsumerAlert` in the following situations:

- WebSocket sends the error code `ClosePolicyViolation (1008)`
- The nozzle receives a **CounterEvent** with the value `TruncatingBuffer.DroppedMessages`

In either case, the nozzle sends the `slowConsumerAlert` event to OMS as the following **ValueMetric**:

| ValueMetric                    | MetricKey |
|--------------------------------|-----------|
| nozzle.alert.slowConsumerAlert | 1         |

See the *Slow Nozzle Alerts* section of the [Loggregator Guide for Cloud Foundry Operators](#) for more information.

## (Optional) Step 5: Scale the Deployment

### Scale the Nozzle

If the nozzle is unable to keep up with processing logs from the Firehose, Loggregator alerts the nozzle. When the nozzle receives the alert, it sends a `slowConsumerAlert` to OMS. If this happens, scaling up the nozzle minimizes data loss.

If an operator chooses to scale up their deployment, the Firehose evenly distributes events across all instances of the nozzle. See the *Scaling Nozzles* section of the [Loggregator Guide for Cloud Foundry Operators](#) for more information.

Operators can [create an alert rule](#) for the `slowConsumerAlert` message.

### Scale Loggregator

Loggregator sends `LGR` log messages to indicate problems with the logging process. See the *Scaling Loggregator* section of the [Loggregator Guide for Cloud Foundry Operators](#) for more information.

Operators can [create an alert rule](#) for the `LGR` message.

Managing apps index

---

title: Managing Apps with the cf CLI

## owner:

The following list provides information about managing apps with the Cloud Foundry Command Line Interface (cf CLI):

- [Running Tasks](#)
- [Scaling an App Using cf scale](#)
- [Using Application Health Checks](#)

## Running Tasks

Page last updated:

This topic describes how to run tasks in Cloud Foundry. A task is an application or script whose code is included as part of a deployed application, but runs independently in its own container.

### About Tasks

In contrast to a long running process (LRP), tasks run for a finite amount of time, then stop. Tasks run in their own containers and are designed to use minimal resources. After a task runs, Cloud Foundry destroys the container running the task.

As a single-use object, a task can be checked for its state and for a success or failure message.



**Note:** Running a task consumes an application instance, and will be billed accordingly.

### Use Cases for Tasks

Tasks are used to perform one-off jobs, which include the following:

- Migrating a database
- Sending an email
- Running a batch job
- Running a data processing script
- Processing images
- Optimizing a search index
- Uploading data
- Backing-up data
- Downloading content

### How Tasks Are Run

Tasks are always executed asynchronously, meaning that they run independently from the parent application or other tasks that run on the same application.

The life-cycle of a task is as follows:

1. A user initiates a task in Cloud Foundry using one of the following mechanisms:
  - `cf run-task APPNAME "TASK"` command. See the [Running Tasks](#) section of this topic for more information.
  - Cloud Controller v3 API call. See the [Tasks](#) [API](#) reference page for more information.
  - Cloud Foundry Java Client. See the [Cloud Foundry Java Client Library](#) and [Cloud Foundry Java Client](#) [API](#) topics for more information.
2. Cloud Foundry creates a container specifically for the task.
3. Cloud Foundry runs the task on the container using the value passed to the `cf run-task` command.
4. Cloud Foundry destroys the container.

The container also inherits environment variables, service bindings, and security groups bound to the application.



**Note:** You cannot SSH into the container running a task.

### Task Logging and Execution History

Any data or messages the task outputs to STDOUT or STDERR is available on the app's firehose logs. A syslog drain attached to the app receives the task log output.

The task execution history is retained for one month.

## Manage Tasks


At the system level, a user with admin-level privileges can use the Cloud Controller v3 API to view all tasks that are running within an org or space. For more information, see the documentation for the [Cloud Controller v3 API](#).

In addition, admins can set the default memory and disk usage quotas for tasks on a global level. Initially, tasks use the same memory and disk usage defaults as applications. However, the default memory and disk allocations for tasks can be defined separately from the default app memory and disk allocations.

The default memory and disk allocations are defined using the **Default App Memory** and **Default Disk Quota per App** fields. These fields are available in the **Application Developer Controls** configuration screen of Pivotal Application Service (PAS).

## Run a Task on an Application

You can use the Cloud Foundry Command Line Interface (cf CLI) to run a task in the context of an application.

 **Note:** To run tasks with the cf CLI, you must install cf CLI v6.23.0 or later. See the [Installing the Cloud Foundry Command Line Interface](#) topic for information about downloading, installing, and uninstalling the cf CLI.

To run a task on an application, perform the following steps:

1. Push your application:


```
$ cf push APP-NAME
```

2. Run your task on the deployed application:

```
$ cf run-task APP-NAME "TASK" --name TASK-NAME
```

The following example runs a database migration as a task on the `my-app` application:

```
$ cf run-task my-app "bin/rails db:migrate" --name my-task
Creating task for app my-app in org jdoe-org / space development as jdoe@pivotal.io...
OK
Task 1 has been submitted successfully for execution.
```

 **Note:** To re-run a task, you must run it as a new task using the above command.

Use the `cf logs APP-NAME --recent` command to display the recent logs of the application and all its tasks.

The following example displays the logs of a successful task:

```
$ cf logs my-app --recent
2017-01-03T15:58:06.57-0800 [APP/TASK/my-task/0]OUT Creating container
2017-01-03T15:58:08.45-0800 [APP/TASK/my-task/0]OUT Successfully created container
2017-01-03T15:58:13.32-0800 [APP/TASK/my-task/0]OUT D, [2017-01-03T23:58:13.322258 #7] DEBUG -- : (15.9ms) CREATE TABLE "schema_migrations" ("version" character varying
2017-01-03T15:58:13.33-0800 [APP/TASK/my-task/0]OUT D, [2017-01-03T23:58:13.337723 #7] DEBUG -- : (11.9ms) CREATE TABLE "ar_internal_metadata" ("key" character varying P
2017-01-03T15:58:13.34-0800 [APP/TASK/my-task/0]OUT D, [2017-01-03T23:58:13.340234 #7] DEBUG -- : (1.6ms) SELECT pg_try_advisory_lock(3720865444824511725);
2017-01-03T15:58:13.35-0800 [APP/TASK/my-task/0]OUT D, [2017-01-03T23:58:13.351853 #7] DEBUG -- : ActiveRecord::SchemaMigration Load (0.7ms) SELECT "schema_migrations".
2017-01-03T15:58:13.35-0800 [APP/TASK/my-task/0]OUT I, [2017-01-03T23:58:13.357294 #7] INFO -- : Migrating to CreateArticles (20161118225627)
2017-01-03T15:58:13.35-0800 [APP/TASK/my-task/0]OUT D, [2017-01-03T23:58:13.359565 #7] DEBUG -- : (0.5ms) BEGIN
2017-01-03T15:58:13.35-0800 [APP/TASK/my-task/0]OUT = 20161118225627 CreateArticles: migrating =====
2017-01-03T15:58:13.50-0800 [APP/TASK/my-task/0]OUT Exit status 0
2017-01-03T15:58:13.56-0800 [APP/TASK/my-task/0]OUT Destroying container
2017-01-03T15:58:15.65-0800 [APP/TASK/my-task/0]OUT Successfully destroyed container
```

The following example displays the logs of a failed task:



```
$ cf logs my-app --recent
2016-12-14T11:09:26.09-0800 [APP/TASK/my-task/0]OUT Creating container
2016-12-14T11:09:28.43-0800 [APP/TASK/my-task/0]OUT Successfully created container
2016-12-14T11:09:28.85-0800 [APP/TASK/my-task/0]ERR bash: bin/rails: command not found
2016-12-14T11:09:28.85-0800 [APP/TASK/my-task/0]OUT Exit status 127
2016-12-14T11:09:28.89-0800 [APP/TASK/my-task/0]OUT Destroying container
2016-12-14T11:09:30.50-0800 [APP/TASK/my-task/0]OUT Successfully destroyed container
```

If your task name is unique, you can `grep` the output of the `cf logs` command for the task name to view task-specific logs.

## List Tasks Running on an Application

To list the tasks for a given application, run the `cf tasks APP-NAME`. For example:

```
$ cf tasks my-app
Getting tasks for app my-app in org jdoe-org / space development as jdoe@pivotal.io...
OK

id name state start time command
2 339044ef FAILED Wed, 23 Nov 2016 21:52:52 UTC echo foo; sleep 100; echo bar
1 8d0618cf SUCCEEDED Wed, 23 Nov 2016 21:37:28 UTC bin/rails db:migrate
```

Each task has one of the following states:

| State     | Description                                                                                                  |
|-----------|--------------------------------------------------------------------------------------------------------------|
| RUNNING   | The task is currently in progress.                                                                           |
| FAILED    | The task did not complete. This state occurs when a task does not work correctly or a user cancels the task. |
| SUCCEEDED | The task completed successfully.                                                                             |

## Cancel a Task

After running a task, you may be able to cancel it before it finishes. To cancel a running task, use the `cf terminate-task APP-NAME TASK-ID` command. For example:


```
$ cf terminate-task my-app 2
Terminating task 2 of app my-app in org jdoe-org / space development as jdoe@pivotal.io...
OK
```

## Scaling an Application Using cf scale

Page last updated:

Factors such as user load, or the number and nature of tasks performed by an application, can change the disk space and memory the application uses. For many applications, increasing the available disk space or memory can improve overall performance. Similarly, running additional instances of an application can allow the application to handle increases in user load and concurrent requests. These adjustments are called **scaling** an application.

Use [cf scale](#) to scale your application up or down to meet changes in traffic or demand.

 **Note:** You can configure your app to scale automatically based on rules that you set. See the [Scaling an Application Using Autoscaler](#) and [Using the App Autoscaler CLI](#) topics for more information.

## Scaling Horizontally

Horizontally scaling an application creates or destroys instances of your application.

Incoming requests to your application are automatically load balanced across all instances of your application, and each instance handles tasks in parallel with every other instance. Adding more instances allows your application to handle increased traffic and demand.

Use `cf scale APP -i INSTANCES` to horizontally scale your application. Cloud Foundry will increase or decrease the number of instances of your application to match `INSTANCES`.

```
$ cf scale myApp -i 5
```

## Scaling Vertically

Vertically scaling an application changes the disk space limit or memory limit that Cloud Foundry applies to all instances of the application.

Use `cf scale APP -k DISK` to change the disk space limit applied to all instances of your application. `DISK` must be an integer followed by either an **M**, for megabytes, or **G**, for gigabytes.

```
$ cf scale myApp -k 512M
```

Use `cf scale APP -m MEMORY` to change the memory limit applied to all instances of your application. `MEMORY` must be an integer followed by either an **M**, for megabytes, or **G**, for gigabytes.

```
$ cf scale myApp -m 1G
```

## Using Application Health Checks

Page last updated:

This topic describes how to configure health checks for your applications in Cloud Foundry.

### Overview

An application health check is a monitoring process that continually checks the status of a running Cloud Foundry app.

Developers can configure a health check for an application using the Cloud Foundry Command Line Interface (cf CLI) or by specifying the `health-check-http-endpoint` and `health-check-type` fields in an application manifest.

To configure a health check using the cf CLI, follow the instructions in the [Configure Health Checks](#) section below. For more information about using an application manifest to configure a health check, see the [health-check-http-endpoint](#) and [health-check-type](#) sections of the *Deploying with Application Manifest* topic.

Application health checks function as part of the app lifecycle managed by [Diego architecture](#).


### Configure Health Checks

To configure a health check while creating or updating an application, use the `cf push` [command](#):

```
$ cf push YOUR-APP -u HEALTH-CHECK-TYPE -t HEALTH-CHECK-TIMEOUT
```

Replace the placeholders in the example command above as follows:

- `HEALTH-CHECK-TYPE`: Valid health check types are `port`, `process`, and `http`. See the [Health Check Types](#) section below for more information.
- `HEALTH-CHECK-TIMEOUT`: The timeout is the amount of time allowed to elapse between starting up an application and the first healthy response. See the [Health Check Timeouts](#) section for more information.


 **Note:** The health check configuration you provide with `cf push` overrides any configuration in the application manifest.


To configure a health check for an existing application or to add a custom HTTP endpoint, use the `cf set-health-check` [command](#):

```
$ cf set-health-check YOUR-APP HEALTH-CHECK-TYPE --endpoint CUSTOM-HTTP-ENDPOINT
```

Replace the placeholders in the example command above as follows:

- `HEALTH-CHECK-TYPE`: Valid health check types are `port`, `process`, and `http`. See the [Health Check Types](#) section below for more information.
- `CUSTOM-HTTP-ENDPOINT`: A `http` health check defaults to using `/` as its endpoint, but you can specify a custom endpoint. See the [Health Check HTTP Endpoints](#) section below for more information.

 **Note:** You can change the health check configuration of a deployed app with `cf set-health-check`, but you must restart the app for the changes to take effect.

 **Note:** You can also use the `v3-set-health-check` CLI command to change the individual health check invocation timeout for an app. This option also requires restarting the app. See the [Cloud Foundry CLI Reference Guide](#) [for more information](#).

## Understand Health Checks

### Health Check Lifecycle

The following table describes how application health checks work in Cloud Foundry.

| Stage | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Application developer deploys an app to Cloud Foundry.                                                                                                                                                                                                                                                                                                                                                |
| 2     | When deploying the app, the developer specifies a health check type for the app and, optionally, a timeout. If the developer does not specify a health check type, then the monitoring process defaults to a <code>port</code> health check.                                                                                                                                                          |
| 3     | Cloud Controller stages, starts, and runs the app.                                                                                                                                                                                                                                                                                                                                                    |
| 4     | Based on the type specified for the app, Cloud Controller configures a health check that runs periodically for each app instance.                                                                                                                                                                                                                                                                     |
| 5     | When Diego starts an app instance, the application health check runs every 2 seconds until a response indicates that the app instance is healthy or until the health check timeout elapses. The 2-second health check interval is not configurable.                                                                                                                                                   |
| 6     | When an app instance becomes healthy, its route is advertised, if applicable. Subsequent health checks are run every 30 seconds once the app becomes healthy. The 30-second health check interval is not configurable.                                                                                                                                                                                |
| 7     | If a previously healthy app instance fails a health check, Diego considers that particular instance to be unhealthy. As a result, Diego stops and deletes the app instance, then reschedules a new app instance. This stoppage and deletion of the app instance is reported back to the Cloud Controller as a crash event.                                                                            |
| 8     | When an app instance crashes, Diego immediately attempts to restart the app instance several times. After three failed restarts, Cloud Foundry waits 30 seconds before attempting another restart. The wait time doubles each restart until the ninth restart, and remains at that duration until the 200th restart. After the 200th restart, Cloud Foundry stops trying to restart the app instance. |

## Health Check Types

The following table describes the types of health checks available for applications and recommended circumstances in which to use them:

| Health Check Type    | Recommended Use Case                                                   | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>http</code>    | The app can provide an <code>HTTP 200</code> response.                 | The <code>http</code> health check performs a GET request to the configured HTTP endpoint on the app's default port. When the health check receives an <code>HTTP 200</code> response, the app is declared healthy. We recommend using the <code>http</code> health check type whenever possible. A healthy HTTP response ensures that the web app is ready to serve HTTP requests. The configured endpoint must respond within 1 second to be considered healthy.<br><b>WARNING:</b> To prevent false negatives, use a dedicated endpoint for healthcheck where response time and result do not depend on business logic. |
| <code>port</code>    | The app can receive TCP connections (including HTTP web applications). | A health check makes a TCP connection to the port or ports configured for the app. For applications with multiple ports, a health check monitors each port. If you do not specify a health check type for your app, then the monitoring process defaults to a <code>port</code> health check. The TCP connection must be established within 1 second to be considered healthy.                                                                                                                                                                                                                                             |
| <code>process</code> | The app does not support TCP connections (for example, a worker).      | For a <code>process</code> health check, Diego ensures that any process declared for the app stays running. If the process exits, Diego stops and deletes the app instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                |


## Health Check Timeouts


The value configured for the health check timeout is the amount of time allowed to elapse between starting up an app and the first healthy response from the app. If the health check does not receive a healthy response within the configured timeout, then the app is declared unhealthy.

In Pivotal Cloud Foundry, the default timeout is 60 seconds and the maximum configurable timeout is 600 seconds. You can modify the timeout in the **Application Containers** pane of the Pivotal Application Service (PAS) tile.

## Health Check HTTP Endpoints

Only used by `http` type, the `--endpoint` flag of the `cf set-health-check` command specifies the path portion of a URI that must be served by the app and return `HTTP 200` when the app is healthy.

 **Note:** This command will only check the health of the default port of the app.

 **Note:** For HTTP apps, we recommend setting the health check type to `http` instead of a simple port check.

## Configuring Container-to-Container Networking

This topic describes how to configure the Container-to-Container Networking feature, which allows direct network traffic between apps. For an overview of how Container-to-Container Networking works, see the [Container-to-Container Networking](#) topic.

Container-to-Container Networking enables PCF to generate logs whenever containers communicate or attempt to communicate with each other. See [App Traffic Logging](#) for how to manage app traffic logging.

### Configure the Overlay Network

Container-to-Container Networking uses an overlay network to manage communication between app instances. By default, each Diego cell in the overlay network is allocated a /24 range that supports 254 containers per cell, one container for each of the usable IP addresses, .1 through .254. For more information about the overlay network, see [Overlay Network](#) in *Container-to-Container Networking*.

### Configure the Number of Diego Cells

If you want to modify the number of Diego cells supported by the overlay network, follow the steps below:

1. In Ops Manager, select the PAS tile.
2. Select **Networking**.
3. Under **Overlay Subnet**, enter an IP range for the overlay network. By default, Ops Manager uses `10.255.0.0/16`. Modifying the subnet range allocated to the overlay network changes the number of Diego cells supported in your deployment. Use the table below as a reference.

| Overlay subnet mask | Number of cells | Containers per cell |
|---------------------|-----------------|---------------------|
| /20                 | 15              | 254                 |
| /16                 | 255             | 254                 |
| /12                 | 4,095           | 254                 |

**⚠ warning:** The overlay network IP address range must not conflict with any other IP addresses in the network. If a conflict exists, Diego cells cannot reach any endpoint that has a conflicting IP address.

## Create and Manage Networking Policies

This section describes how to create and modify Container-to-Container Networking policies using the Cloud Foundry Command Line Interface (cf CLI). The cf CLI only supports configuring policies for apps within the same space. To configure policies for apps in different orgs and spaces, use the [Policy Server External API](#).

**💡 Note:** With the NSX-T integration, container networking policies and ASGs continue to work as normal. Advanced ASG logging is not supported with NSX-T.

### Prerequisites

- Ensure that you are using cf CLI v6.30 or higher:

```
$ cf version
```

For more information about updating the cf CLI, see the [Installing the cf CLI](#) topic.

### Grant Permissions

CF admins use the following UAA scopes to grant specific users or groups permissions to configure network policies:

| UAA Scope                  | Suitable for...  | Allows users to create policies...      |
|----------------------------|------------------|-----------------------------------------|
| <code>network.admin</code> | operators        | for any apps in the CF deployment       |
| <code>network.write</code> | space developers | for apps in spaces that they can access |

If you are a CF admin, you already have the `network.admin` scope. An admin can also grant the `network.admin` scope to a space developer.

For more information, see [Creating and Managing Users with the UAA CLI \(UAAC\)](#) and [Orgs, Spaces, Roles, and Permissions](#).

To grant all Space Developers permissions to configure network policies, open the **Application Developer Controls** pane in your PAS tile and enable the **Allow Space Developers to manage network policies** checkbox.

## Add a Network Policy

To add a policy that allows direct network traffic from one app to another, run the following command:

```
cf add-network-policy SOURCE_APP --destination-app DESTINATION_APP --protocol (tcp | udp) --port RANGE
```

Replace the placeholders in the above command as follows:

- `SOURCE_APP` is the name of the app that sends traffic.
- `DESTINATION_APP` is the name of the app that will receive traffic.
- `PROTOCOL` is one of the following: `tcp` or `udp`.
- `RANGE` are the ports at which to connect to the destination app. The allowed range is from `1` to `65535`. You can specify a single port, such as `8080`, or a range of ports, such as `8080-8090`.

The following example command allows access from the `frontend` app to the `backend` app over TCP at port 8080:

```
$ cf add-network-policy frontend --destination-app backend --protocol tcp --port 8080
Adding network policy to app frontend in org my-org / space dev as admin...
OK
```

## List Policies

You can list all the policies in your space, or just the policies for which a single app is the source:

- To list all the policies in your space, run `cf network-policies`.

```
$ cf network-policies
```

- To list the policies for an app, run `cf network-policies --source MY-APP`. Replace `MY-APP` with the name of your app.

```
$ cf network-policies --source example-app
```

The following example command lists policies for the app `frontend`:

```
$ cf network-policies --source frontend
Listing network policies in org my-org / space dev as admin...

source destination protocol ports
frontend backend tcp 8080
```

## Remove a Network Policy

To remove a policy that allows direct network traffic from an app, run the following command:

```
cf remove-network-policy SOURCE_APP --destination-app DESTINATION_APP --protocol PROTOCOL --port RANGE
```

Replace the placeholders in the above command to match an existing policy, as follows:

- `SOURCE_APP` is the name of the app that sends traffic.
- `DESTINATION_APP` is the name of the app that receives traffic.
- `PROTOCOL` is either `tcp` or `udp`.
- `PORTS` are the ports connecting the apps. The allowed range is from `1` to `65535`. You can specify a single port, such as `8080`, or a range of ports, such as `8080-8090`.

The following command deletes the policy that allowed the `frontend` app to communicate with the `backend` app over TCP on port 8080:

```
$ cf remove-network-policy frontend --destination-app backend --protocol tcp --port 8080
Removing network policy to app frontend in org my-org / space dev as admin...
OK
```

## App Service Discovery

When app service discovery is enabled, apps pushed to Pivotal Application Service can establish container-to-container communications through a known route served by internal BOSH DNS. This allows front end apps to easily connect with back end apps.

To establish container-to-container communications between a front end and back end app, a developer:

1. Launches a back end app that publishes a local endpoint.
2. Maps a named route to the endpoint.
3. Creates a network policy that allows direct traffic from the front end to the back end app.
4. Launches the front end app.

See [Cats and Dogs with Service Discovery](#) in GitHub for an example, written in Go, that demonstrates communication between front end and back end apps.

## Enable App Service Discovery

To enable app service discovery, open the **Application Developer Controls** pane in your PAS tile and enable the **Enable Service Discovery for Apps** checkbox.



## Cloud Foundry Environment Variables

Page last updated:

Environment variables are the means by which the Cloud Foundry (CF) runtime communicates with a deployed application about its environment. This page describes the environment variables that the runtime and buildpacks set for applications.

For information about setting your own application-specific environment variables, see the [Environment Variable](#) section of the *Deploying with Application Manifests* topic.

## View Environment Variables

Install the Cloud Foundry Command Line Interface (cf CLI), and use the [cf env](#) command to view the Cloud Foundry environment variables for your application. The `cf env` command displays the following environment variables:

- The `VCAP_APPLICATION` and `VCAP_SERVICES` variables provided in the container environment
- The user-provided variables set using the [cf set-env](#) command

```
$ cf env my-app
Getting env variables for app my-app in org my-org / space my-space as
admin...
OK
System-Provided:
```

```
{
 "VCAP_APPLICATION": {
 "application_id": "fa05c1a9-0fc1-4fbd-bae1-139850dec7a3",
 "application_name": "my-app",
 "application_uris": [
 "my-app.192.0.2.34.xip.io"
],
 "application_version": "fb8fbcc6-8d58-479e-bcc7-3b4ce5a7f0ca",
 "cf_api": "https://api.example.com",
 "limits": {
 "disk": 1024,
 "fds": 16384,
 "mem": 256
 },
 "name": "my-app",
 "space_id": "06450c72-4669-4dc6-8096-45f9777db68a",
 "space_name": "my-space",
 "uris": [
 "my-app.192.0.2.34.xip.io"
],
 "users": null,
 "version": "fb8fbcc6-8d58-479e-bcc7-3b4ce5a7f0ca"
 }
}
```

```
User-Provided:
MY_DRAIN: http://drain.example.com
MY_ENV_VARIABLE: 100
```

## Application-Specific System Variables

The subsections that follow describe the environment variables that Cloud Foundry makes available to your application container. Some of these variables are the same across instances of a single application, and some vary from instance to instance.

You can access environment variables programmatically, including variables defined by the buildpack. For more information, refer to the buildpack documentation for [Java](#), [Node.js](#), and [Ruby](#).

| Env Var                              | Running | Staging | Task |
|--------------------------------------|---------|---------|------|
| <code>CF_INSTANCE_ADDR</code>        | x       | x       | x    |
| <code>CF_INSTANCE_GUID</code>        | x       |         | x    |
| <code>CF_INSTANCE_INDEX</code>       | x       |         |      |
| <code>CF_INSTANCE_INTERNAL_IP</code> | x       | x       | x    |

|                   |   |   |   |
|-------------------|---|---|---|
| CF_INSTANCE_IP    | X | X | X |
| CF_INSTANCE_PORT  | X | X | X |
| CF_INSTANCE_PORTS | X | X | X |
| CF_STACK          |   | X |   |
| DATABASE_URL      | X |   | X |
| HOME              | X | X | X |
| INSTANCE_GUID     | X |   |   |
| INSTANCE_INDEX    | X |   |   |
| LANG              | X | X | X |
| MEMORY_LIMIT      | X | X | X |
| PATH              | X | X | X |
| PORT              | X |   |   |
| PWD               | X | X | X |
| TMPDIR            | X |   | X |
| USER              | X | X | X |
| VCAP_APP_HOST     | X |   |   |
| VCAP_APP_PORT     | X |   |   |
| VCAP_APPLICATION  | X | X | X |
| VCAP_SERVICES     | X | X | X |

## CF\_INSTANCE\_ADDR

The [CF\\_INSTANCE\\_IP](#) and [CF\\_INSTANCE\\_PORT](#) of the app instance in the format `IP:PORT`.

Example: `CF_INSTANCE_ADDR=1.2.3.4:5678`

## CF\_INSTANCE\_GUID

The UUID of the particular instance of the app.

Example: `CF_INSTANCE_GUID=41653aa4-3a3a-486a-4431-ef258b39f042`

## CF\_INSTANCE\_INDEX

The index number of the app instance.

Example: `CF_INSTANCE_INDEX=0`

## CF\_INSTANCE\_IP

The external IP address of the host running the app instance.

Example: `CF_INSTANCE_IP=1.2.3.4`

## CF\_INSTANCE\_INTERNAL\_IP

The internal IP address of the container running the app instance.

Example: `CF_INSTANCE_INTERNAL_IP=5.6.7.8`

## CF\_INSTANCE\_PORT

The external, or *host-side*, port corresponding to the internal, or *container-side*, port with value [PORT](#). This value is generally different from the [PORT](#) of the app instance.

Example: `CF_INSTANCE_PORT=61045`

## CF\_INSTANCE\_PORTS

The list of mappings between internal, or *container-side*, and external, or *host-side*, ports allocated to the instance's container. Not all of the internal ports are necessarily available for the application to bind to, as some of them may be used by system-provided services that also run inside the container. These internal and external values may differ.

Example: `CF_INSTANCE_PORTS=[{external:61045,internal:8080},{external:61046,internal:2222}]`

## DATABASE\_URL

For apps bound to certain services that use a database, CF creates a `DATABASE_URL` environment variable based on the [VCAP\\_SERVICES](#) environment variable at runtime.

CF uses the structure of the `VCAP_SERVICES` environment variable to populate `DATABASE_URL`. CF recognizes any service containing a JSON object with the following form as a candidate for `DATABASE_URL` and uses the first candidate it finds.

```
{
 "some-service": [
 {
 "credentials": {
 "uri": "SOME-DATABASE-URL"
 }
 }
]
}
```

For example, consider the following `VCAP_SERVICES`:

```
VCAP_SERVICES =
{
 "elephantsql": [
 {
 "name": "elephantsql-c6c60",
 "label": "elephantsql",
 "credentials": {
 "uri": "postgres://exampleuser:examplepass@babar.elephantsql.com:5432/exampledb"
 }
 }
]
}
```

Based on this `VCAP_SERVICES`, CF creates the following `DATABASE_URL` environment variable:

```
DATABASE_URL = postgres://exampleuser:examplepass@babar.elephantsql.com:5432/exampledb
```

## HOME

Root folder for the deployed application.

Example: `HOME=/home/vcap/app`

## LANG

LANG is required by buildpacks to ensure consistent script load order.

Example: `LANG=en_US.UTF-8`

## MEMORY\_LIMIT

The maximum amount of memory that each instance of the application can consume. You specify this value in an application manifest or with the cf CLI when pushing an application. The value is limited by space and org quotas.

If an instance exceeds the maximum limit, it will be restarted. If Cloud Foundry is asked to restart an instance too frequently, the instance will instead be terminated.

Example: `MEMORY_LIMIT=512M`

## PORT

The port on which the app should listen for requests. The Cloud Foundry runtime allocates a port dynamically for each instance of the application, so code that obtains or uses the app port should refer to it using the `PORT` environment variable.

Example: `PORT=8080`

## PWD

Identifies the present working directory, where the buildpack that processed the application ran.

Example: `PWD=/home/vcap/app`

## TMPDIR

Directory location where temporary and staging files are stored.

Example: `TMPDIR=/home/vcap/tmp`

## USER

The user account under which the application runs.

Example: `USER=vcap`

## VCAP\_APP\_PORT

Deprecated name for the [PORT](#) variable defined above.

## VCAP\_APPLICATION

This variable contains the associated attributes for a deployed application. Results are returned in JSON format. The table below lists the attributes that are returned.

| Attribute                     | Description                                              |
|-------------------------------|----------------------------------------------------------|
| <code>application_id</code>   | GUID identifying the application.                        |
| <code>application_name</code> | The name assigned to the application when it was pushed. |
| <code>application_uris</code> | The URIs assigned to the application.                    |
|                               |                                                          |

|                                   |                                                                                                                                                                                                                                                                     |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>application_version</code>  | GUID identifying a version of the application. Each time an application is pushed or restarted, this value is updated.                                                                                                                                              |
| <code>cf_api</code>               | Location of the Cloud Controller API for the CF Deployment where the app runs.                                                                                                                                                                                      |
| <code>host</code>                 | Deprecated. IP address of the application instance.                                                                                                                                                                                                                 |
| <code>limits</code>               | The limits to disk space, number of files, and memory permitted to the app. Memory and disk space limits are supplied when the application is deployed, either on the command line or in the application manifest. The number of files allowed is operator-defined. |
| <code>name</code>                 | Identical to <code>application_name</code> .                                                                                                                                                                                                                        |
| <code>space_id</code>             | GUID identifying the application's space.                                                                                                                                                                                                                           |
| <code>space_name</code>           | Human-readable name of the space where the app is deployed.                                                                                                                                                                                                         |
| <code>start</code>                | Human-readable timestamp for the time the instance was started. Not provided on Diego Cells.                                                                                                                                                                        |
| <code>started_at</code>           | Identical to <code>start</code> . Not provided on Diego Cells.                                                                                                                                                                                                      |
| <code>started_at_timestamp</code> | Unix epoch timestamp for the time the instance was started. Not provided on Diego Cells.                                                                                                                                                                            |
| <code>state_timestamp</code>      | Identical to <code>started_at_timestamp</code> . Not provided on Diego Cells.                                                                                                                                                                                       |
| <code>uris</code>                 | Identical to <code>application_uris</code> . You must ensure that both <code>application_uris</code> and <code>uris</code> are set to the same value.                                                                                                               |
| <code>users</code>                | Deprecated. Not provided on Diego Cells.                                                                                                                                                                                                                            |
| <code>version</code>              | Identical to <code>application_version</code> .                                                                                                                                                                                                                     |

The following example shows how to set the `VCAP_APPLICATION` environment variable:

```
VCAP_APPLICATION={"instance_id":"fe98dc76ba549876543210abcd1234",
"instance_index":0,"host":"0.0.0.0","port":61857,"started_at":"2013-08-12
00:05:29 +0000","started_at_timestamp":1376265929,"start":"2013-08-12 00:05:29
+0000","state_timestamp":1376265929,"limits":{"mem":512,"disk":1024,"fds":16384}
,"application_version":"ab12cd34-5678-abcd-0123-abcdef987654","application_name"
:"styx-james","application_uris":["my-app.example.com"],"version":"ab1
2cd34-5678-abcd-0123-abcdef987654","name":"my-app","uris":["my-app.example.com"]
,"users":null}
```

## VCAP\_SERVICES

For [bindable services](#), Cloud Foundry adds connection details to the `VCAP_SERVICES` environment variable when you restart your application, after binding a service instance to your application.

The results are returned as a JSON document that contains an object for each service for which one or more instances are bound to the application. The service object contains a child object for each service instance of that service that is bound to the application. The attributes that describe a bound service are defined in the table below.

The key for each service in the JSON document is the same as the value of the “label” attribute.

| Attribute                  | Description                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------|
| <code>binding_name</code>  | The name assigned to the service binding by the user.                                            |
| <code>instance_name</code> | The name assigned to the service instance by the user.                                           |
| <code>name</code>          | The <code>binding_name</code> if it exists; otherwise the <code>instance_name</code> .           |
| <code>label</code>         | The name of the service offering.                                                                |
| <code>tags</code>          | An array of strings an app can use to identify a service instance.                               |
| <code>plan</code>          | The service plan selected when the service instance was created.                                 |
| <code>credentials</code>   | A JSON object containing the service-specific credentials needed to access the service instance. |

To see the value of `VCAP_SERVICES` for an application pushed to Cloud Foundry, see [View Environment Variable Values](#).

The example below shows the value of `VCAP_SERVICES` for bound instances of several services available in the [Pivotal Web Services](#) Marketplace.

```
VCAP_SERVICES=
{
 "elephantsql": [
 {
 "name": "elephantsql-binding-c6c60",
 "binding_name": "elephantsql-binding-c6c60",
 "instance_name": "elephantsql-c6c60",
 "label": "elephantsql",
 "tags": [
 "postgres",
 "postgresql",
 "relational"
],
 "plan": "turtle",
 "credentials": {
 "uri": "postgres://exampleuser:examplepass@babar.elephantsql.com:5432/exampleuser"
 }
 }
],
 "sendgrid": [
 {
 "name": "mysendgrid",
 "binding_name": null,
 "instance_name": "mysendgrid",
 "label": "sendgrid",
 "tags": [
 "smtp"
],
 "plan": "free",
 "credentials": {
 "hostname": "smtp.sendgrid.net",
 "username": "QvsXmbJ3rK",
 "password": "HCHMOYluTv"
 }
 }
]
}
```

## Environment Variable Groups

Environment variable groups are system-wide variables that enable operators to apply a group of environment variables to all running applications and all staging applications separately.

An environment variable group consists of a single hash of name-value pairs that are later inserted into an application container at runtime or at staging. These values can contain information such as HTTP proxy information. The values for variables set in an environment variable group are case-sensitive.

When creating environment variable groups, consider the following:

- Only the Cloud Foundry operator can set the hash value for each group.
- All authenticated users can get the environment variables assigned to their application.
- All variable changes take effect after the operator restarts or restages the applications.
- Any user-defined variable takes precedence over environment variables provided by these groups.

The table below lists the commands for environment variable groups.

| CLI Command                                                               | Description                                                               |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <code>running-environment-variable-group</code> or <code>revg</code>      | Retrieves the contents of the running environment variable group.         |
| <code>staging-environment-variable-group</code> or <code>sevg</code>      | Retrieves the contents of the staging environment variable group.         |
| <code>set-staging-environment-variable-group</code> or <code>ssevg</code> | Passes parameters as JSON to create a staging environment variable group. |
| <code>set-running-environment-variable-group</code> or <code>srevg</code> | Passes parameters as JSON to create a running environment variable group. |

The following examples demonstrate how to retrieve the environment variables:

```
$ cf revg
Retrieving the contents of the running environment variable group as
sampledeveloper@example.com...
OK
Variable Name Assigned Value
HTTP Proxy 198.51.100.130

$ cf sevg
Retrieving the contents of the staging environment variable group as
sampledeveloper@example.com...
OK
Variable Name Assigned Value
HTTP Proxy 203.0.113.105
EXAMPLE-GROUP 2001

$ cf apps
Getting apps in org SAMPLE-ORG-NAME / space dev as
sampledeveloper@example.com...
OK

name requested state instances memory disk urls
my-app started 1/1 256M 1G my-app.com

$ cf env APP-NAME
Getting env variables for app APP-NAME in org SAMPLE-ORG-NAME / space dev as
sampledeveloper@example.com...
OK

System-Provided:

{
 "VCAP_APPLICATION": {
 "application_name": "APP-NAME",
 "application_uris": [
 "my-app.example.com"
],
 "application_version": "7d0d64be-7f6f-406a-9d21-504643147d63",
 "limits": {
 "disk": 1024,
 "fds": 16384,
 "mem": 256
 },
 "name": "APP-NAME",
 "space_id": "37189599-2407-9946-865e-8ebd0e2df89a",
 "space_name": "dev",
 "uris": [
 "my-app.example.com"
],
 "users": null,
 "version": "7d0d64be-7f6f-406a-9d21-504643147d63"
 }
}

Running Environment Variable Groups:
HTTP Proxy: 198.51.100.130

Staging Environment Variable Groups:
EXAMPLE-GROUP: 2001
HTTP Proxy: 203.0.113.105
```

The following examples demonstrate how to set environment variables:

```
$ cf ssevg '{"test1":"198.51.100.130","test2":"203.0.113.105"}'
Setting the contents of the staging environment variable group as admin...
OK

$ cf sevg
Retrieving the contents of the staging environment variable group as admin...
OK
Variable Name Assigned Value
test 198.51.100.130
test2 203.0.113.105

$ cf srevg '{"test3":"2001","test4":"2010"}'
Setting the contents of the running environment variable group as admin...
OK

$ cf revg
Retrieving the contents of the running environment variable group as admin...
OK
Variable Name Assigned Value
test3 2001
test4 2010
```





## Cloud Controller API Client Libraries

This topic describes the client libraries available for developers who want to consume the Cloud Controller API (CAPI).

### Overview

CAPI is the entry point for most operations within the Cloud Foundry (CF) platform. You can use it to manage orgs, spaces, and apps, which includes user roles and permissions. You can also use CAPI to manage the services provided by your CF deployment, including provisioning, creating, and binding them to apps.

For more information, see the [CAPI documentation](#).

### Client Libraries

While you can develop apps that consume CAPI by calling it directly as in the API documentation, you may want to use an existing client library. See the available client libraries below.

#### Supported

CF currently supports the following clients for CAPI:

- [Java](#)
- [Scripting](#) with the Cloud Foundry Command Line Interface (cf CLI)

#### Experimental

The following client is experimental and a work in progress:

- [Golang](#)

#### Unofficial

CF does not support the following clients, but they may be supported by third-parties:

- [Golang](#)
- [Golang](#)
- [Node.js](#)

## Considerations for Designing and Running an Application in the Cloud

Page last updated:

### Application Design for the Cloud

Applications written in supported application frameworks often run unmodified on Cloud Foundry, if the application design follows a few simple guidelines. Following these guidelines makes an application cloud-friendly, and facilitates deployment to Cloud Foundry and other cloud platforms.

The following guidelines represent best practices for developing modern applications for cloud platforms. For more detailed reading about good app design for the cloud, see [The Twelve-Factor App](#).

For more information about the features of HTTP routing handled by the Cloud Foundry router, see the [HTTP Routing](#) topic. For more information about the lifecycle of application containers, see the [Application Container Lifecycle](#) topic.

### Avoid Writing to the Local File System

Applications running on Cloud Foundry should not write files to the local file system for the following reasons:

- **Local file system storage is short-lived.** When an application instance crashes or stops, the resources assigned to that instance are reclaimed by the platform including any local disk changes made since the app started. When the instance is restarted, the application will start with a new disk image. Although your application can write local files while it is running, the files will disappear after the application restarts.
- **Instances of the same application do not share a local file system.** Each application instance runs in its own isolated container. Thus a file written by one instance is not visible to other instances of the same application. If the files are temporary, this should not be a problem. However, if your application needs the data in the files to persist across application restarts, or the data needs to be shared across all running instances of the application, the local file system should not be used. We recommend using a shared data service like a database or blobstore for this purpose.

For example, instead of using the local file system, you can use a Cloud Foundry service such as the MongoDB document database or a relational database like MySQL or Postgres. Another option is to use cloud storage providers such as [Amazon S3](#), [Google Cloud Storage](#), [Dropbox](#), or [Box](#). If your application needs to communicate across different instances of itself, consider a cache like Redis or a messaging-based architecture with RabbitMQ.

If you must use a file system for your application because for example, your application interacts with other applications through a network attached file system, or because your application is based on legacy code that you cannot rewrite, consider using [Volume Services](#) to bind a network attached file system to your application.

### Cookies Accessible across Applications

In an environment with shared domains, cookies might be accessible across applications.

Many tracking tools such as Google Analytics and Mixpanel use the highest available domain to set their cookies. For an application using a shared domain such as `example.com`, a cookie set to use the highest domain has a `Domain` attribute of `.example.com` in its HTTP response header. For example, an application at `my-app.shared-domain.example.com` might be able to access the cookies for an application at `your-app.shared-domain.example.com`.

You should decide whether or not you want your applications or tools that use cookies to set and store the cookies at the highest available domain.

### Port Considerations

Clients connect to applications running on Cloud Foundry by making requests to URLs associated with the application. Cloud Foundry allows HTTP requests to applications on ports 80 and 443. For more information, see the [Routes and Domains](#) topic.

Cloud Foundry also supports WebSocket handshake requests over HTTP containing the `Upgrade` header. The Cloud Foundry router handles the upgrade and initiates a TCP connection to the application to form a WebSocket connection.

To support WebSockets, the operator must configure the load balancer correctly. Depending on the configuration, clients may have to use a different port for WebSocket connections, such as port 4443, or a different domain name. For more information, see the [Supporting WebSockets](#) topic.

### Cloud Foundry Updates and Your Application

For application management purposes, Cloud Foundry may need to stop and restart your application instances. If this occurs, Cloud Foundry performs the following steps:

1. Cloud Foundry sends a single `termination signal` to the root process that your start command invokes.
2. Cloud Foundry waits 10 seconds to allow your application to cleanly shut down any child processes and handle any open connections.
3. After 10 seconds, Cloud Foundry forcibly shuts down your application.

Your application should accept and handle the termination signal to ensure that it shuts down gracefully. To achieve this, the application is expected to follow the steps below when shutting down:

1. Application receives termination signal
2. Application closes listener so that it stops accepting new connections
3. Application finishes serving in-flight requests
4. Application closes existing connections as their requests complete
5. Application shuts down or is killed

See the [Sample HTTP Application](#) [GitHub repository](#) for an implementation of the expected shutdown behavior in Golang.

## Ignore Unnecessary Files When Pushing

By default, when you push an application, all files in the application's project directory tree are uploaded to your Cloud Foundry instance, except version control and configuration files or folders with the following names:

- `.cfignore`
- `_darcs`
- `.DS_Store`
- `.git`
- `.gitignore`
- `.hg`
- `manifest.yml`
- `.svn`

In addition to these, if API request diagnostics are directed to a log file and the file is within the project directory tree, it is excluded from the upload. You can direct these API request diagnostics to a log file using `cf config --trace` or the `CF_TRACE` environment variable.

If the application directory contains other files, such as `temp` or `log` files, or complete subdirectories that are not required to build and run your application, you might want to add them to a `.cfignore` file to exclude them from upload. Especially with a large application, uploading unnecessary files can slow application deployment.

To use a `.cfignore` file, create a text file named `.cfignore` in the root of your application directory structure. In this file, specify the files or file types you wish to exclude from upload. For example, these lines in a `.cfignore` file exclude the “tmp” and “log” directories.

```
tmp
log
```

The file types you will want to exclude vary, based on the application frameworks you use. For examples of commonly-used `.gitignore` files, see <https://github.com/github/gitignore>.

## Run Multiple Instances to Increase Availability

Singleton apps may become temporarily unavailable for reasons that include:

- During an upgrade, Pivotal Cloud Foundry (PCF) gracefully shuts down the apps running on each Diego cell and then restarts them on another Diego cell. Single app instances may become temporarily unavailable if the replacement instance does not become healthy within the cell's evacuation

timeout, which defaults to 10 minutes.

- Unexpected faults in PCF system components or underlying infrastructure, such as container-host VMs or IaaS Availability Zones, may cause lone app instances to disappear or become unroutable for a minute or two.

To avoid the risk of an app becoming temporarily unavailable, developers can run more than one instance of the app.

## Using Buildpacks

A buildpack consists of bundles of detection and configuration scripts that provide framework and runtime support for your applications. When you deploy an application that needs a buildpack, Cloud Foundry installs the buildpack on the Diego cell where the application runs.

For more information, see the [Buildpacks](#) [↗](#) topic.

## PCF Security and Compliance Guide

### For Security Professionals and PCF Users

This guide explains how Pivotal Cloud Foundry (PCF) manages network access, roles and permissions, internal communications, container hardening, and other security issues. It is intended to give security professionals a complete view of PCF security, and to help all PCF users, not just the security experts, keep the platform secure.

In addition, this guide provides information about PCF compliance with published control standards and regulations such as [NIST Special Publication 800-53\(r4\)](#) and [GDPR](#).

### Pivotal Security Processes and CVE Reports

Pivotal publishes security updates regularly in response to privately- and publicly-reported Common Vulnerabilities and Exposures (CVEs).

- See the latest CVEs on the [Pivotal Application Security Team](#) page.
- To learn about Pivotal's vulnerability reporting and responsible disclosure process, read [PCF Security Overview and Policy](#).
- To learn about the testing, release and security lifecycle of PCF, see [PCF Testing, Release, and Security Lifecycle](#).

### Security

- [Security Concepts](#): Provides links to conceptual documentation about how security is implemented in PCF.
- [PCF Infrastructure Security](#): Provides guidance and procedures for securing PCF infrastructure such as hardening stemcells and managing the certificates that enable TLS communication.
- [Network Security](#): Covers the security aspects of PCF networking such as the paths, ports, and protocols that components use to communicate.
- [Credential and Identity Management](#): Describes how PCF manages permissions and trust for PCF user accounts. Also provides documentation about CredHub, the credential management system that BOSH uses to store deployment credentials and that PCF runtimes use to create and manage app and service credentials.
- [Security for Apps and Services](#): Collects documentation about the security mechanisms that surround apps and services running on PCF.

### Compliance

- [NIST Controls and PCF](#): Provides a dedicated site that assesses Pivotal Cloud Foundry against NIST SP 800-53(r4) Controls.
- [General Data Protection Regulation](#): Provides an overview of the General Data Protection Regulation (GDPR) and where Pivotal Cloud Foundry (PCF) may store personal data

## Security Processes

This section explains how Pivotal responds to security vulnerabilities, and how it tests and updates its stemcells, the versioned operating systems that its products run on.

- [Pivotal Cloud Foundry Security Overview and Policy](#): Covers Pivotal's responsible disclosure and vulnerability response procedures for the Pivotal Cloud Foundry (PCF) platform.
- [PCF Testing, Release, and Security Lifecycle](#): Explains how Pivotal's practices, tools, and organizational structures work together to create and support stable releases of PCF.
- [PKS Security Disclosure and Release Process](#) [↗](#): Describes the processes for disclosing security issues and releasing related fixes for Pivotal Container Service (PKS), Kubernetes, Cloud Foundry Container Runtime (CFCR), VMware NSX, and VMware Harbor.

## Pivotal Cloud Foundry Security Overview and Policy

Page last updated:

This document outlines our security policy and is addressed to operators deploying [Pivotal Cloud Foundry](#) (PCF) using Pivotal Cloud Foundry Operations Manager.

For a comprehensive overview of the security architecture of each PCF component, refer to the [Cloud Foundry Security](#) topic.

## How Pivotal Monitors for Security Vulnerabilities

Pivotal receives private reports on vulnerabilities from customers and from field personnel via our secure disclosure process. We also monitor public repositories of software security vulnerabilities to identify newly discovered vulnerabilities that might affect one or more of our products.

## How to Report a Vulnerability

Pivotal encourages users who become aware of a security vulnerability in our products to contact Pivotal with details of the vulnerability. Please send descriptions of any vulnerabilities found to [security@pivotal.io](mailto:security@pivotal.io). Please include details on the software and hardware configuration of your system so that we can reproduce the issue.



**Note:** We encourage use of encrypted email. Our public PGP key is located at <http://www.pivotal.io/security>.

## Notification Policy

PCF has many customer stakeholders who need to know about security updates. When there is a possible security vulnerability identified for a PCF component, we do the following:

1. Assess the impact to PCF.
2. If the vulnerability would affect a PCF component, we schedule an update for the impacted component(s).
3. Update the affected component(s) and perform system tests.
4. Announce the fix publicly via the following channels:
  - a. Automated notification to end users who have downloaded or subscribed to a PCF product on [Pivotal Network](#) when a new, fixed version is available.
  - b. Adding a new post to <http://www.pivotal.io/security>.

## Classes of Vulnerabilities

Attackers can exploit vulnerabilities to compromise user data and processing resources. This can affect data confidentiality, integrity, and availability to different degrees. For vulnerabilities related to Ubuntu provided packages, Pivotal follows [Canonical's priority levels](#). For other vulnerabilities, Pivotal follows [Common Vulnerability Scoring System v3.0 standards](#) when assessing severity.

Pivotal uses Canonical's Ubuntu distribution of Linux for PCF Ubuntu stemcells and rootfs. Canonical provides Pivotal with support services allowing us to escalate CVEs that we determine may affect PCF. In general, Pivotal does not escalate to upstream open source software components or vendors for Medium or Low CVEs that are not yet patched. PCF may escalate on behalf of a customer for High or Critical CVEs. PCF customers who are interested in addressing CVEs in Ubuntu that are not yet patched can establish their own support relationship with [Canonical](#).

Pivotal reports the severity of vulnerabilities using the following severity classes:

### High

High severity vulnerabilities are those that can be exploited by an unauthenticated or authenticated attacker, from the Internet or those that break the guest/host Operating System isolation. The exploitation could result in the complete compromise of confidentiality, integrity, and availability of user data

and/or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between Virtual Machines and/or the Host Operating System. This rating also applies to those vulnerabilities that could lead to the complete compromise of availability when the exploitation is by a remote unauthenticated attacker from the Internet or through a breach of virtual machine isolation.

## Moderate

Moderate vulnerabilities are those in which the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to the compromise of confidentiality, integrity, or availability of user data and/or processing resources.

## Low

Low vulnerabilities are all other issues that have a security impact. These include vulnerabilities for which exploitation is believed to be extremely difficult, or for which successful exploitation would have minimal impact.

## Release Policy

PCF schedules regular monthly releases of software in the PCF Suite to address Low / Medium severity vulnerability exploits. When High severity vulnerability exploits are identified, PCF releases fixes to software in the PCF Suite on-demand, with as fast a turnaround as possible.

## Alerts/Actions Archive

<http://www.pivotal.io/security> 



## PCF Testing, Release, and Security Lifecycle

Page last updated:

This topic explains how Pivotal's development practices, automated build tools, and organizational structures work together to create and support stable releases of Pivotal Cloud Foundry (PCF).

### Summary

- PCF teams building system components receive frequent feedback, which helps to secure code from exposure to vulnerability.
- Every PCF release follows a strict workflow and passes through numerous quality and compliance checks before distribution.
- Teams build tests into the product consistently and run them automatically with any code change.

### Release Mechanics

Pivotal releases, patches, and supports multiple versions of PCF simultaneously. This section explains the versioning and support conventions Pivotal follows.

### Versioning

Pivotal numbers PCF releases following a [semantic versioning](#) style format, *X.Y.Z*, where *X* and *Y* indicate major and minor releases, and *Z* designates patch releases. Major and minor releases change PCF functionality; patch releases are backward-compatible security patches or bug fixes.

### Support

As of PCF 1.8, Pivotal supports each major and minor PCF release according to the following criteria:

- Pivotal supports the release for at least 9 months following its first publication date.
- Pivotal supports the last three major or minor releases, even if this extends coverage beyond 9 months.

Support includes maintenance updates and upgrades, bug and security fixes, and technical assistance. The [Pivotal Support Policy](#) describes support standards, technical guidance, and publication phases in more detail. The Pivotal Support Services [Terms and Conditions](#) defines Pivotal support in legal terms.

### Patch Releases

Patch releases are more frequent and less predictable than major/minor releases. The v1.6.x line provides a good example of their frequency. PCF 1.6.1 was released on October 26, 2015. Through August 2016, 36 additional patches of Elastic Runtime 1.6.x and 18 patches of Ops Manager 1.6.x provided security and bug fixes to customers.

Pivotal identifies security issues using standard nomenclature from [Common Vulnerabilities and Exposures \(CVE\)](#), [Ubuntu Security Notices \(USN\)](#), and other third party sources. Read about security fixes in core Cloud Foundry code or packaged dependencies in the release notes for [Ops Manager](#) and [Pivotal Application Service \(PAS\)](#).

[Pivotal.io/security](#) maintains a running list of security fixes in PCF and PCF dependencies. Consult that page to see the most recent findings from Pivotal's security team.

### Upgrading

All PCF releases pass through extensive test suites that include automated unit, integration, and acceptance tests on multiple IaaSes. Regardless of this extensive testing, Pivotal recommends that you test major and minor releases in a non-production environment before implementing them across your deployment. Upgrade your production environment as soon as possible after you validate the new release on your test environment.

## Release Testing, Integration, and Validation

This section describes Pivotal's software development processes and explains compliance and regulatory standards to which Pivotal software adheres.

### Test-Driven Development

Pivotal's development process relies on a strict workflow with continuous automated testing. Pivotal R&D does not separate engineering and testing teams. Rather, every Pivot on each engineering team is responsible for ensuring the quality of their code. They write tests for all of the software components that they develop, often before writing the software itself.

With every software change, automated build pipelines trigger these tests for the new software component and for everything it touches. If a new code check-in does not pass its tests or causes a failure elsewhere, it pauses the build pipeline for the entire team, or sometimes all of Pivotal R&D. The transparency of this process encourages developers to work together to address code issues quickly.

Pivotal applies the following automated testing approaches, scenarios, and frameworks to PCF components and to the release as a whole:

- **Unit tests:** Development teams write unit tests to express and validate desired functional behavior of product components. Typical frameworks used are [RSpec](#) and [Ginkgo](#). These tests run continuously throughout the development cycle.
- **OSS integration tests:** The Release Integration team exercises a full deployment of open-source Cloud Foundry to validate all end-user features. They maintain the [Cloud Foundry Acceptance Test](#) (CATs) suite alongside the OSS cf-release. Cloud Foundry component teams also contribute acceptance test suites at the OSS Integration Test level. These tests exercise and validate their components' functional, performance, and integration health.
- **PCF integration tests:** The PCF Release Engineering (RelEng) team validates the quality and cross-product integration health of the commercial PCF release. RelEng runs OSS Acceptance Tests against all supported releases. These tests run on full PCF instances configured to represent diverse real-world customer scenarios on various IaaSes and using both internal and external load balancer, database, blobstore, and user store solutions.

### Additional Pre-Release Gates: Internal, PWS, and Compliance

In addition to its automated unit and integration testing, Pivotal deploys all upgrades slated for upcoming PCF releases on at-scale test environments. Prior to each Major or Minor commercial release, Pivotal runs the entire Pivotal Cloud Foundry Suite of services on several internally-managed large integration environments that run customer-like data and workloads.

Pivotal also pushes upcoming PCF feature upgrades and patches to its [Pivotal Web Services](#) platform, where customers continually deploy and host hundreds of mission-critical applications at scale, 24/7. The PWS environment gives Pivotal a continuous source of real-world usage and performance metrics that inform product development teams.

All PCF product teams participate in go-to-market steps for each release, as is often required for shipping a legally compliant product. Examples include [Open Source License File](#) attribution and an Export Compliance classification.

## Patch Releases: Security and Bug Fixes

Pivotal uses established processes to track, disclose, and remediate vulnerabilities in PCF and related dependent components. This section explains how Pivotal identifies vulnerabilities and implements fixes for them.

### Identifying Security Vulnerabilities

Pivotal has an established process to track and patch vulnerabilities in software dependencies and PCF software. Additionally, [pivotal.io/security](#) describes a responsible disclosure process for reporting vulnerabilities identified in Pivotal software by 3rd parties.

Pivotal uses multiple methods to identify security vulnerabilities in Pivotal software and dependencies internally, including:

- Security notifications from [Canonical](#) for their Ubuntu operating system, provided through Pivotal's commercial relationship with Canonical
- Software component scans several times per day, using 3rd party security software which updates continuously from external security vulnerability sources
- Dependency analysis software that identifies and catalogs software dependencies
- Security vulnerability notifications from known software dependencies

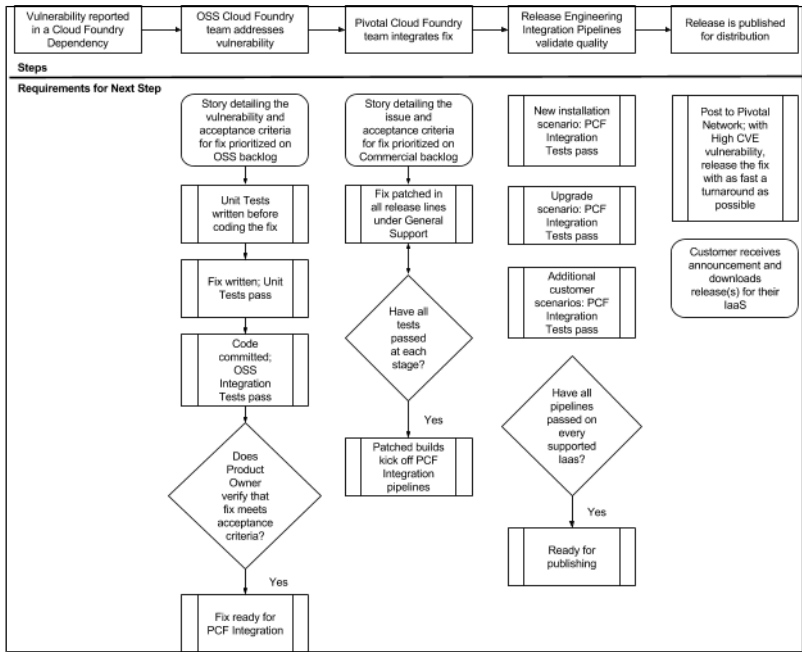
Pivotal also monitors externally-reported vulnerabilities from many sources, including:

- 3rd party security analysis requested by Pivotal
- Cloud Foundry Foundation security notifications from member companies
- Customer, prospect and other 3rd party security reports

When Pivotal discovers a potential security vulnerability in PCF, the security team opens an issue to assess it. If it confirms the vulnerability exists, Pivotal identifies and updates affected components with plans to backport the fix to stable releases. Fixes are implemented on a target timeline based on the [severity level](#) of the vulnerability.







## Fix, Test, and Release Lifecycle

This flowchart details the steps that Pivotal performs on a typical high-priority CVE, to publish a patch release fix on <https://network.pivotal.io> [↗](#):



## Security Concepts

This section provides links to conceptual documentation that describes how Pivotal Cloud Foundry (PCF) implements security at different levels of the platform.

- [Cloud Foundry Security](#) : Provides an overview of the measures Cloud Foundry implements to minimize security risks.
- [Container Security](#) : Describes how PCF isolates containers and limits privileges for containers.
- [Container-to-Container Networking](#) : Illustrates how the Container-to-Container Networking feature enables and secures internal app-to-app communication.
- [Application Security Groups](#) : Explains the different types of application security groups, how they work and how to apply them.
- [Application SSH Components and Processes](#) : Provides an overview of the components that support SSH access to apps.
- [Floating Stemcells](#) : Describes how PCF automatically upgrades all compatible products when a new stemcell is available.

## PCF Infrastructure Security

This section provides links to topics about security infrastructure in Pivotal Cloud Foundry (PCF).

- [Stemcell Security](#): Details how Pivotal tests and updates its stemcells, which supply the base versioned operating system for all PCF products.
- [Certificates and TLS in PCF](#): Provides information on how to manage the certificates that enable TLS communications in PCF.
- [Disk Encryption](#): Describes how to encrypt disks or rotate disk encryption keys in a PCF deployment.
- [Security Event Logging](#): Provides a reference of security-related events logged by the Cloud Controller, CredHub and UAA components in PCF.

## Stemcell Security

This section provides links to topics about how Pivotal implements security in the stemcell layer of Pivotal Cloud Foundry (PCF).

- [Floating Stemcells](#): How PCF automatically upgrades all compatible products when a new stemcell is available.
- [Linux Stemcell Hardening](#): How Pivotal secures Linux stemcells through regular testing and minimizing their surface of vulnerability.

For more information about stemcell availability and related security fixes, see [Stemcell Release Notes](#).

## Linux Stemcell Hardening

 **Note:** This document applies to stemcell v3263 and later.

Customers and prospects often ask for details on stemcell hardening, i.e., the process by which we secure Pivotal Cloud Foundry by reducing its vulnerability surface from outside access. This document provides responses to some commonly-asked questions regarding the security configuration enhancements and hardening tests that Pivotal applies to the Cloud Foundry (“CF”) stemcell. This information will be helpful to customer accreditation teams who are responsible for running configuration scans of a Cloud Foundry deployment, and also to auditors who need a documentation artifact to feed into the customers’ existing security assessment processes.

1. **WHAT IS A STEMCELL?** A stemcell is a versioned Operating System (“OS”) image wrapped with IaaS specific packaging. A typical stemcell contains a bare minimum OS skeleton with a few common utilities pre-installed, a BOSH Agent, and a few configuration files to securely configure the OS by default. For example: with vSphere, the official stemcell for Ubuntu Trusty is an approximately 500MB VMDK file. With AWS, official stemcells are published as MIs that can be used in an AWS account. Stemcells do not contain any specific information about any software that will be installed once that stemcell becomes a specialized machine in the cluster; nor do they contain any sensitive information which would make them unable to be shared with other BOSH users. This clear separation between base OS and later-installed software is what makes stemcells a powerful concept. In addition to being generic, stemcells for one OS (e.g. all Ubuntu Trusty and Xenial stemcells) are exactly the same for all infrastructures. This property of stemcells allows BOSH users to quickly and reliably switch between different infrastructures without worrying about the differences between OS images. The CF BOSH team is responsible for producing and maintaining an official set of stemcells. Cloud Foundry currently supports Ubuntu Trusty and Xenial on vSphere, AWS, OpenStack, Google, and Azure infrastructures.
2. **WHAT IS STEMCELL HARDENING?** Stemcell hardening is the process of securing a stemcell by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one. There are various methods of hardening Linux systems. Common techniques include reducing available methods of attack by implementing more restrictive and/or conservative configurations of the OS kernel and system services, changing default passwords, the removal of unnecessary software, unnecessary usernames and logins, and the disabling or removal of unnecessary services.
3. **WHAT IS OUR GENERAL APPROACH TO STEMCELL HARDENING?** The CF stemcell is essentially a distinct Linux distribution. As such, industry-standard benchmarks are not entirely appropriate when assessing the security posture of the stemcell, but Pivotal has considered and incorporated hardening guidance from various sources both commercial and government. Some parts of the existing recommended industry-standard hardening configurations will certainly apply, but some other parts do not apply. In addition, because each stemcell is a unique Linux distribution, existing industry-standard benchmarks are silent on some important aspects of hardening the stemcell configurations. The following paragraphs describe the different categories of stemcell hardening configurations, and provide a count of the number of tests currently in each category. **Note:** The most current description of what has been delivered is always available in the BOSH public Pivotal Trackers.
  - a. **Baseline Passing:** common hardening tests that pass without any changes to the stemcell or to test procedures. *(130 tests)*
  - b. **Test Amended:** Stemcells are optimized for cloud deployment and some configuration settings are not stored in traditionally-expected locations. The industry standard test was changed to conform with stemcell design to accurately check the recommended setting. This new test reflects the changes to the industry standard test but the stemcell adheres to commonly accepted guidance. *(36 tests)*
  - c. **Additional Hardening:** Configuration hardening improvements that have been made to the stemcell. As with most software, a stemcell’s security improves over time and every stemcell release is tested to ensure that it is suitable for use with its associated CF release. Later releases of a stemcell may include additional security features that were not present in earlier releases. *(86 tests)*
  - d. **New CF-specific Tests:** New tests that have been added to check CF stemcell-specific configurations. These tests are not yet part of any industry standard Ubuntu benchmark. This category of tests is still under development and additional tests will be added over time. *(20 tests)*
4. **WHAT ARE THE MAJOR FOCUS AREAS FOR OUR STEMCELL HARDENING APPROACH?**
  - a. **Maintenance, Updates, and Patching**
    - i. Regular patches and feature enhancements are delivered via routine BOSH deployments of updated stemcells (obviates apt-get upgrade).
  - b. **File System Hardening**
    - i. The /tmp directory is configured to be on a separate partition.
    - ii. Users cannot create character or block special devices in the /tmp filesystem.
    - iii. Users cannot create set uid files in the /tmp filesystem.
    - iv. Users cannot run executable binaries from the /tmp filesystem.
    - v. The temporary storage directories such as /tmp and /var/tmp are mounted on a dedicated partition, and configured with appropriately limiting options such as nodev, nosuid, and noexec.
    - vi. Each of the following directories is in a separate partition, with mount options managed via BOSH agent:
      - /var
      - /var/log
      - /var/log/audit
      - /home

- /tmp

- vii. File system mount options for users' home directories are limited via appropriate mount options including noexec.
- viii. Removable media may not be mounted as character or block special device.
  - ix. Executable programs may not run from removable media.
  - x. setuid and setgid are not allowed on removable media.
  - xi. Users cannot create special devices in shared memory partitions.
  - xii. Users cannot put privileged programs onto shared memory partitions.
  - xiii. Users cannot execute programs from shared memory partitions.
  - xiv. Users cannot delete or rename files in world-writable directories such as /tmp that are owned by other users.
  - xv. Supplementary and exotic Linux file systems that are unused in CF have been disabled.
  - xvi. Additional supplementary and exotic Linux file systems that are unused in CF have been disabled.
  - xvii. Automount of USB drives or disks is not permitted.

## c. Boot Security

- i. The owner and group for the bootloader config (/boot/grub/grub.cfg) is set to root. Only root has read and write access to this file.
- ii. Boot loader has been configured so that a password is required to reboot the system.
- iii. Unauthorized users cannot reboot the system into single user mode.

## d. Process Security

- i. Users cannot override the soft limit for core dumps.
- ii. Randomized virtual memory region placement is enabled.
- iii. Prelinking of shared libraries is disabled.

## e. Minimization of Attack Surface

- i. The Network Information Service ("NIS") is not used in CF and is not installed.
- ii. The Berkeley rsh-server package is not used in CF and is disabled.
- iii. Classic rsh-related tools are not used in CF and are not installed.
- iv. The following servers are not used on CF stemcells and are disabled:

- talk server
- telnet server
- tftp-server
- Avahi
- print
- DHCP
- DNS
- FTP
- IMAP
- POP
- HTTP
- SNMP

- v. The talk client is not used in CF and is not installed.
- vi. The eXtended InterNET Daemon (xinetd) is not used in CF and is disabled.
- vii. The following network services are not used in CF and are disabled:

- chargen
- daytime
- echo
- discard
- time

- viii. The X Window system is not used in CF and is not installed.
- ix. NTP time setting is synchronized on the stemcell via the ntpdate utility.
- x. The Samba daemon is not used in CF and is disabled.
- xi. The Mail Transfer Agents (MTA) process only local mail.
- xii. The rsync service is not used in CF and is disabled.
- xiii. The biosdevname tool is disabled.

## f. Network Security

- i. IPv4 networking is configured such that IP forwarding is disabled.
- ii. The IPv4 networking has been configured such that the host cannot send ICMP redirects.
- iii. IPv4 networking has been configured such that the system does not accept source routed packets.
- iv. IPv4 networking is configured such that ICMP redirects are not accepted.
- v. ICMP echo and timestamp requests with broadcast or multicast destinations will be ignored.



- vi. The stemcell will ignore malformed ICMP error responses.
- vii. IPv4 networking is configured for source route validation.
- viii. TCP SYN cookies are enabled.
- ix. Stemcells are set to refuse IPv6 router advertisements.
- x. The `/etc/hosts.allow` file exists and is empty.
- xi. The `/etc/hosts.allow` and `/etc/hosts.deny` files are protected from unauthorized write access.
- xii. The `/etc/hosts.deny` file exists and is empty.
- xiii. The following protocols are not used in CF and are disabled:

- SCTP
- DCCP
- TIPC
- LDAP
- RDS

- xiv. Wireless interfaces are disabled.
- xv. IPv6 is not used in CF deployments and the IPv6 protocol is disabled.

## g. Auditing

- i. Audit log file size is configured for a manageable maximum size of 6 MB.
- ii. The system auditd logs have been configured such that the system is resilient in the event of a denial of service attack on the auditd daemon.
- iii. Auditd daemon is configured such that all auditd logs are kept after rotation.
- iv. The auditd service is enabled.
- v. Auditing of successful and failed login/logout events is enabled.
- vi. The Linux auditing subsystem has been configured in accordance with best practice industry guidance to capture all security-relevant events. The `/etc/audit/audit.rules` configuration now contains more than 50 monitoring rules.
- vii. Audit records are created for loading and unloading of kernel modules and for system calls.
- viii. File Integrity Monitoring can be done on the stemcell (via a BOSH Add-on).

## h. Authentication and Authorization

- i. The cron daemon is enabled.
- ii. Access to the `/etc/crontab` file is limited to root.
- iii. Access to the cron utility configuration via the hourly, daily, weekly, and monthly directories is limited.
- iv. User authorization to schedule cron jobs is limited.
- v. Only the `vcap` user is whitelisted to use the cron and at utilities.
- vi. Password requirements follow industry best practice guidance and enforce a minimum length of 14 characters, with at least one each of: digit, uppercase, lowercase and special characters.
- vii. Password reuse: users cannot reuse their twenty most recent passwords.
- viii. SSH protocol version is configured for SSH-2.
- ix. Logging level for SSH event is INFO.
- x. Minimum permissions are set on `/etc/ssh/sshd_config`.
- xi. SSH X11 forwarding is disabled.
- xii. The `MaxAuthTries` parameter for SSH is set to 3 attempts per connection.
- xiii. SSH is configured to require passwords and ignore host-based authentication.
- xiv. Root logins are not allowed over SSH.
- xv. Users cannot set environment variables through the SSH daemon.
- xvi. SSH has been configured to use strong ciphers:

- aes128-ctr
- aes192-ctr
- aes256-ctr

- xvii. Idle SSH sessions are terminated after 15 minutes, and no client “keep alive” messages are sent.
- xviii. Idle SSH sessions are terminated after 15 minutes. No client “keep alive” messages are sent.
- xix. The SSH login banner may be configured to display site-specific text before user authentication is permitted (via BOSH Add-on).
- xx. Root login is only permitted via console, not via tty devices.
- xxi. Only the `vcap` user is authorized in the sudo group.
- xxii. Only users in the root group (a.k.a. wheel) are authorized to run the `su` command.

## i. Compliance

- i. Contents of `/etc/issue` and `/etc/issue.net` have been configured to the phrase: “Unauthorized use is strictly prohibited. All access and activity is subject to logging and monitoring.” This may be amended if and as necessary via a BOSH Add-on.
- ii. The Message of the Day file `/etc/motd` is not used, but may be populated via a BOSH Add-on if needed.
- iii. Identification of the OS and/or version information about the OS does not appear in any login banners.

## j. File System Permissions








- i. The `/etc/passwd`, `/etc/shadow`, and `/etc/group` files are protected from unauthorized write access.
- ii. Use and/or presence of any world-writable files has been audited, and minimized to the extent possible for CF.
- iii. By default, all stemcell files are owned by a known user and group, and may not belong to a non-existent user or group.
- iv. Use of SUID and GUID is restricted, and only the `/usr/bin/sudo` and `/bin/su` programs are authorized as SUID and/or GUID programs.

## k. User Account Management

- i. Users cannot change their password more than once a day.
- ii. Users are notified 7 days before their passwords expire.
- iii. Interactive logins are disabled for system accounts.
- iv. The GID for the root account is 0.
- v. User accounts may not have empty passwords.
- vi. NIS is not used in CF, and integration of OS security configuration with legacy NIS permissioning is not enabled (e.g., for `/etc/passwd`, `shadow`, and `group`).
- vii. By default, the only UID 0 account present is root.
- viii. By default, the root PATH does not include any risky directory such as the current working (`.`) or any writable directory.
- ix. Minimum privileges are applied to all users' hidden configuration ("dot") files.
  - x. The `.netrc` and `.rhosts` and `.forward` files are not used in CF and are not present in any user home directory.
- xi. Any group present in the `/etc/passwd` file must also exist in the `/etc/group` file.
- xii. Users defined in `/etc/passwd` must have a valid home directory.
- xiii. Users must own their home directories.
- xiv. All references to user and group names, as well as UID and/or GID identifiers, are self consistent, with no duplicates or orphans allowed.
- xv. By default, the shadow group is not used in CF and must be empty.

## Certificates and TLS in PCF

This section provides links to topics about certificate and TLS infrastructure in Pivotal Cloud Foundry (PCF).

- [TLS Connections in PCF](#) : Provides information on TLS is used in PCF deployments, including supported TLS cipher-suites.
- [Securing Traffic into Cloud Foundry](#) : Provides instructions on how to how to configure Transport Layer Security (TLS) termination for HTTP traffic into PCF.
- [Providing a Certificate for Your TLS Termination Point](#)  Describes how to configure TLS certificates for Pivotal Application Service (PAS).
- [Managing Certificates with the Ops Manager API](#) : Describes how to manage internal certificate authorities (CAs) and certificates in PCF that are visible to the Ops Manager API.
- [Rotating Certificates](#) : Describes how to rotate internal CAs and certificates in PCF.
- [Adding a Custom Certificate Authority](#) : Describes how to add a custom CA to issue digital certificates in a Pivotal Cloud Foundry (PCF) deployment
- [Trusted System Certificates](#) : Discusses where apps deployed to PAS can find trusted system certificates.

TLS Connections in PCF

This topic classifies the different paths through which external clients, internal components, app containers, and app services communicate in Pivotal Cloud Foundry (PCF), and how the platform uses Transport Layer Security (TLS) protocols to secure these communications.

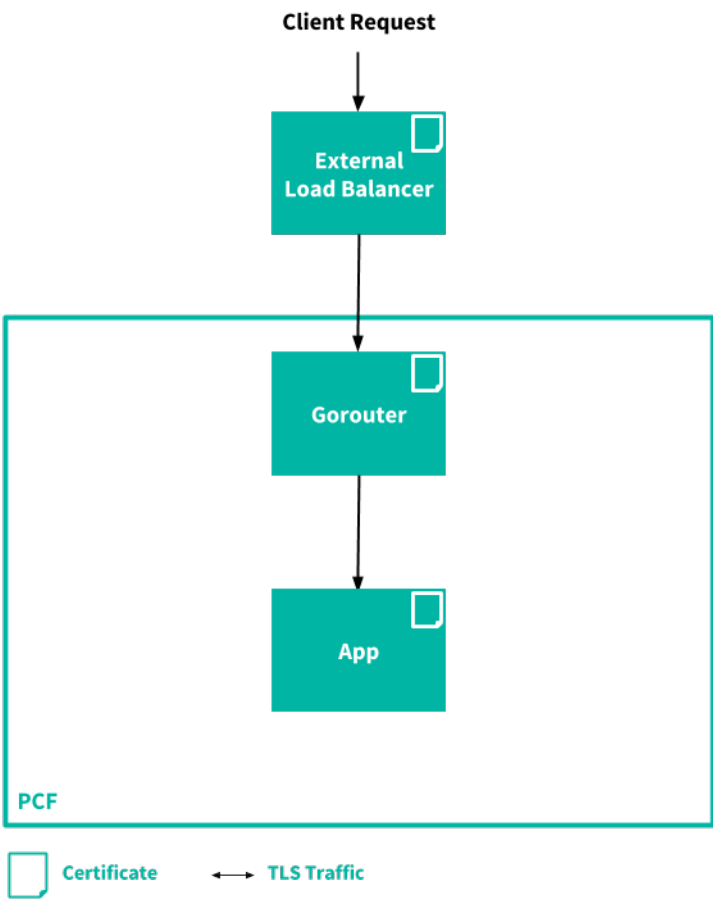
Types of Network Communication in PCF

This section classifies the different types of network communication in PCF and how they are secured with TLS.

Within a PCF deployment, TLS secures connections between components like the BOSH Director and service tiles. PCF components also use TLS connections to secure communications with external hardware, such as customer load balancers.

Between an External Client and an App

The following diagram illustrates the flow of communication from a client making a request to an app:

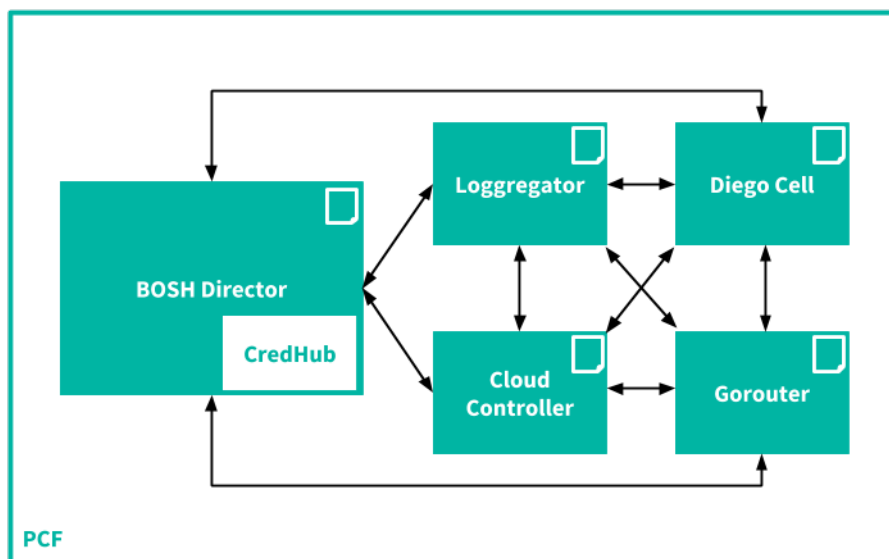


The following table describes each component involved in receiving a client request and where their certificates for TLS termination originate.

| Component              | Certificate Source                                                                                                                      |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| External Load Balancer | Enterprise Root CA.                                                                                                                     |
| Gorouter               | Enterprise Root CA.                                                                                                                     |
| App                    | PCF root CA dedicated to app instance identity. For more information, see <a href="#">App Instance Container Identity Credentials</a> . |

Between Platform Components

The following diagram illustrates communication between platform components, secured with TLS.



The CredHub instance in BOSH generates certificates for all components in PCF. The certificates are self signed by default. To issue certificates signed by your enterprise, you can add a custom CA to CredHub.

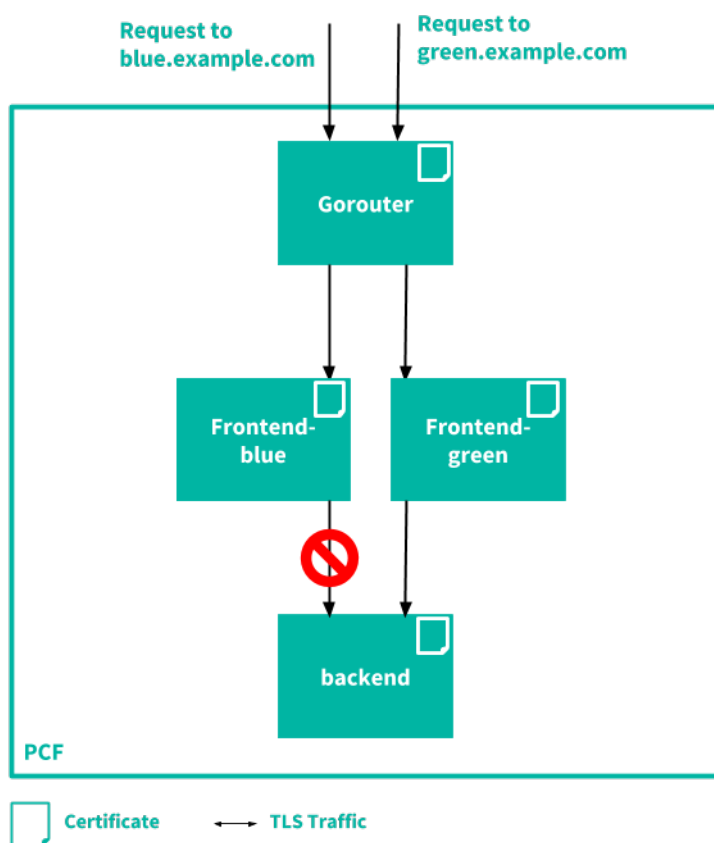
## Component Communication Details

The following topics list the paths, ports, and protocols that subsystems within Pivotal Application Service (PAS) use to communicate.

- [Cloud Controller Network Communications](#)
- [Diego Network Communications](#)
- [Loggregator Network Communications](#)
- [MySQL Network Communications](#)
- [NATS Network Communications](#)
- [Routing Network Communications](#)
- [UAA Network Communications](#)

## Between Apps

The following diagram illustrates TLS communications between apps running on PCF. In this example, the `frontend-blue` and `frontend-green` apps both receive client requests, but only the `frontend-green` app is allowed to communicate with the `backend` app.

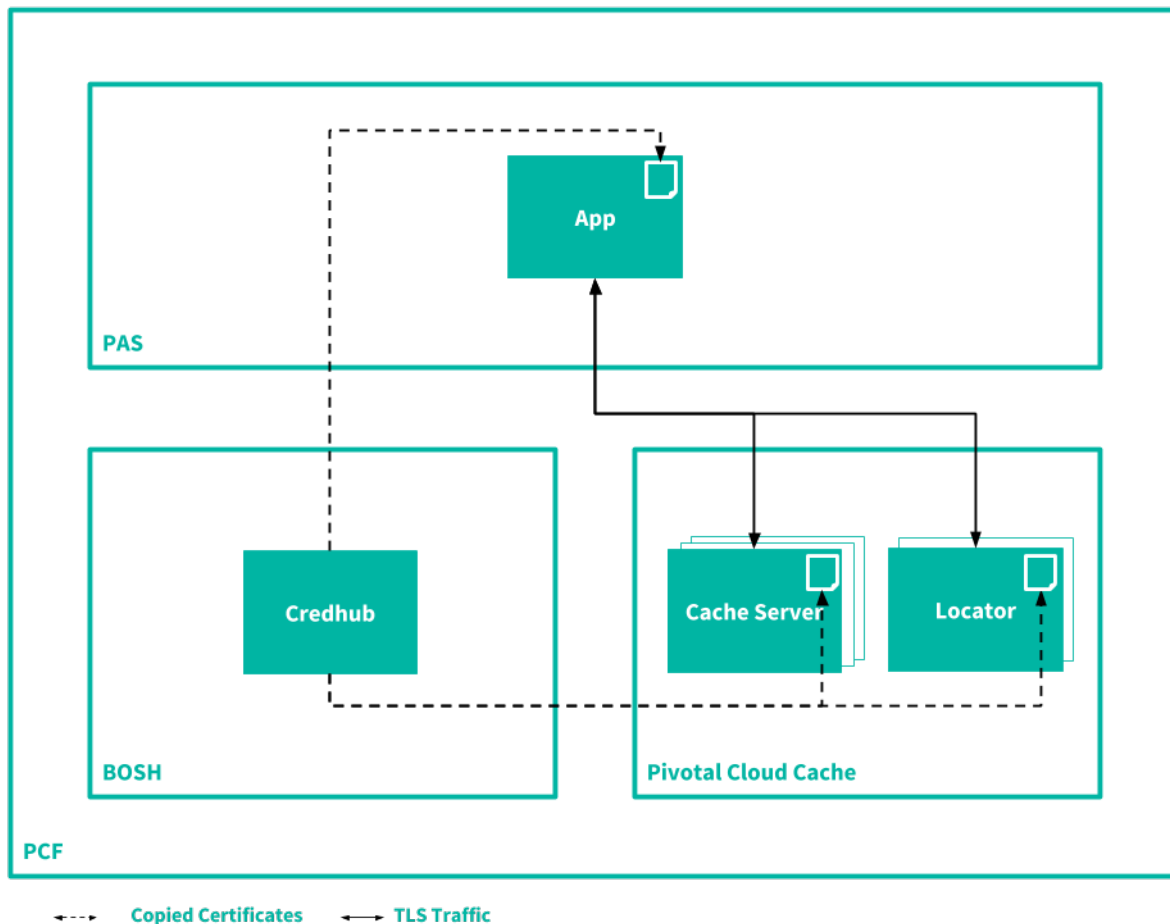


Apps can communicate with each other over TLS using certificates generated by a PCF root CA dedicated to app instance identity. For more information, see [App Instance Container Identity Credentials](#).

Developers specify which apps are allowed to communicate using container networking policies. For more information, see [Configuring Container-to-Container Networking](#).

## Between Apps and On-Platform Services

The following diagram illustrates TLS communication between apps and managed, on-platform services. It uses Pivotal Cloud Cache as an example of a managed service.

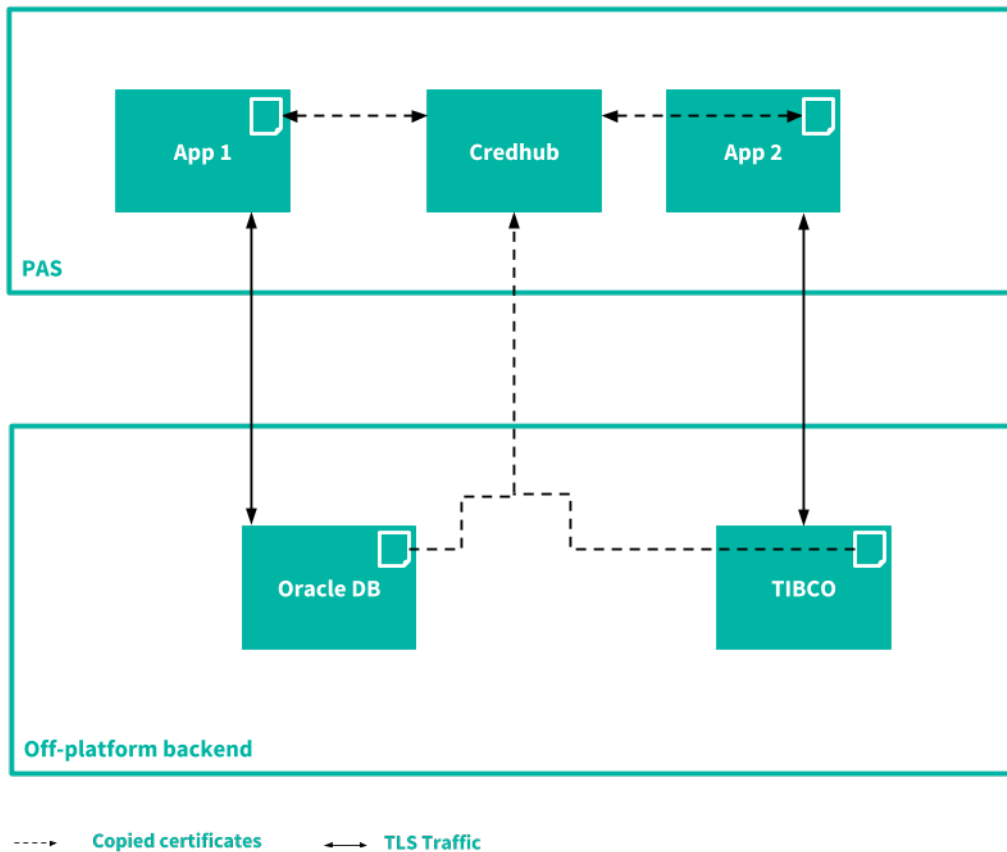


BOSH CredHub issues certificates to the Pivotal Cloud Cache components. For the app, the developer must retrieve a copy of this certificate using the CredHub API and place it in the truststore for the app. For more information, see the [Developing an App Under TLS](#) document in the Pivotal Cloud Cache documentation.

Separately, PAS Runtime Credhub might store credentials for the app to access a service over the TLS connection, adding a second layer of security. For more information, see [Securing Services Instance Credentials with Runtime CredHub](#).

## Between Apps and External Services

The following diagram illustrates communications between apps and external, brokered services secured with TLS.



The developer must retrieve the certificate from the external service and provide it to their app. One way to do this is by placing the certificate in Runtime CredHub and modifying your app to consume the certificate through the [CredHub Service Broker for PCF](#).

## App Instance Container Identity Credentials

Each app instance container in PCF has its own identity credentials. This section is meant to help PCF operators and developers [understand](#) and [use](#) these credentials.

### About App Instance Identity Credentials

See the following table to learn about app instance identity credentials.

| Attribute                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                      | <ul style="list-style-type: none"> <li>For app developers to enable secure TLS communications from their apps.</li> <li>For PCF to use internally to validate the identities of app instances.</li> </ul>                                                                                                                                                                                                                           |
| <b>Type</b>                         | <ul style="list-style-type: none"> <li>A PEM-encoded <a href="#">X.509</a> certificate and <a href="#">PKCS #1 RSA</a> private key.</li> </ul>                                                                                                                                                                                                                                                                                      |
| <b>Location</b>                     | <ul style="list-style-type: none"> <li>PCF presents the certificate and private key to the app instance through the container filesystem.</li> </ul>                                                                                                                                                                                                                                                                                |
| <b>Properties of certificate</b>    | <ul style="list-style-type: none"> <li>The <b>Common Name</b> is the app instance GUID.</li> <li>The <b>Subject</b> of the certificate contains an <i>Organizational Unit</i> in the form of <code>app:APP-GUID</code>.</li> <li>The certificate contains a <b>Subject Alternative Name (SAN)</b> with the IP address for the app instance container.</li> <li>The certificate is valid for 24 hours after being issued.</li> </ul> |
| <b>Contents of certificate file</b> | <ul style="list-style-type: none"> <li>A chain of PEM-encoded certificates, with the instance-specific certificate first in the list and any intermediates following it.</li> </ul>                                                                                                                                                                                                                                                 |
|                                     | <ul style="list-style-type: none"> <li>PCF includes a root Certificate Authority (CA) dedicated to app instance identity. This CA is saved in the system trust</li> </ul>                                                                                                                                                                                                                                                           |



|                   |                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------|
| Issuing authority | store for buildpack-based apps and in a file in <code>/etc/cf-system-certificates</code> in all app instance containers. |
|-------------------|--------------------------------------------------------------------------------------------------------------------------|

## Using the Credentials

If you want to enable secure TLS communications from an app using container instance identity credentials, ensure that you do the following:

- **Add the credentials to your development stack configuration:**
  - The credentials must be present in your development stack configuration for your app to use them. You can retrieve the credentials through following environment variables, which PCF sets to the locations of key and certificate files.

| Credential / Keypair Element | Environment Variable          | Command to Retrieve Credential Value                     |
|------------------------------|-------------------------------|----------------------------------------------------------|
| Certificate Chain            | <code>CF_INSTANCE_CERT</code> | <code>cf ssh APP-NAME -c 'cat \$CF_INSTANCE_CERT'</code> |
| Private Key                  | <code>CF_INSTANCE_KEY</code>  | <code>cf ssh APP-NAME -c 'cat \$CF_INSTANCE_KEY'</code>  |


- **Reload the credential files before they expire:**
  - PCF rotates the credentials shortly before the current certificate expires. Apps that use these credentials must reload the certificate and key file contents either periodically or in reaction to filesystem watcher events.
- **Configure external clients or servers to trust the root CA:**
  - To enable secure TLS communication between an app and a client or server external to PCF, you must configure the external client or server to trust the CA that issues app instance container identity credentials. See the *Issuing Authority* row of the table in [About App Instance Identity Credentials](#).

## Additional Information

For more information about instance identity credentials, see the [Instance Identity](#) document in the diego-release repository.

## TLS Cipher Suites

By default, PCF uses a limited set of cipher suites to secure its internal communications. However, some components used in PCF, like the Gorouter and HAProxy, may support additional TLS cipher suites to accommodate older clients outside of PCF.

 The AWS Classic load balancer does not support the recommended TLS cipher suites. See [Securing Traffic into Cloud Foundry](#) for details and mitigations.

For components that allow you to configure TLS cipher suites, only specify the TLS cipher suites that you need.

## TLS Cipher Suite Recommendations

The default and recommended version of TLS to use is TLS v1.2.

The recommended TLS cipher suites to use within PCF are the following:

- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

## Gorouter Configuration


As part of your PAS networking configuration, you must specify the TLS cipher suites that the Gorouter uses to secure its communications. Only specify the cipher suites that you need.

The recommended TLS cipher suites for the Gorouter are:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

You can specify other cipher suites and a different minimum version of TLS support if your deployment requires it. For a list of other cipher suites and other versions of TLS that are optionally supported by the Gorouter, see [Securing Traffic into Cloud Foundry](#).

For instructions on how to configure the TLS cipher suites for the Gorouter, see the PAS installation documentation for the IaaS of your deployment. For example, if you are deploying PAS on GCP, see [Step 6: Configure Networking](#).

 **Note:** In PAS v2.3, traffic between the Gorouter and Cloud Controller is encrypted. To ensure there is no downtime while upgrading from v2.2 to v2.3, download the latest patch for v2.2. This patch contains the configuration `router.backends.enable_tls: true` in the Gorouter manifest.

## HAProxy Configuration

As part of your PAS networking configuration, you must specify the TLS cipher suites that HAProxy uses to secure its communications. Only specify the cipher suites that you need.

The recommended TLS cipher suites for HAProxy are:

- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

You can specify other cipher suites and a different minimum version of TLS support if your deployment requires it. For a list of other cipher suites and other versions of TLS that are optionally supported by HAProxy, see [ciphers - Cipher Suite Names](#) in the OpenSSL documentation.

If you use the default and recommended Gorouter TLS cipher suites in PAS, then ensure you have included these Gorouter TLS cipher suites in your HAProxy TLS cipher suite configuration.

If you change the default Gorouter TLS cipher suites in PAS, and you change the TLS cipher suites for HAProxy, ensure that you have at least one overlapping TLS cipher suite within the two sets.

For instructions on how to configure the TLS cipher suites for HAProxy, see the PAS installation documentation for the IaaS of your deployment. For example, if you are deploying PAS on GCP, see [Step 6: Configure Networking](#).


## Custom Certificate Authorities

This topic provides an overview of using custom certificate authorities (CAs) in a Pivotal Cloud Foundry (PCF) deployment.

### Overview

To secure traffic in your PCF deployment, you must provide a CA to issue digital certificates. This can be either a Pivotal-generated or custom CA. When you add and activate a new CA, a digital certificate is issued to BOSH Director. BOSH Director then passes the certificate to other components in your PCF deployment.

Pivotal recommends you supply a CA from a trusted provider when using a production environment. While you can create your own custom CAs if necessary, a trusted CA is more secure because it has been authenticated by the trusted entities permitted to issue them.

 **Note:** Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are not supported in PCF.

### Add a Custom CA

You can add a new custom CA as part of the procedure for rotating CAs and other certificate types in PCF. To add and activate a new custom CA in PCF, see [Rotate Root and Leaf Certificates](#).

## Managing Certificates with the Ops Manager API

This topic describes how to manage and retrieve information about certificates in PCF using the Ops Manager API.

### Overview

The Ops Manager API includes endpoints for managing and retrieving information about certificates in a PCF deployment.

For more information about Ops Manager API endpoints for managing certificates, see [Certificate Authorities](#) in the Ops Manager API documentation.

### Prerequisites

To use the Ops Manager API, you must generate an access token by authenticating with the Ops Manager User Account and Authentication (UAA) server.

For more information about authenticating with UAA, see [Using Ops Manager API](#).

### Generate a Single RSA Certificate

To generate and return a new RSA certificate signed by the root certificate authority (CA), use `curl` to make the following API call:

```
curl "https://OPS-MAN-FQDN/api/v0/certificates/generate \
-X POST \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

Where `YOUR-UAA-ACCESS-TOKEN` is your Ops Manager access token without any newline characters such as `\n`.

### Retrieve the Ops Manager Root CA

You can view the Ops Manager root CA as a file or in JSON format.

#### Retrieve the Ops Manager Root CA as a File

To return the Ops Manager root CA as a file, use `curl` to make the following API call:

```
curl "https://OPS-MAN-FQDN/download/_root/_ca/_cert \
-X GET \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

Where `YOUR-UAA-ACCESS-TOKEN` is your Ops Manager access token without any newline characters such as `\n`.

#### Retrieve the Ops Manager Root CA as JSON

To return the Ops Manager root CA as JSON, use `curl` to make the following API call:

```
curl "https://OPS-MAN-FQDN/api/v0/security/root/_ca/_certificate \
-X GET \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

Where `YOUR-UAA-ACCESS-TOKEN` is your Ops Manager access token without any newline characters such as `\n`.

### List all RSA Certificates

To return metadata from all deployed RSA certificates visible to Ops Manager, except the root CAs, use `curl` to make the following API call:

```
curl "https://OPS-MAN-FQDN/api/v0/deployed/certificates \
-X GET \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

Where `YOUR-UAA-ACCESS-TOKEN` is your Ops Manager access token without any newline characters such as `\n`.

## Rotating Certificates

This topic describes how to rotate the root certificate authorities (CAs) and leaf certificates in Pivotal Cloud Foundry (PCF) that are visible to the Ops Manager API.

This topic includes the following:

- A list of the different types of certificates that require planned rotation. See [Certificate Types](#).
- Instructions for checking the expiration date of and rotating the Ops Manager root CAs and leaf certificates. See [Master Procedure: Check and Rotate Certificates](#).

For information about rotating IPsec certificates, see [Rotating IPsec Certificates](#).

For information about using trusted third-party certificates for both apps hosted on PCF and internal PCF components, see [Setting Trusted Certificates](#).

.

## Overview

The Ops Manager API manages and lists internal certificates that enable PCF components to communicate with each other securely using TLS. It can also list certificates used externally, such as SAML certificates that authenticate to an external identity provider.

To keep PCF running, you must keep track of which certificates are set to expire soon, and rotate them before they expire. To do this, follow the instructions in [Master Procedure: Check and Rotate Certificates](#).

## Certificate Types

PCF uses a root CA and various leaf certificates. Root CAs are self-signed certificates that issue leaf certificates. Root CAs can be generated by Pivotal or custom.

Leaf certificates are signed by a CA and are used to identify resources in PCF. Both root CAs and leaf certificates require planned rotation in PCF.

The following types of PCF certificates require planned rotation:

- **Ops Manager Root CA:** The Ops Manager root CA issues other certificates that PCF uses. The root CA can be a Pivotal-generated CA or your own custom CA. For more information about viewing the root CAs for Ops Manager, see [Listing the Root Certificate Authorities](#).
- **Non-configurable Certificates:** Non-configurable certificates are leaf certificates either created by a CA stored in Ops Manager, or created and stored by CredHub and managed by Ops Manager calls to the CredHub API. Non-configurable certificates are issued directly by the Ops Manager root CA, or by intermediate CAs in a chain of trust originated by the root CA. For more information about viewing non-configurable leaf certificates, see [Getting Information About Certificates for Products](#). For more information about generating non-configurable leaf certificates, see [Generating New Certificates](#).
- **Configurable Certificates:** Configurable certificates are leaf certificates supplied by the user and pasted into configuration fields in Ops Manager. Some configuration panes include a **Generate RSA Certificate** button that supplies valid certificates, but users can obtain configurable certificates from elsewhere. For more information about viewing configurable leaf certificates, see [Getting Information About Certificates for Products](#).
- **Non-rotatable Certificates:** Non-rotatable certificates are leaf certificates that, like non-configurable certificates, are issued by the root CA. Unlike non-configurable certificates, non-rotatable certificates cannot be rotated by the Ops Manager API. For more information about viewing non-rotatable leaf certificates, see [Getting Information About Certificates for Products](#).

In addition to the types of certificates listed above, some Pivotal products issue their own tile certificates that are not managed by or visible to the Ops Manager API. These tile certificates do not require planned rotation because they rotate automatically with product upgrades.

Pivotal Application Service (PAS) and Pivotal Container Service (PKS) both use tile certificates in addition to their Ops Manager certificates.

## Master Procedure: Check and Rotate Certificates

The following master procedure checks expiration dates of different types of internal certificates and rotates them only as necessary. You can run this procedure only when records show that your certificates will expire soon, or else periodically to comply your organization's security compliance policies.

To check and rotate certificates, do the following:

- 

c. If you have non-configurable leaf certificates expiring soon, but not your root CA, follow the [Rotate Non-Configurable Certificates](#) procedure.

d. If you have configurable leaf certificates expiring soon, but not your root CA, follow the [Rotate Configurable Certificates](#) procedure.

Complete the following procedures to check the expiration dates and types of CAs and leaf certificates that the Ops Manager API lists and manages.

This procedure describes how to check the expiration date for the Ops Manager root CA. The Ops Manager root CA expires four years after creation.

1. Perform the steps in the [Using Ops Manager API](#) topic to target and authenticate with the Ops Manager User Account and Authentication (UAA) server. Record your Ops Manager access token, and use it for `YOUR-UAA-ACCESS-TOKEN` in the steps below.



2. To retrieve the Ops Manager root CA, use `curl` to make an Ops Manager API call to the `https://OPS-MAN-FQDN/api/v0/certificate_authorities` endpoint. For example:


3. To make the JSON output more readable, you can pipe it to [jq](#) or another text editor with JSON formatting.

4. In the `certificate_authorities` list returned, if there is more than one, find the CA with `"active": true`.
5. To determine its expiration date of the active CA, refer to its `expires_on` value. For example, the root CA shown below expires on September 5, 2019:

This procedure describes how to check the expiration dates of non-configurable and configurable leaf certificates. Non-configurable leaf certificates expire after two years. Configurable leaf certificates generated by Ops Manager also typically expire after two years.

2.2

1. If you haven't already, perform the steps in the [Using Ops Manager API](#) topic to target and authenticate with the Ops Manager User Account and Authentication (UAA) server. Record your Ops Manager access token, and use it for `YOUR-UAA-ACCESS-TOKEN` in the steps below.

 **Note:** When you record your Ops Manager access token, remove any newline characters such as `\n`.

2. To check the system for certificates that expire within a given time interval, use `curl` to call the `https://OPS-MAN-FQDN/api/v0/deployed/certificates?expires_within=TIME` API endpoint, replacing `TIME` with an integer-letter code. Valid letter codes are `d` for days, `w` for weeks, `m` for months, and `y` for years.

For example, the following command searches for certificates expiring within six months:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/certificates?expires_within=6m" \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

Replace `YOUR-UAA-ACCESS-TOKEN` with the `access_token` value you recorded in the previous step.

3. To make the JSON output more readable, you can pipe it to [jq](#) or another text editor with JSON formatting.
4. To determine the expiration date of each certificate, refer to its `expires_on` value.
5. To determine the type of each certificate in the output, follow the [Identify Non-Configurable, Configurable, and Unrotatable Leaf Certificates](#) procedure.

## Identify Non-Configurable, Configurable, and Unrotatable Leaf Certificates

Output from the `deployed/certificates` endpoint, such as the output generated in the [Check Leaf Certificate Expiration Dates](#) procedure, combines information about non-configurable, configurable, and unrotatable leaf certificates into a single list.

You need to manually rotate the different leaf certificate types in different ways.


The following rules identify the type of each leaf certificate requiring rotation:

- **Non-Rotatable Certificates:** Non-Rotatable leaf certificates have the following property value:
  - `variable_path` is `/opsmgr/bosh_dns/tls_ca`

If you have non-rotatable certificates expiring soon, call [Pivotal Support](#).
- **Non-Configurable Certificates:** Non-Configurable leaf certificates have the following property values, but are not non-rotatable as identified above:
  - `configurable` is `false`
  - `location` is either `ops_manager` or `credhub`
- **Configurable Certificates:** Configurable leaf certificates have the following property value:
  - `configurable` is `true`

## Rotate CAs and Leaf Certificates

The following procedures rotate CAs and leaf certificates that are listed or managed by the Ops Manager API.

 **Note:** The rotation procedures described in this topic does not work when your certificates have already expired. If your certificates have expired, contact [Pivotal Support](#) for guidance.

### Rotate Root and Leaf Certificates

This procedure uses the Ops Manager API to rotate the Ops Manager root CA and non-configurable leaf certificates.

Rotating the Ops Manager root CA automatically rotates all configurable leaf certificates. You can also rotate configurable leaf certificates separately from rotating the root CA. For information about rotating configurable leaf certificates without also rotating the root CA, see [Rotate Configurable Certificates](#).

PCF users never need to manually rotate intermediate CAs, because they rotate automatically when the root CA is rotated.



To prevent system downtime, this procedure includes two BOSH redeployments. When you click **Apply Changes** for the first time, BOSH applies new certificates to PCF components alongside the old ones. The second **Apply Changes** then deletes the old certificates. Each successful redeploy verifies that the certificate rotation process is proceeding correctly.

**⚠ warning:** You must complete these steps in the exact order specified. Otherwise, you risk damaging your deployment.

## Step 1: Add a New Root CA

Follow this procedure to add a new root CA for Ops Manager. The new root CA can be a Pivotal-generated CA or your own custom CA.

To add a new root CA for Ops Manager, do the following:

1. If you haven't already, perform the steps in the [Using Ops Manager API](#) topic to target and authenticate with the Ops Manager User Account and Authentication (UAA) server. Record your Ops Manager access token, and use it for `YOUR-UAA-ACCESS-TOKEN` in the following procedures.

**💡 Note:** When you record your Ops Manager access token, remove any newline characters such as `\n`.

2. Use Ops Manager to generate a new CA, or else add your own custom CA.

**💡 Note:** Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are not supported in PCF.

- To use your own custom CA, call the Ops Manager API `generate` endpoint as follows:

```
curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities" \
-X POST \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN" \
-H "Content-Type: application/json" \
-d '{"cert_pem": "-----BEGIN CERTIFICATE-----\nYOUR-CERTIFICATE", "private_key_pem": "-----BEGIN RSA PRIVATE KEY-----\nYOUR-KEY"}'
```

Where:

- `YOUR-CERTIFICATE` is your custom CA.
- `YOUR-KEY` is your RSA key.
- `YOUR-UAA-ACCESS-TOKEN` is your UAA access token.

If the command succeeds, the API returns a response that includes the new CA certificate:

```
HTTP/1.1 200 OK
{
 "certificate_authorities": [
 {
 "guid": "f7bc18f34f2a7a9403c3",
 "issuer": "YOUR-CA",
 "created_on": "2017-01-09",
 "expires_on": "2021-01-09",
 "active": true,
 "cert_pem": "-----BEGIN CERTIFICATE-----\nMIIC+zCCAeOgAwIBAgI....etc"
 }
]
}
```

- To use a Pivotal-generated CA, call the Ops Manager API `generate` endpoint as follows:

```
$ curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities/generate" \
-X POST \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN" \
-H "Content-Type: application/json" \
-d '{}'
```

If the command succeeds, the API returns a response that includes the new CA certificate:

```

HTTP/1.1 200 OK
{
 "guid": "f7bc18f34f2a7a9403c3",
 "issuer": "Pivotal",
 "created_on": "2017-01-19",
 "expires_on": "2021-01-19",
 "active": false,
 "cert_pem": "-----BEGIN EXAMPLE CERTIFICATE-----
MIIC+zCCAeOgAwIBAgIBADANBgkqhkiG9w0BAQADFQswCQYDVQQGEwJVUzEQ
EXAMPLEoCgwHUGI2b3RhbDAeFw0xNDartheyMTQyMjVhFw0yMTAxMTkyMTQyMjVh
EXAMPLEoBgNVBAYTAIVTMRAwDgYDVVaderdQaXZvdGFsMIIBIjANBgkqhkiG9w0B
EXAMPLEoAQA8AMIIBBgKCAQEAyV4OhPIIZTEym9OcdNvip9Ev0ijPPLo9WPLUMzT
EXAMPLEo/TgD+DP09mwVXiQwBlJmoj9DqRED1x/6bc0Ki/BAFo/P4MmOKm3QnDCt
EXAMPLEFooggA++2HYrNTKWJ5fsXmERs8IK9AXXT7RKXhkyWWU3oNGf7zo0e3YKp
EXAMPLEeh1NwIbNcGT1AurlDsxY0ZY1HVzBLTisMyDogJmSLcSOW3qUDQjatjXKw
EXAMPLEEojG3nv2hvd4/tOtiHuKM3+AGbnaS2MdlOvFoh/7Y79tUp89csK0sg6Ou
EXAMPLEEohe4DcKw5CzUtIhKNXgHyeoVOBPcVQTp4Ijp1iQIDAQABo0IwQDADBgNV
EXAMPLEEoyH4y7VeuImLStXM0CKR8uVqxX/gwDwYDVROTAQH/BAUwAwEB/zAOBgNV
EXAMPLEoEoBKAQYwDQYJKoZIhvcNAQELBQADggEBALmHOPxdyBGnuR0HgR9V4Tww
EXAMPLEoGALMKV77am5z6G2Oq5cwACFWAFftrPG4W9Jm577QtewiY/Rad/PbkY0YSY
EXAMPLEEokrtnjxjx10H2sr7qLBFjJ0wBZHhVmDsO6A9PkfAPu4eJvqRMuL/xGmSQ
EXAMPLEoCyNmnZ7FgHyFbd9D9X5YW8fWGSvBPPikeONdRvjw9aEeAtbGEh8eZCP
EXAMPLEEob33RuR+CTNqThXY9k8d7/7ba4KVdd4gP8ynFgwnvDQOjCJZ6Go5QY5HA
EXAMPLEoPFW8pAYevWrXKR0rE8fL5o9qgTjymO+5yyvvWYrKPqqlUlvMcdNr84=
-----END EXAMPLE CERTIFICATE-----
"

```

3. Confirm that your new CA has been added by listing all of the root CAs for Ops Manager:

```
$ curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities" \
-X GET \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

The API call returns something like the following:

```
HTTP/1.1 200 OK
{
 "certificate_authorities": [
 {
 "guid": "f7bc18f34f2a7a9403c3",
 "issuer": "Pivotal",
 "created_on": "2017-01-09",
 "expires_on": "2021-01-09",
 "active": true,
 "cert_pem": "-----BEGIN CERTIFICATE-----\nMIIC+zCCAeOgAwIBAgI...etc"
 }
 {
 "guid": "a8ee01e33e3e33303e3",
 "issuer": "Pivotal",
 "created_on": "2017-04-09",
 "expires_on": "2021-04-09",
 "active": false,
 "cert_pem": "-----BEGIN CERTIFICATE-----\nzBBBC+eAAe1gAwAAeZ....etc"
 }
]
}
```

Identify your newly added CA, which has `active` set to `false`. Record its GUID.

4. Navigate to `https://OPS-MAN-QDN` in a browser and log in to Ops Manager.
5. Click the **BOSH Director** tile in the **Installation Dashboard**.
6. Select the **Director Config** pane.
7. Select **Recreate All VMs**. This propagates the new CA to all VMs to prevent downtime.
8. Go back to the Installation Dashboard. For each service tile you have installed, do the following:
  - a. Click the tile.
  - b. Click the **Errands** tab.
  - c. Enable the **Recreate All Service Instances** errand if provided. If you do not see this errand, contact [Pivotal Support](#).
9. Click **Review Pending Changes**, then **Apply Changes**. When the deploy finishes, continue to the next section.

## Step 2: Activate the New CA

To activate the new CA, do the following:

1. Use `curl` to make an Ops Manager API call that activates the new CA, replacing `CERT-GUID` with the GUID of your CA that you retrieved in the previous section:

```
$ curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities/CERT-GUID/activate" \
-X POST \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN" \
-H "Content-Type: application/json" \
-d '{}'
```

The API returns a successful response:

```
HTTP/1.1 200 OK
```

2. List your root CAs again to confirm that the new CA is active:

```
$ curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities" \
-X GET \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

Examine the response to ensure that your new CA has `active` set to `true`.

## Step 3 (Optional): Rotate Configurable Certificates

If you have configurable certificates expiring soon, complete the [Rotate Configurable Certificates](#) procedure, so that your next deploy includes both new configurable certificates and new non-configurable certificates. You can also rotate your configurable certificates later and perform an additional deploy.

## Step 4: Rotate Non-Configurable Certificates from the New Root

To rotate non-configurable certificates from the new root CA, do the following:

1. Use `curl` to make an API call to regenerate all non-configurable certificates and apply the new CA to your existing BOSH Director:

```
curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities/active/regenerate" \
-X POST \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN" \
-H "Content-Type: application/json" \
-d '{}'
```

The API returns a successful response:

```
HTTP/1.1 200 OK
```

2. Click the **BOSH Director** tile in the **Installation Dashboard**.
3. Select the **Director Config** pane.
4. Select **Recreate All VMs**. This propagates the new CA to all VMs to prevent downtime.
5. Go back to the Installation Dashboard. For each service tile you have installed, do the following:
  - a. Click the tile.
  - b. Click the **Errands** tab.
  - c. Enable the **Recreate All Service Instances** errand if provided. If you do not see this errand, contact [Pivotal Support](#).
6. Navigate to Ops Manager, click **Review Pending Changes**, and click **Apply Changes** to perform a second redeploy.

## Step 5: (Optional) Delete the Old CA

**⚠ warning:** Be sure to include the **Review Pending Changes** and **Apply Changes** from [Step 4: Rotate Non-Configurable certificates from the New Root](#) before you proceed to deleting the old CA.

If you want to delete the old CA, do the following:

1. List your root CAs to retrieve the GUID of your old, inactive CA:

```
$ curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities" \
-X GET \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

2. Use `curl` to make an API call to delete your old CA, replacing `OLD-CERT-GUID` with the GUID of your old, inactive CA:

```
$ curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities/OLD-CERT-GUID" \
-X DELETE \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN"
```

The API returns a successful response.

```
HTTP/1.1 200 OK
```

3. Navigate to Ops Manager, click **Review Pending Changes**, and click **Apply Changes**.

## Rotate Non-Configurable Certificates

This procedure regenerates non-configurable leaf certificates visible to the Ops Manager API, whether they are managed and stored by Ops Manager directly, or by CredHub at Ops Manager request.

Run by itself, this procedure does not rotate or otherwise affect the Ops Manager root CA.

To rotate non-configurable certificates, do the following:

1. Use `curl` to make an API call to regenerate all non-configurable certificates and apply the new CA to your existing BOSH Director:

```
$ curl "https://OPS-MAN-FQDN/api/v0/certificate_authorities/active/regenerate" \
-X POST \
-H "Authorization: Bearer YOUR-UAA-ACCESS-TOKEN" \
-H "Content-Type: application/json" \
-d '{}'
```

The API returns a successful response:

```
HTTP/1.1 200 OK
```

2. Navigate to Ops Manager, click **Review Pending Changes**, and click **Apply Changes** to perform a second redeploy.

## Rotate Configurable Certificates

Configurable certificates are generated by the user and pasted into Ops Manager configuration panes where needed. Examples include certificates that terminate SSL traffic into PAS, or authenticate a Single Sign-On (SSO) service plan to an external SAML server.

For specific instructions on how to rotate SAML certificates for both PAS and the SSO service, see [Identity Provider SAML Certificates](#). These certificates expire every two years, and every IdP has its own certificate that may require its own rotation cadence.

For Ops Manager, PAS, and other runtimes, Pivotal recommends only rotating configurable certificates within the more inclusive [Rotate Root and Leaf Certificates](#) procedure. But if you are sure that only your configurable certificates need rotation, and no others, you can run this procedure by itself and click **Apply Changes** at the end.

To rotate configurable certificates, do the following:

1. If you haven't already, use the Ops Manager API `deployed/certificates` endpoint to retrieve information about your expiring configurable certificates, as described in the procedures [Check Leaf Certificate Expiration Dates](#) and [Identify Non-Configurable, Configurable, and Unrotatable Leaf Certificates](#). The information for each configurable certificate looks like this:

```
{
 "configurable": true,
 "property_reference": ".properties.networking_poe_ssl_certs[0].certificate",
 "property_type": "rsa_cert_credentials",
 "product_guid": "cf-36066831c119c39736d3",
 ...
 "valid_until": "2019-01-25T22:07:58Z"
},
```

2. For each configurable certificate that expires soon:

a. Find the text field the certificate is configured within the Ops Manager interface.

- The `product_guid` field in the API output can help identify which tile the certificate is configured in. For example, the prefix `p-bosh-` refers to the BOSH Director tile, and the prefix `cf-` refers to the PAS tile.
- The `property_reference` field in the API output can often help identify which **Settings** pane the certificate is configured in. For example, the `uaa.service_provider_key_credentials` property is configured in the PAS tile > **UAA** pane.
- You might have to look through multiple configuration panes to identify where a certificate is configured.

b. Paste a new value for the certificate into the field

c. Click **Save** at the bottom of each pane in which you have provided new certificates.

3. If you are rotating configurable certificates within the [Rotate Root and Leaf Certificates](#) procedure, continue to the next step. Otherwise, if you are rotating configurable certificates only, return to the **Installation Dashboard**, click **Review Pending Changes**, and click **Apply Changes**.

## Identity Provider SAML Certificates

SAML service provider credentials are one example of configurable certificates in PCF. When PAS is configured to use SAML as an identity provider, it uses a configurable CA certificate to authenticate to an external SAML server, by generating ephemeral certificates that PAS includes in its outbound request message headers. This CA has a two-year expiration period.

In addition, the [SSO](#) service shares the use of PAS SAML certificates for every SAML external Identity Provider (IdP) integration, such as trust, partnership, or Federation. You must rotate these in lockstep with PAS.

The [Rotate Your SAML CA for SSO](#) procedure below provides an example of how to rotate certificates for each IdP, including temporarily disabling certificate validation on the IdP side during the rotation.

The Knowledge Base article [PCF Advisory - SAML Service Provider Credential Certificates Expire after 2 Years](#) provides more information about rotating SAML certificates.

## Rotate Your SAML CA for PAS and the SSO Service

SAML service provider credentials are only required for your PAS deployment if all of these conditions are met:

- You are using SSO in production for login to PAS or using the SSO service for login to apps.
- You are using SAML identity providers for PAS or SSO service plans.
- You had Ops Manager generate a certificate for you by clicking the **Generate RSA Certificate** button.
- You are validating the signature of SAML authentication request with your identity provider.

To regenerate and rotate SAML service provider certificates without disrupting PAS or your apps using the SSO service, do the following:

1. Disable certificate validation in your identity provider.
2. For PAS, follow the procedure in the table below that corresponds to your use case. This includes downloading and importing a new certificate and updated SAML metadata in your identity provider.

| Solution Name                                        | Procedure                                                        |
|------------------------------------------------------|------------------------------------------------------------------|
| <a href="#">CA Single Sign-On aka CA SiteMinder</a>  | <a href="#">Configuring CA as an Identity Provider</a>           |
| <a href="#">Ping Federate</a>                        | <a href="#">Configuring PingFederate as an Identity Provider</a> |
| <a href="#">Active Directory Federation Services</a> | <a href="#">Configuring ADFS as an Identity Provider</a>         |

3. For the SSO service, follow the procedure in the table below that corresponds to your use case. This includes downloading the SAML Service Provider metadata for each SAML identity provider integration, such as trust, partnership, or Federation, and importing the updated SAML Service Provider metadata in your identity provider.

| Solution Name            | Procedure                                                      |
|--------------------------|----------------------------------------------------------------|
| ADFS                     | <a href="#">Configuring a Single Sign-On Service Provider</a>  |
| CA SSO                   | <a href="#">Configuring a Single Sign-On Service Provider</a>  |
| Okta                     | <a href="#">Configure Okta as an Identity Provider</a>         |
| PingFederate             | <a href="#">Configure PingFederate as an Identity Provider</a> |
| Additional Documentation | <a href="#">Integration Guides</a>                             |

4. Re-enable certificate validation in your identity provider.

## Trusted System Certificates

Page last updated:

A Cloud Foundry Administrator can deploy a set of trusted system certificates. These trusted certificates are available in Linux-based application instances running on the Diego backend. Such instances include buildpack-based apps using the cflinuxfs2 stack and Docker-image-based apps.

If the administrator configures these certificates, they are available inside the instance containers as files with extension `.cert` in the read-only `/etc/cf-system-certificates` directory.

For cflinuxfs2-based apps, these certificates are also installed directly in the `/etc/ssl/certs` directory, and are available automatically to libraries such as `openssl` that respect that trust store. If the administrator configure these certificates, the location of the certificates is provided in the environment variable `CF_SYSTEM_CERT_PATH` on the instance container.

## Disk Encryption

This topic describes how to secure Pivotal Cloud Foundry (PCF) VMs by encrypting their disks or rotating their disk encryption keys.

### Introduction

Disk encryption protects data integrity if computing resources are stolen physically.

Disk encryption for VMs works at the IaaS level. An IaaS encrypts disks when it first creates them, or re-encrypts them when it rotates encryption keys. To encrypt disks in PCF, you must:

1. Configure the IaaS to encrypt disks when it creates or re-creates them.
2. Trigger BOSH to re-create the existing VMs that use the disks, and create encrypted disks from now on for new VMs.

The procedures below detail how to do this for each IaaS.

### Disks You Can Encrypt on a PCF VM

- The root file system for the VM. For BOSH-created VMs, this comes from the stemcell.
- Ephemeral disk for the VM.
- Persistent disk for the VM.

### Which VMs Each Procedure Encrypts

For each IaaS, there are two disk encryption procedures, which encrypt different VMs:

- The **BOSH Director** procedure encrypts the disks used by the BOSH Director VM when you first create a PCF environment.
- The **BOSH-Deployed VM** procedure encrypts disks for the VMs that the BOSH Director creates, after BOSH has been deployed.

## Encrypt Disks or Rotate Keys

You can use the same procedure to either encrypt disks for the first time or rotate encryption keys.

For BOSH-deployed VMs, some IaaSes let you associate a policy with the BOSH process that automatically encrypts all disks BOSH creates. On AWS, BOSH must explicitly tell the IaaS to encrypt each disk that it creates, and passes in an encryption key. The following table summarizes these differences:

| IaaS                          | How configured                                             | How encrypted                                         | User can supply key | BOSH stores key ID |
|-------------------------------|------------------------------------------------------------|-------------------------------------------------------|---------------------|--------------------|
| AWS                           | User pastes key ARN (ID) into Ops Manager                  | BOSH tells IaaS to encrypt disks it creates           | Yes                 | Yes                |
| Azure (with Managed Disks)    | User configures IaaS to associate encrypt policy with BOSH | IaaS automatically encrypts disks it creates for BOSH | No                  | No                 |
| Azure (with Storage Accounts) | User configures IaaS to associate encrypt policy with BOSH | IaaS automatically encrypts disks it creates for BOSH | Yes                 | No                 |
| vSphere                       | User configures IaaS to associate encrypt policy with BOSH | IaaS automatically encrypts disks it creates for BOSH | Yes                 | No                 |

### Azure

Azure provides virtual disk space through [Azure Storage](#) accounts. In some regions, Azure offers a [Managed Disks](#) service for storage accounts, which allocates disk space flexibly on demand.



## Managed Disks vs Unmanaged Storage Accounts

For disk encryption, Pivotal recommends Managed Disks storage where available. With Managed Disks, encryption keys are managed by the IaaS, so you need not (and cannot) supply your own keys. You also do not need to re-create VMs after encrypting disks or rotating encryption keys, because the IaaS propagates the change to all VMs automatically.

## Encrypt Azure Disks

Follow the steps below to initiate or rotate disk encryption for BOSH-deployed VMs on Azure:

1. Log in to Azure Portal and follow the [Encryption workflow](#) to encrypt new and existing PCF VMs.
2. For unmanaged Storage Account disks, follow the [Recreate BOSH-Deployed Disks](#) procedure below to propagate the change to existing VMs.
  - With Managed Disks, you can skip this step.

For more information about how BOSH integrates with IaaS-level disk encryption on Azure, see [Encryption](#) under *Microsoft Azure* in the BOSH documentation.

## vSphere v6.5 or Later

vSphere supports disk encryption in versions 6.5 and later for encrypted VMs. Follow the steps below to initiate or rotate disk encryption for BOSH-deployed VMs on vSphere v6.5+:

1. Log in to vCenter and follow the [Encrypt an Existing Virtual Machine or Virtual Disk](#) procedure in the *VMware Docs*.
2. Follow the [Recreate BOSH-Deployed Disks](#) procedure below to propagate the change to existing VMs.

For more information about how BOSH integrates with IaaS-level disk encryption on vSphere, see [Encryption](#) under *vSphere* in the BOSH documentation.

## AWS (Ops Manager v2.0 and later)

On AWS, you can use your Amazon account key to encrypt Linux EBS volumes, or supply your own key.

For instructions on how to encrypt BOSH-deployed VMs and the Ops Manager VM on AWS, see [Configuring Amazon EBS Encryption](#).

For more information about how BOSH integrates with IaaS-level disk encryption on AWS, see [Encryption](#) under *Amazon Web Services* in the BOSH documentation.

## Recreate BOSH-Deployed Disks

Unless you are using Azure Managed Disks, you need to manually recreate disks on BOSH-deployed VMs after you have added or rotated disk encryption keys. To manually recreate disks, do the following:

1. Configure Ops Manager to encrypt VM root, ephemeral disk, and persistent disk on next deploy:
  - **Root File System:** To recreate the root file system for VMs, you must upload a new stemcell. If you are already running the latest stemcell, you can:
    - Wait until a new stemcell comes out, typically less than two weeks.
    - Call [Pivotal Support](#) if propagating disk encryption is urgent.
  - **Ephemeral Disks:** In the **Director Config** pane of the Ops Manager tile, enable the **Recreate All VMs** checkbox.
  - **Persistent Disks**
    - PCF v2.3 and later: In the **Director Config** pane of the Ops Manager tile, enable the **Recreate All Persistent Disks** checkbox.
    - PCF v2.2 and earlier: In the **Resource Config** pane of all tiles, change the disk or VM sizes of all VMs that you need to encrypt.
2. Click **Review Pending Changes** and **Apply Changes**.



## Security Event Logging

Page last updated:

This topic describes how to enable and interpret security event logging for the Cloud Controller, the User Account and Authentication (UAA) server, and CredHub. Operators can use these logs to retrieve information about a subset of requests to the Cloud Controller, UAA server, and CredHub for security or compliance purposes.

## Cloud Controller Logging

The Cloud Controller logs security events to syslog. You must configure a syslog drain to forward your system logs to a log management service.

See the [Configuring System Logging in PAS](#) topic for more information.

## Format for Log Entries

Cloud Controller logs security events in the [Common Event Format](#) (CEF). CEF specifies the following format for log entries:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

Entries in the Cloud Controller log use the following format:

```
CEF:CEF_VERSION|cloud_foundry|cloud_controller_ng|CC_API_VERSION|
SIGNATURE_ID|NAME|SEVERITY|rt=TIMESTAMP suser=USERNAME suid=USER_GUID
cs1Label=userAuthenticationMechanism cs1=AUTH_MECHANISM
cs2Label=vcapRequestId cs2=VCAP_REQUEST_ID request=REQUEST
requestMethod=REQUEST_METHOD cs3Label=result cs3=RESULT
cs4Label=httpStatusCode cs4=HTTP_STATUS_CODE src=SOURCE_ADDRESS
dst=DESTINATION_ADDRESS cs5Label=xForwardedFor cs5=X_FORWARDED_FOR_HEADER
```

Refer to the following list for a description of the properties shown in the Cloud Controller log format:

- `CEF_VERSION`: The version of CEF used in the logs.
- `CC_API_VERSION`: The current Cloud Controller API version.
- `SIGNATURE_ID`: The method and path of the request. For example, `GET /v2/app:GUID`.
- `NAME`: The same as `SIGNATURE_ID`.
- `SEVERITY`: An integer that reflects the importance of the event.
- `TIMESTAMP`: The number of milliseconds since the Unix epoch.
- `USERNAME`: The name of the user who originated the request.
- `USER_GUID`: The GUID of the user who originated the request.
- `AUTH_MECHANISM`: The user authentication mechanism. This can be `oauth-access-token`, `basic-auth`, or `no-auth`.
- `VCAP_REQUEST_ID`: The VCAP request ID of the request.
- `REQUEST`: The request path and parameters. For example, `/v2/info?MY-PARAM=VALUE`.
- `REQUEST_METHOD`: The method of the request. For example, `GET`.
- `RESULT`: The meaning of the HTTP status code of the response. For example, `success`.
- `HTTP_STATUS_CODE`: The HTTP status code of the response. For example, `200`.
- `SOURCE_ADDRESS`: The IP address of the client who originated the request.
- `DESTINATION_ADDRESS`: The IP address of the Cloud Controller VM.
- `X_FORWARDED_FOR_HEADER`: The contents of the X-Forwarded-For header of the request. This is empty if the header is not present.

## Example Log Entries

The following list provides several example requests with the corresponding Cloud Controller log entries.

- An anonymous `GET` request:

```
CEF:0|cloud_foundry|cloud_controller_ng|2.54.0|GET /v2/info|GET
/v2/info|0|rt=1460690037402 suser= suid= request=/v2/info
requestMethod=GET src=127.0.0.1 dst=192.0.2.1
cs1Label=userAuthenticationMechanism cs1=no-auth cs2Label=vcapRequestId
cs2=c4bac383-7cc9-4d9f-b1c0-1iq8c0baa000 cs3Label=result cs3=success
cs4Label=httpStatusCode cs4=200 cs5Label=xForwardedFor
cs5=198.51.100.1
```

- A `GET` request with basic authentication:

```
CEF:0|cloud_foundry|cloud_controller_ng|2.54.0|GET /v2/syslog_drain_urls|GET
/v2/syslog_drain_urls|0|rt=1460690165743 suser=bulk_api suid=
request=/v2/syslog_drain_urls?batch_size=1000 requestMethod=GET
src=127.0.0.1 dst=192.0.2.1 cs1Label=userAuthenticationMechanism
cs1=basic-auth cs2Label=vcapRequestId cs2=79187189-e810-33dd-6911-b5d015bbc999
::eat1234d-4004-4622-ad11-9iaai88e3ae9 cs3Label=result cs3=success
cs4Label=httpStatusCode cs4=200 cs5Label=xForwardedFor cs5=198.51.100.1
```

- A `GET` request with OAuth access token authentication:

```
CEF:0|cloud_foundry|cloud_controller_ng|2.54.0|GET /v2/routes|GET
/v2/routes|0|rt=1460689904925 suser=admin suid=c7ca208f-8a9e-4aab-
92f5-28795f86d62a request=/v2/routes?inline-relations-depth=1&q=
host%3Adora%3Bdomain_guid%3B777-1o9f-5f5n-i888-o2025cb2dfc3
requestMethod=GET src=127.0.0.1 dst=192.0.2.1
cs1Label=userAuthenticationMechanism cs1=oauth-access-token
cs2Label=vcapRequestId cs2=79187189-990i-8930-52b2-9090b2c5poz0
::5a265621-b223-4520-afae-ab7d0ee7c75b cs3Label=result cs3=success
cs4Label=httpStatusCode cs4=200 cs5Label=xForwardedFor cs5=198.51.100.1
```

- A `GET` request that results in a 404 error:

```
CEF:0|cloud_foundry|cloud_controller_ng|2.54.0|GET /v2/apps/7f310103-
39aa-4a8c-b92a-9ff8a6a2fa6b|GET /v2/apps/7f310103-39aa-4a8c-b92a-
9ff8a6a2fa6b|0|rt=1460691002394 suser=bob suid=a00i2026-55io-3983-
555o-40e611410aec request=/v2/apps/7f310103-39aa-4a8c-b92a-9ff8a6a2fa6b
requestMethod=GET src=127.0.0.1 dst=192.0.2.1
cs1Label=userAuthenticationMechanism cs1=oauth-access-token cs2Label=vcapRequestId
cs2=49f21579-9eb5-4bdf-6e49-e77d2de647a2::9f8841e6-e04a-498b-b3ff-d59cfe7cb7ea
cs3Label=result cs3=clientError cs4Label=httpStatusCode cs4=404
cs5Label=xForwardedFor cs5=198.51.100.1
```

- A `POST` request that results in a 403 error:

```
CEF:0|cloud_foundry|cloud_controller_ng|2.54.0|POST /v2/apps|POST
/v2/apps|0|rt=1460691405564 suser=bob suid=4f9a33f9-fb13-4774-a708-
f60c939625cd request=/v2/apps?async=true requestMethod=POST
src=127.0.0.1 dst=192.0.2.1 cs1Label=userAuthenticationMechanism
cs1=oauth-access-token cs2Label=vcapRequestId cs2=booc03111-9999-4003-88ab-
20i9r33333ou::5a4993fc-722f-48bc-aff4-99b2005i9bb5 cs3Label=result
cs3=clientError cs4Label=httpStatusCode cs4=403 cs5Label=xForwardedFor
cs5=198.51.100.1
```

## UAA Logging

UAA logs security events to a file located at `/var/vcap/sys/log/uaa/uaa.log` on the UAA virtual machine (VM). Because these logs are automatically rotated, you must configure a syslog drain to forward your system logs to a log management service.

See the [Configuring System Logging in PAS](#) topic for more information.

## Log Events

UAA logs identify the following categories of events:

- Authorization and Password Events
- SCIM Administration Events

- Token Events
- Client Administration Events
- UAA Administration Events

To learn more about the names of the events included in these categories and the information they record in the UAA logs, see [User Account and Authentication Service Audit Requirements](#).

## Example Log Entries

The following sections provide several example requests with the corresponding UAA log entries.

### Successful User Authentication

```
Audit: TokenIssuedEvent ("["openid", "scim.read", "uaa.user",
"cloud_controller.read", "password.write", "cloud_controller.write",
"scim.write"]"): principal=a42026d6-5533-1884-ef2-838abcd0i3e3,
origin=[client=cf, user=bob], identityZoneId=[uaa]
```

- This entry records a `TokenIssuedEvent`.
- UAA issued a token associated with the scopes `"openid", "scim.read", "uaa.user", "cloud_controller.read", "password.write", "cloud_controller.write", "scim.write"` to the user `bob`.

### Failed User Authentication

```
Audit: UserAuthenticationFailure ('bob@example.com'):
principal=61965469-c821-46b7-825f-630e12a51d6c,
origin=[remoteAddress=198.51.100.1, clientId=cf],
identityZoneId=[uaa]
```

- This entry records a `UserAuthenticationFailure`.
- The user `bob@example.com` originating at `198.51.100.1` failed to authenticate.

### Successful User Creation

```
Audit: UserCreatedEvent ("["user_id=61965469-c821-
46b7-825f-630e12a51d6c", "username=bob@example.com"]"):
principal=91220262-d901-44c0-825f-633i33b55d6c,
origin=[client=cf, user=admin, details=(198.51.100.1,
tokenType=bearertokenValue=<TOKEN>,
sub=20i03423-dd8e-33e1-938d-e9999e30f500,
iss=https://uaa.example.com/oauth/token)], identityZoneId=[uaa]
```

- This entry records a `UserCreatedEvent`.
- The `admin` user originating at `198.51.100.1` created a user named `bob@example.com`.

### Successful User Deletion

```
Audit: UserDeletedEvent ("["user_id=61965469-c821-
46b7-825f-630e12a51d6c", "username=bob@example.com"]"):
principal=61965469-c821-46b7-825f-630e12a51d6c,
origin=[client=admin, details=(remoteAddress=198.51.100.1,
tokenType=bearertokenValue=<TOKEN>,
sub=admin, iss=https://uaa.example.com/oauth/token)], identityZoneId=[uaa]
```

- This entry records a `UserDeletedEvent`.
- The `admin` user originating at `198.51.100.1` deleted a user named `bob@example.com`.

## CredHub Logging

CredHub logs security events to a file located at `/var/vcap/sys/log/credhub/credhub_security_events.log` on the CredHub VM. Because these logs are automatically rotated, you must configure a syslog drain to forward your system logs to a log management service.

See the [Configuring System Logging in PAS](#) topic for more information.

## Format for Log Entries

CredHub logs security events in the [Common Event Format](#) (CEF). CEF specifies the following format for log entries:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```


Entries in the CredHub log use the following format:

```
CEF:0|cloud_foundry|credhub|CREDHUB_SERVER_VERSION|
SIGNATURE_ID|NAME|0|rt=TIMESTAMP suser=USERNAME suid=USER_GUID
cs1Label=userAuthenticationMechanism cs1=AUTH_MECHANISM
request=REQUEST requestMethod=REQUEST_METHOD
cs3Label=versionUuid cs3=VERSION_UUID
cs4Label=httpStatusCode cs4=HTTP_STATUS_CODE src=SOURCE_ADDRESS dst=DESTINATION_ADDRESS
cs2Label=resourceName cs2=RESOURCE_NAME
cs5Label=resourceUuid cs5=RESOURCE_UUID deviceAction=OPERATION
cs6Label=requestDetails cs6=REQUEST_DETAILS
```

Refer to the following list for a description of the properties shown in the CredHub log.

- `CEF_VERSION` : The version of CEF used in the logs.
- `CREDHUB_SERVER_VERSION` : The current CredHub server version.
- `SIGNATURE_ID` : The method and path of the request. For example, `GET /v2/app:GUID`.
- `NAME` : The same as `SIGNATURE_ID`.
- `TIMESTAMP` : The number of milliseconds since the Unix epoch.
- `USERNAME` : The name of the user who originated the request, as defined by UAA. In the case of mTLS, no-auth, or not defined, this value is empty.
- `USER_GUID` : The “actor” identifier. For example, `mtls-app:GUID`. If there is no authenticated user, this value is empty.
- `AUTH_MECHANISM (cs1)` : The user authentication mechanism. This can be `oauth-access-token`, `mtls-auth`, or `no-auth`.
- `REQUEST` : The request path and parameters. For example, `/v2/info?MY-PARAM=VALUE`.
- `REQUEST_METHOD` : The method of the request. For example, `GET`.
- `HTTP_STATUS_CODE (cs4)` : The HTTP status code of the response. For example, `200`.
- `SOURCE_ADDRESS` : The IP address of the client who originated the request.
- `DESTINATION_ADDRESS` : The IP address of the CredHub VM.
- `RESOURCE_NAME (cs2)` : The credential path name. For example, `/my/awesome/credential`.
- `RESOURCE_UUID (cs5)` : The top-level credential UUID. This is not the credential version.
- `VERSION_UUID (cs3)` : The credential version UUID.
- `OPERATION (deviceAction)` : The device action. The possible operations include the following:
  - `get`
  - `set`
  - `generate`
  - `regenerate`
  - `bulk-regenerate`
  - `delete`
  - `find`
  - `get-permissions`
  - `add-permission`
  - `delete-permission`
  - `interpolate`
  - `info`
  - `version`

- o `health`
  - o `key-usage`
  - o `update-transitional-version`
- `REQUEST_DETAILS (cs6)` : A JSON blob that differs per request.

 **Note:** The CredHub logs include descriptions for each custom label. For example, the logs include `cs2Label=resourceName` to define the `cs2` label. The value for `resourceName` appears in the log next to `cs2=/path/to/credential`.

## Example Log Entries

The following sections provide several example requests with the corresponding CredHub log entries.

### Accessing a Credential

```
CEF:0|cloud_foundry|credhub|2.0.0-beta.28|GET /api/v1/data|
GET /api/v1/data|0|rt=1530901816757
suser=app:3c538393-d192-4e23-8c83-456654b3fa6c
suid=mtls-app:3c538393-d192-4e23-8c83-456654b3fa6c
cs1Label=userAuthenticationMechanism
cs1=mutual_tls request=/api/v1/data?path=0b353167-0d5a-48c7-5036-7eaa
requestMethod=GET
cs3Label=versionUuid cs3=null
cs4Label=httpStatusCode cs4=200 src=10.0.0.1 dst=credhub.service.cf.internal
cs2Label=resourceName cs2=null
cs5Label=resourceUuid cs5=null deviceAction=FIND
cs6Label=requestDetails
cs6={"nameLike":null,"path":"0b353167-0d5a-48c7-5036-7eaa","paths":null}
```

- A user authenticated to the CredHub instance using `mutual_tls` from `10.0.0.1`.
- The authenticated user accessed a CredHub credential.

### Setting a Credential

```
CEF:0|cloud_foundry|credhub|2.0.0-beta.28|PUT /api/v1/data|
PUT /api/v1/data|0|rt=1530901097921
suser=cc_service_key_client suid=uua-client:cc_service_key_client
cs1Label=userAuthenticationMechanism
cs1=uua request=/api/v1/data requestMethod=PUT
cs3Label=versionUuid cs3=32b3d5bf-463a-4045-a6b5-65c97c61059a
cs4Label=httpStatusCode cs4=200 src=10.0.0.1 dst=credhub.service.cf.internal
cs2Label=resourceName cs2=/1530901097842989110
cs5Label=resourceUuid cs5=ccda25c5-a40a-4512-b6f5-a42f8c3b5c4c deviceAction=SET
cs6Label=requestDetails
cs6={"name":"/1530901097842989110","type":"json","mode":null,
"additionalPermissions":[{"actor":"uua-client:cc_service_key_client",
"allowedOperations":["READ","WRITE","DELETE","WRITE_ACL","READ_ACL"]}]}
```

- A user authenticated to the CredHub instance with UAA from `10.0.0.1`.
- The authenticated user set a CredHub credential.

### Generating a Credential

```
CEF:0|cloud_foundry|credhub|2.0.0-beta.28|POST /api/v1/data|
POST /api/v1/data|0|rt=1530901403532
suser=app:3c538393-d192-4e23-8c83-456654b3fa6c
suid=mtls-app:3c538393-d192-4e23-8c83-456654b3fa6c
cs1Label=userAuthenticationMechanism
cs1=mutual_tls request=/api/v1/data requestMethod=POST
cs3Label=versionUuid cs3=8c21b7b3-d4bf-4d8a-a0c5-64e8c207cb40
cs4Label=httpStatusCode cs4=200 src=10.0.0.1 dst=credhub.service.cf.internal
cs2Label=resourceName cs2=/0b353167-0d5a-48c7-5036-7eaa/2
cs5Label=resourceUuid cs5=1d55eff3-5264-434c-a127-0810f341cb2b deviceAction=GENERATE
cs6Label=requestDetails cs6={"name":"/my/awesome/credential","type":"password",
"mode":null,"additionalPermissions":[{"actor":"mtls-app:3c538393-d192-4e23-8c83-456654b3fa6c",
"allowedOperations":["READ","WRITE","DELETE","WRITE_ACL","READ_ACL"]}]}
```

- A user authenticated to the CredHub instance using `mutual_tls` from `10.0.0.1`.
- The authenticated user generated a password credential named `/my/awesome/credential`.



## Network Security

This section introduces some of the networking and routing security options for your Pivotal Cloud Foundry (PCF) deployment.

### Securing Traffic and Controlling Routes

You can enable and configure a number of customization options to secure traffic in and out of your PCF deployment.

- [TLS Connections in PCF](#)
- [Securing Traffic into Cloud Foundry](#)
- [Providing a Certificate for Your SSL/TLS Termination Point](#)
- [Enabling TCP Routing](#)

### Using the IPsec Add-On

The IPsec add-on for PCF provides additional security to the network layer for each BOSH-deployed virtual machine (VM).

The PCF IPsec add-on secures network traffic within a Cloud Foundry deployment and provides internal system protection if a malicious actor breaches your firewall.

- [Securing Data in Transit with the IPsec Add-on](#) [↗](#)
- [Rotating IPsec Credentials](#) [↗](#)
- [Installing the Pivotal Cloud Foundry IPsec Add-On](#) [↗](#)

### Network Communication Paths in PCF


- [BOSH DNS Network Communications](#)
- [Cloud Controller Network Communications](#)
- [Consul Network Communications](#)
- [Container-to-Container Network Communications](#)
- [CredHub Network Communications](#)
- [Diego Network Communications](#)
- [JMX Bridge Network Communications](#) [↗](#)
- [Loggregator Network Communications](#)
- [MySQL Network Communications](#)
- [NATS Network Communications](#)
- [Routing Network Communications](#)
- [UAA Network Communications](#)

## BOSH DNS Network Communications

This topic describes [BOSH DNS](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### BOSH DNS Communications

The following table lists network communication paths for BOSH DNS.

 **Note:** Port 8853 is the destination port for communications between BOSH DNS health processes. You must allow TCP traffic on 8853 for all VMs running BOSH DNS.

| Source VM               | Destination VM                | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication                            |
|-------------------------|-------------------------------|------|--------------------------|--------------------|--------------------------------------------------------|
| Any VM running BOSH DNS | backup-prepare                | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | ccdb                          | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | clock_global                  | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | cloud_controller              | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | cloud_controller_worker       | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | consul_server                 | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | diego_brain                   | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | diego_cell                    | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | diego_database                | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | doppler                       | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | ha_proxy                      | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | loggregator_trafficcontroller | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | mysql_proxy*                  | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | mysql_monitor*                | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | nats                          | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | nfs_server†                   | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | router                        | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | syslog_adapter                | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | syslog_scheduler              | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | tcp_router                    | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | uaa                           | 53   | TCP and UDP              | DNS                | Unencrypted. This communication happens inside the VM. |

| DNS                     | UUID                          | Port | TCP and UDP | DNS   | inside the VM.                                         |
|-------------------------|-------------------------------|------|-------------|-------|--------------------------------------------------------|
| Any VM running BOSH DNS | uaadb                         | 53   | TCP and UDP | DNS   | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | Service tile VMs              | 53   | TCP and UDP | DNS   | Unencrypted. This communication happens inside the VM. |
| Any VM running BOSH DNS | backup-prepare                | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | ccdb                          | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | clock_global                  | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | cloud_controller              | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | cloud_controller_worker       | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | consul_server                 | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | diego_brain                   | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | diego_cell                    | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | diego_database                | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | doppler                       | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | ha_proxy                      | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | loggregator_trafficcontroller | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | mysql_proxy*                  | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | mysql_monitor*                | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | nats                          | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | nfs_server†                   | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | router                        | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | syslog_adapter                | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | syslog_scheduler              | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | tcp_router                    | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | uaa                           | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | uaadb                         | 8853 | TCP         | HTTPS | Mutual TLS                                             |
| Any VM running BOSH DNS | Service tile VMs              | 8853 | TCP         | HTTPS | Mutual TLS                                             |

\*Applies only to deployments where internal MySQL is selected as the database.

†Applies only to deployments where the internal NFS server is selected for file storage.



## Cloud Controller Network Communications

This topic describes [Cloud Controller](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### Inbound Communications

The following table lists network communication paths that are inbound to the Cloud Controller.

| Source VM                     | Destination VM                 | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|-------------------------------|--------------------------------|------|--------------------------|--------------------|-----------------------------|
| cloud_controller              | cloud_controller (Routing API) | 443  | TCP                      | HTTPS              | OAuth 2.0                   |
| diego_brain                   | cloud_controller               | 9023 | TCP                      | HTTPS              | Mutual TLS                  |
| diego_brain (SSH Proxy)       | cloud_controller               | 9022 | TCP                      | HTTP               | OAuth 2.0                   |
| diego_cell (Rep)              | cloud_controller               | 9023 | TCP                      | HTTPS              | Mutual TLS                  |
| diego_database (BBS)          | cloud_controller               | 9023 | TCP                      | HTTPS              | Mutual TLS                  |
| doppler (Syslog Drain Binder) | cloud_controller               | 9023 | TCP                      | HTTPS              | Mutual TLS                  |
| loggregator_trafficcontroller | cloud_controller               | 9023 | TCP                      | HTTPS              | Mutual TLS                  |
| router                        | cloud_controller               | 9022 | TCP                      | HTTP               | OAuth 2.0                   |

### Outbound Communications

The following table lists network communication paths that are outbound from the Cloud Controller.

| Source VM                          | Destination VM                             | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication        |
|------------------------------------|--------------------------------------------|------|--------------------------|--------------------|------------------------------------|
| cloud_controller                   | mysql_proxy <sup>*</sup>                   | 3306 | TCP                      | MySQL              | MySQL authentication <sup>**</sup> |
| cloud_controller                   | nfs_server or other blobstore <sup>†</sup> | 4443 | TCP                      | HTTPS              | TLS and basic authentication       |
| cloud_controller                   | uua                                        | 8443 | TCP                      | HTTPS              | OAuth 2.0 or none <sup>‡</sup>     |
| cloud_controller                   | diego_database (BBS)                       | 8889 | TCP                      | HTTPS              | Mutual TLS                         |
| cloud_controller (Route Registrar) | nats                                       | 4222 | TCP                      | NATS               | Basic authentication               |
| cloud_controller (Routing API)     | diego_database (Locket)                    | 8891 | TCP                      | HTTPS              | Mutual TLS                         |
| cloud_controller_worker            | mysql_proxy <sup>*</sup>                   | 3306 | TCP                      | MySQL              | MySQL authentication <sup>**</sup> |
| cloud_controller_worker            | nfs_server or other blobstore <sup>†</sup> | 4443 | TCP                      | HTTPS              | TLS and basic authentication       |
| clock_global                       | mysql_proxy <sup>*</sup>                   | 3306 | TCP                      | MySQL              | MySQL authentication <sup>**</sup> |

<sup>\*</sup>Applies only to deployments where internal MySQL is selected as the database.

<sup>\*\*</sup>MySQL authentication uses the MySQL native password method.

<sup>†</sup>The destination depends on your file storage or blobstore configuration.

<sup>‡</sup>The authentication method depends on the type of request.


### BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

## Consul Communications


If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## Consul Network Communications

This topic describes [Consul](#)  internal network communication paths with other Pivotal Application Service (PAS) components.

### Consul Communications

The following table lists network communication paths for Consul.

 **Note:** Port 8301 is the destination port for communications between Consul agents. You must allow both TCP and UDP traffic on port 8301 for all VMs running Consul. In addition, `consul_server` communicates with Consul VMs, including other Consul servers, on port 8300.

| Source VM             | Destination VM                | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|-----------------------|-------------------------------|------|--------------------------|--------------------|-----------------------------|
| Any VM running Consul | ccdb                          | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | clock_global                  | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | cloud_controller              | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | cloud_controller_worker       | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | consul_server                 | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | diego_brain                   | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | diego_cell                    | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | diego_database                | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | doppler                       | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | ha_proxy                      | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | loggregator_trafficcontroller | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | mysql_proxy <sup>*</sup>      | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | nats                          | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | nfs_server <sup>†</sup>       | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | router                        | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | syslog_adapter                | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | syslog_scheduler              | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | tcp_router                    | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | uaa                           | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | uaadb                         | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | Service tile VMs              | 8301 | TCP and UDP              | Gossip (Serf)      | Shared secret               |
| Any VM running Consul | consul_server                 | 8300 | TCP                      | HTTPS              | Mutual TLS from the same CA |

<sup>\*</sup>Applies only to deployments where internal MySQL is selected as the database.

<sup>†</sup>Applies only to deployments where the internal NFS server is selected for file storage.

## BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

### Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).





## Container-to-Container Networking Communications

This topic describes [Container-to-Container Networking](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### Inbound Communications

The following table lists network communication paths that are inbound to Container-to-Container Networking.

| Source VM                       | Destination VM                                | Port  | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|---------------------------------|-----------------------------------------------|-------|--------------------------|--------------------|-----------------------------|
| diego_cell (Silk CNI)           | diego_cell (Silk Daemon)                      | 23954 | TCP                      | HTTP               | None                        |
| diego_cell (Silk Daemon)        | diego_api (Silk Controller)                   | 4103  | TCP                      | HTTP               | Mutual TLS                  |
| diego_cell (VXLAN Policy Agent) | diego_database (api - Policy Server Internal) | 4003  | TCP                      | HTTP               | Mutual TLS                  |
| diego_cell (BOSH DNS Adapter)   | diego_brain (Service Discovery Controller)    | 8054  | TCP                      | HTTP               | Mutual TLS                  |

### Outbound Communications

The following table lists network communication paths that are outbound from Container-to-Container Networking.

| Source VM                                  | Destination VM                            | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|--------------------------------------------|-------------------------------------------|------|--------------------------|--------------------|-----------------------------|
| diego_database (api - Policy Server)       | uaa                                       | 8443 | TCP                      | HTTPS              | TLS                         |
| diego_database (api - Policy Server)       | cloud_controller (api - Cloud Controller) | 9022 | TCP                      | HTTP               | OAuth 2.0                   |
| diego_database (api - Policy Server)       | mysql_proxy*                              | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| diego_brain (Service Discovery Controller) | nats (NATS)                               | 4222 | TCP                      | HTTP               | Basic authentication        |
| diego_cell (BOSH DNS)                      | diego_cell (BOSH DNS Adapter)             | 8053 | TCP                      | HTTP               | None                        |
| diego_cell (VXLAN Policy Agent)            | mysql_proxy*                              | 3306 | TCP                      | MySQL              | MySQL authentication*       |

\*Applies only to deployments where internal MySQL is selected as the database.

## BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

## Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## CredHub Network Communications

This topic describes [CredHub](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### Inbound Communications

The following table lists network communication paths that are inbound to the CredHub.

| Source VM              | Destination VM | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|------------------------|----------------|------|--------------------------|--------------------|-----------------------------|
| cloud_controller (api) | credhub        | 8844 | TCP                      | HTTPS              | OAuth 2.0                   |
| diego_cell             | credhub        | 8844 | TCP                      | HTTPS              | Mutual TLS†                 |
| windows_cell           | credhub        | 8844 | TCP                      | HTTPS              | Mutual TLS†                 |
| windows2016_cell       | credhub        | 8844 | TCP                      | HTTPS              | Mutual TLS†                 |

### Outbound Communications

The following table lists network communication paths that are outbound from the CredHub.

| Source VM | Destination VM | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|-----------|----------------|------|--------------------------|--------------------|-----------------------------|
| credhub   | uaa            | 8443 | TCP                      | HTTPS              | n/a                         |
| credhub   | mysql_proxy*   | 3306 | TCP                      | MySQL              | MySQL authentication**      |

\*Applies only to deployments where internal MySQL is selected as the database.

\*\*MySQL authentication uses the MySQL native password method.

†Diego cells use the certificate pairs generated for individual containers to authenticate with CredHub on behalf of applications.

## BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

## Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## Diego Network Communications

This topic describes [Diego](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### Inbound Communications

The following table lists network communication paths that are inbound to Diego.

| Source VM                      | Destination VM          | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|--------------------------------|-------------------------|------|--------------------------|--------------------|-----------------------------|
| cloud_controller               | diego_database (BBS)    | 8889 | TCP                      | HTTPS              | Mutual TLS                  |
| cloud_controller (Routing API) | diego_database (Locket) | 8891 | TCP                      | HTTPS              | Mutual TLS                  |

### Diego Internal Communications

The following table lists network communication paths that are internal for Diego.

| Source VM                        | Destination VM                          | Port                | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|----------------------------------|-----------------------------------------|---------------------|--------------------------|--------------------|-----------------------------|
| diego_brain (Auctioneer)         | diego_cell (Rep)                        | 1801                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_brain (Auctioneer)         | diego_database (BBS)                    | 8889                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_brain (Auctioneer)         | diego_database (Locket)                 | 8891                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_brain (SSH Proxy)          | diego_database (BBS)                    | 8889                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_brain (SSH Proxy)          | diego_cell (App instances)              | Varies <sup>‡</sup> | TCP                      | SSH                | SSH                         |
| diego_brain (TPS Watcher)        | diego_database (Locket)                 | 8891                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_cell (local Route Emitter) | diego_database (BBS)                    | 8889                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_cell (Rep)                 | diego_brain (CC Uploader)               | 9091                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_cell (Rep)                 | diego_brain (File Server) <sup>‡*</sup> | 8080                | TCP                      | HTTP               | None                        |
| diego_cell (Rep)                 | diego_database (BBS)                    | 8889                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_cell (Rep)                 | diego_database (Locket)                 | 8891                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_database (BBS)             | diego_brain (Auctioneer)                | 9016                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_database (BBS)             | diego_cell (Rep)                        | 1801                | TCP                      | HTTPS              | Mutual TLS                  |
| diego_database (BBS)             | diego_database (Locket)                 | 8891                | TCP                      | HTTPS              | Mutual TLS                  |

<sup>‡\*</sup>The Diego File Server is responsible for distributing non-sensitive, static platform assets to internal platform components.

### Outbound Communications

The following table lists network communication paths that are outbound from Diego.

| Source VM                        | Destination VM                             | Port   | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|----------------------------------|--------------------------------------------|--------|--------------------------|--------------------|-----------------------------|
| diego_brain                      | cloud_controller                           | 9023   | TCP                      | HTTPS              | Mutual TLS                  |
| diego_brain (SSH Proxy)          | cloud_controller                           | 9022   | TCP                      | HTTP               | OAuth 2.0                   |
| diego_brain (SSH Proxy)          | uaa                                        | 443    | TCP                      | HTTPS              | TLS and OAuth 2.0           |
| diego_cell (local Route Emitter) | nats                                       | 4222   | TCP                      | NATS               | Basic authentication        |
| diego_cell (Rep)                 | cloud_controller                           | 9023   | TCP                      | HTTPS              | Mutual TLS                  |
| diego_cell (Rep)                 | nfs_server or other blobstore <sup>*</sup> | Varies | TCP                      | HTTP               | Signed URLs/TLS             |

|                         |                          |      |     |       |                                    |
|-------------------------|--------------------------|------|-----|-------|------------------------------------|
| diego_database (BBS)    | cloud_controller         | 9023 | TCP | HTTPS | Mutual TLS                         |
| diego_database (BBS)    | mysql_proxy <sup>†</sup> | 3306 | TCP | MySQL | MySQL authentication <sup>**</sup> |
| diego_database (Locket) | mysql_proxy <sup>†</sup> | 3306 | TCP | MySQL | MySQL authentication <sup>**</sup> |

<sup>\*</sup>The destination depends on your PAS blobstore configuration. If you use the internal blobstore, the Diego Cell communicates to the blobstore using TLS on port `4443`.

<sup>\*\*</sup>MySQL authentication uses the MySQL native password method.

<sup>†</sup>Applies only to deployments where internal MySQL is selected as the database.

<sup>‡</sup>These are the host-side ports that map to port 2222 in app instance containers and are typically within the range 61001 to 65534.

## BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

## Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## Loggregator Network Communications

This topic describes [Loggregator](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### Loggregator Communications

The following table lists network communication paths for Loggregator.

| Source VM                                         | Destination VM                 | Port           | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|---------------------------------------------------|--------------------------------|----------------|--------------------------|--------------------|-----------------------------|
| Any*                                              | loggregator_trafficcontroller  | 8081           | TCP                      | HTTP/WebSocket     | OAuth                       |
| Any VM running Metron                             | doppler <sup>†</sup>           | 8082           | TCP                      | gRPC over HTTP/2   | Mutual TLS                  |
| loggregator_trafficcontroller                     | doppler <sup>†</sup>           | 8082           | TCP                      | gRPC over HTTP/2   | Mutual TLS                  |
| loggregator_trafficcontroller                     | uaa                            | 8443           | TCP                      | HTTPS              | TLS                         |
| loggregator_trafficcontroller                     | cloud_controller               | 9023           | TCP                      | HTTPS              | Mutual TLS                  |
| loggregator_trafficcontroller (Reverse Log Proxy) | doppler                        | 8082           | TCP                      | gRPC over HTTP/2   | Mutual TLS                  |
| loggregator_trafficcontroller (Route Registrar)   | nats                           | 4222           | TCP                      | NATS               | Basic authentication        |
| loggregator_trafficcontroller (metrics_forwarder) | BOSH Director (metrics_server) | 25595 and 8443 | TCP                      | gRPC over HTTP/2   | Mutual TLS                  |

\*Any source VM can send requests to the specified destination within its subnet.

<sup>†</sup> Starting from ERT v1.11, Metron does not use the UDP protocol to communicate with Doppler. Starting in PAS v2.0, Doppler no longer uses the UDP protocol or the HTTP/WebSocket protocol.

### BOSH DNS Communications


By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

### Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## MySQL Network Communications

This topic describes MySQL internal network communication paths with other Pivotal Application Service (PAS) components.

 **Note:** These communications only apply to deployments where internal MySQL is selected as the PAS database.

### Inbound Communications

The following table lists network communication paths that are inbound to MySQL VMs.

| Source VM                       | Destination VM | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|---------------------------------|----------------|------|--------------------------|--------------------|-----------------------------|
| cloud_controller                | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| cloud_controller_worker         | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| clock_global                    | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| credhub                         | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| diego_cell (VXLAN Policy Agent) | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| diego_database (Policy Server)  | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| diego_database (BBS)            | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| diego_database (Locket)         | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |
| uaa                             | mysql_proxy    | 3306 | TCP                      | MySQL              | MySQL authentication*       |

(\*) MySQL authentication uses the MySQL native password method.

### Internal Communications

The following table lists network communication paths that are internal to MySQL VMs.

| Source VM     | Destination VM                   | Port       | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|---------------|----------------------------------|------------|--------------------------|--------------------|-----------------------------|
| mysql         | mysql (Galera)                   | 4567       | TCP                      | MySQL              | MySQL authentication*       |
| mysql_monitor | mysql (MySQL Server)             | 3306       | TCP                      | HTTP               | Basic authentication        |
| mysql_monitor | mysql_proxy (Proxy health check) | 443/8080** | TCP                      | HTTP               | Basic authentication        |
| mysql_proxy   | mysql (MySQL Server)             | 3306       | TCP                      | HTTP               | MySQL authentication*       |
| mysql_proxy   | mysql (Galera health check)      | 9200       | TCP                      | HTTP               | Basic authentication        |

(\*) MySQL authentication uses the MySQL native password method.

(\*\*) Port 443 is used if mysql\_proxy is registered with Gorouter. If not registered, mysql\_proxy uses port 8080 instead.

### Outbound Communications

The following table lists network communication paths that are outbound from MySQL.

| Source VM                     | Destination VM | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|-------------------------------|----------------|------|--------------------------|--------------------|-----------------------------|
| mysql_monitor                 | uaa            | 8443 | TCP                      | HTTPS              | OAuth                       |
| mysql_proxy (Route Registrar) | nats           | 4222 | TCP                      | NATS               | Basic authentication        |

### BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

## Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## NATS Network Communications

This topic describes [NATS](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### Publish Communications

The following table lists network communications that are published to NATS.

| Source VM                                          | Destination VM | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|----------------------------------------------------|----------------|------|--------------------------|--------------------|-----------------------------|
| cloud_controller<br>(Route Registrar)              | nats           | 4222 | TCP                      | NATS               | Basic authentication        |
| loggregator_trafficcontroller<br>(Route Registrar) | nats           | 4222 | TCP                      | NATS               | Basic authentication        |
| mysql_proxy<br>(Route Registrar)*                  | nats           | 4222 | TCP                      | NATS               | Basic authentication        |
| nfs_server<br>(Route Registrar)†                   | nats           | 4222 | TCP                      | NATS               | Basic authentication        |
| uaa<br>(Route Registrar)                           | nats           | 4222 | TCP                      | NATS               | Basic authentication        |
| diego_cell<br>(local Route Emitter)                | nats           | 4222 | TCP                      | NATS               | Basic authentication        |

\*Applies only to deployments where internal MySQL is selected as the database.

†Applies only to deployments where the internal NFS server is selected for file storage.

### Subscribe Communications

The following table lists network communications that are subscribed to NATS.

| Source VM | Destination VM | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|-----------|----------------|------|--------------------------|--------------------|-----------------------------|
| router    | nats           | 4222 | TCP                      | NATS               | Basic authentication        |

### BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

### Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).



## Routing Network Communications

This topic describes the internal network communication paths of the routing subsystem with other Pivotal Application Service (PAS) components.

### HTTP Routing

The following table lists network communication paths for HTTP routing.

| Source VM                        | Destination VM    | Port   | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|----------------------------------|-------------------|--------|--------------------------|--------------------|-----------------------------|
| diego_cell (local Route Emitter) | nats              | 4222   | TCPs                     | NATS               | Basic authentication        |
| Load balancer                    | router (Gorouter) | 80     | TCP                      | HTTP               | None                        |
| Load balancer                    | router (Gorouter) | 443    | TCP                      | HTTPS              | TLS                         |
| router (Gorouter)                | nats              | 4222   | TCP                      | NATS               | Basic authentication        |
| router (Gorouter)                | System components | Varies | TCP                      | Varies             | None                        |
| router (Gorouter)                | App containers    | Varies | TCP                      | Varies             | Optional TLS                |
| haproxy                          | router (Gorouter) | 80     | TCP                      | HTTP               | None                        |
| haproxy                          | router (Gorouter) | 443    | TCP                      | HTTPS              | TLS                         |
| Load balancer                    | haproxy           | 80     | TCP                      | HTTP               | None                        |
| Load balancer                    | haproxy           | 443    | TCP                      | HTTPS              | TLS                         |

### TCP Routing (Optional)

The following table lists network communication paths for TCP routing.

| Source VM                        | Destination VM                  | Port        | Transport Layer Protocol | App Layer Protocol | Security and Authentication |
|----------------------------------|---------------------------------|-------------|--------------------------|--------------------|-----------------------------|
| cloud_controller                 | cloud_controller (Routing API)* | 443         | TCP                      | HTTPS              | TLS and OAuth 2.0           |
| cloud_controller (Routing API)   | diego_database (Locket)         | 8891        | TCP                      | HTTPS              | Mutual TLS                  |
| cloud_controller (Routing API)   | mysql_proxy                     | 3306        | TCP                      | MySQL              | MySQL authentication**      |
| cloud_controller (Routing API)   | uaa                             | 8443        | TCP                      | HTTPS              | TLS                         |
| diego_brain (global TCP Emitter) | cloud_controller (Routing API)  | 3000        | TCP                      | HTTP               | OAuth 2.0                   |
| diego_brain (global TCP Emitter) | uaa                             | 8443        | TCP                      | HTTPS              | TLS                         |
| diego_cell (local Route Emitter) | cloud_controller (Routing API)  | 3000        | TCP                      | HTTP               | OAuth 2.0                   |
| diego_cell (local Route Emitter) | uaa                             | 8443        | TCP                      | HTTPS              | TLS                         |
| Load balancer                    | tcp_router                      | 1024-65535† | TCP                      | TCP                | None                        |
| router (Gorouter)                | cloud_controller (Routing API)  | 3000        | TCP                      | HTTP               | OAuth 2.0                   |
| router (Gorouter)                | uaa                             | 8443        | TCP                      | HTTPS              | TLS                         |
| tcp_router                       | cloud_controller (Routing API)  | 3000        | TCP                      | HTTP               | OAuth 2.0                   |
| tcp_router                       | uaa                             | 8443        | TCP                      | HTTPS              | TLS                         |

\* This communication happens through a load balancer and a Gorouter. Requests are received by Routing API on port 3000.

<sup>†</sup> You can use this port range to configure the port in the PAS tile.

<sup>\*\*</sup> MySQL authentication uses the MySQL native password method.

## BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

## Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## UAA Network Communications

This topic describes [User Account and Authentication \(UAA\)](#) internal network communication paths with other Pivotal Application Service (PAS) components.

### Inbound Communications

The following table lists network communication paths that are inbound to UAA.

| Source VM                     | Destination VM | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication    |
|-------------------------------|----------------|------|--------------------------|--------------------|--------------------------------|
| cloud_controller              | uaa            | 8443 | TCP                      | HTTPS              | OAuth 2.0 or none <sup>*</sup> |
| diego_brain (SSH Proxy)       | uaa            | 443  | TCP                      | HTTPS              | OAuth 2.0                      |
| loggregator_trafficcontroller | uaa            | 8443 | TCP                      | HTTPS              | TLS                            |
| mysql_monitor                 | uaa            | 8443 | TCP                      | HTTPS              | OAuth                          |
| router                        | uaa            | 8443 | TCP                      | HTTPS              | OAuth 2.0                      |

<sup>\*</sup>The authentication method depends on the type of request.

### Outbound Communications: Internal to PCF

The following table lists network communication paths that are outbound from UAA.

| Source VM             | Destination VM           | Port | Transport Layer Protocol | App Layer Protocol | Security and Authentication        |
|-----------------------|--------------------------|------|--------------------------|--------------------|------------------------------------|
| uaa                   | mysql_proxy <sup>*</sup> | 3306 | TCP                      | MySQL              | MySQL authentication <sup>**</sup> |
| uaa (Route Registrar) | nats                     | 4222 | TCP                      | NATS               | Basic authentication               |

<sup>\*</sup>Applies only to deployments where internal MySQL is selected as the database.

<sup>\*\*</sup> MySQL authentication uses the MySQL native password method.

### Outbound Communications: External to PCF

The following table lists network communication paths from UAA that are outbound to external systems.

| Source VM | Destination VM | Port                           | Transport Layer Protocol | App Layer Protocol | Authentication |
|-----------|----------------|--------------------------------|--------------------------|--------------------|----------------|
| uaa       | LDAP           | LDAP server communication port | TCP                      | LDAP/LDAPS         | LDAP bind      |
| uaa       | SAML/OIDC      | 80 or 443 (HTTP port)          | TCP                      | HTTP/HTTPS         | Key            |

## BOSH DNS Communications

By default, PAS components and app containers look up services using the BOSH DNS service discovery mechanism. To support this lookup, BOSH Director colocates a BOSH DNS server on every deployed VM. For more information, see [BOSH DNS Network Communications](#).

## Consul Communications

If you disabled BOSH DNS for PAS components and other VMs by selecting **Disable BOSH DNS server for troubleshooting purposes** in the BOSH Director tile **Director Config** pane, PAS components call out to Consul for service discovery. For more information, see [Consul Network Communications](#).

## Credential and Identity Management

This section provides links to different aspects of identity management, including credential management handled by CredHub, user creation and permissions management, and authentication for Pivotal Cloud Foundry (PCF).

### General Identity Management

The following topics provide general information about credential and identity management in PCF.

- [Pivotal Cloud Foundry User Types](#)
- [Retrieving Credentials from Your Deployment](#)

### CredHub Documentation

CredHub provides centralized credential management in Pivotal Cloud Foundry (PCF). Credentials can include passwords, certificates, and SSH keys.

CredHub centralizes and secures credential generation, storage, lifecycle management, and system access.

For more information about CredHub, see the following topics.

- [CredHub](#): Provides an overview of CredHub.
- [CredHub Credential Types](#): Provides a reference of credential types supported in CredHub.

### UAA Documentation

PCF uses UAA to manage account roles and permissions in PCF runtimes. UAA supports access control as OAuth2 services and can store user information internally, or connect to external user stores through LDAP or SAML.

For more information about UAA, see the following topics.

- [UAA Overview](#)
- [UAA Concepts](#)
- [UAA Architecture](#)
- [Identity Providers in UAA](#)

### PCF Roles and User Accounts

The following topics describe how to manage PCF roles and user accounts in PCF.




- [Creating and Managing Users with the UAA CLI \(UAAC\)](#)
- [Adding Existing SAML or LDAP Users to a PCF Deployment](#)

### Ops Manager Roles and Permissions

- [Creating UAA Clients for BOSH Director](#)
- [Configuring Role-Based Access Control \(RBAC\) in Ops Manager](#)
- [Creating and Managing Ops Manager User Accounts](#)

### PAS Roles and Permissions

This section provides links to Pivotal Application Service (PAS) roles and permissions documentation.

- [Orgs, Spaces, Roles, and Permissions](#) 
- [Creating New PAS User Accounts](#) 
- [Managing User Roles with Apps Manager](#) 

## PKS Roles and Permissions

This section provides links to Pivotal Container Service (PKS) roles and permissions documentation.

- [Managing Users in PKS with UAA](#) 

## Pivotal Cloud Foundry User Types

Page last updated:

This topic describes the types of users in a Pivotal Cloud Foundry (PCF) deployment, their roles and permissions, and who creates and manages their user accounts.

The users who run a PCF deployment and have admin privileges are [operators](#). With Pivotal Application Service (PAS) installed to host apps, you add two more user types: [PAS users](#) who develop the apps and manage the development environment, and [end users](#) who just run the apps.

PCF distinguishes between these three user types and multiple user roles that exist within a single user type. Roles are assigned categories that more specifically define functions that a user can perform. A user may serve in more than one role at the same time.

## Operators

Operators have the highest, admin-level permissions. We also refer to operators as Ops Manager admins and PAS admins because they perform an admin role within these contexts.

## Tools and Tasks

Operators fulfill system administrator roles covering the entire PCF deployment. They work primarily with their IaaS and Ops Manager, to configure and maintain PAS component VMs. The component VMs, in turn, support the VMs that host applications. Typical operator tasks include:

- Deploying and configuring Ops Manager, PAS, and other product and service tiles.
- Maintaining and upgrading PCF deployments.
- Creating user accounts for PAS users and the orgs that PAS users work within.
- Creating service plans that define the access granted to end users.

## User Accounts

When Ops Manager starts up for the first time, the operator specifies one of the following authentication systems for operator user accounts:

- Internal authentication, using a new UAA database that Ops Manager creates.
- External authentication, through an existing identity provider accessed through SAML protocol.

The operator can then use the UAAC to [create more](#) operator accounts.

## PAS Users

PAS users are app developers, managers, and auditors who work within orgs and spaces, the virtual compartments within a deployment where PAS users can run apps and locally manage their roles and permissions.

A Role-Based Access Control (RBAC) system defines and maintains the different PAS user roles:

- Org Manager, Org Auditor, Org Billing Manager
- Space Manager, Space Developer, Space Auditor

The [Orgs, Roles, Spaces, Permissions](#) topic describes the PAS user roles, and what actions they can take within the orgs and spaces they belong to. Some of these permissions depend on the values of [feature flags](#).

## Tools

Space Developer users work with their software development tools and the apps deployed on host VMs.

All PAS users use system tools such as the Cloud Foundry Command Line Interface (cf CLI), PCF Metrics, and [Apps Manager](#), a dashboard for managing PAS users, orgs, spaces, and apps.

## User Accounts

When an operator configures PAS for the first time, they specify one of the following authentication systems for PAS user accounts:

1. Internal authentication, using a new UAA database created for PAS. This system-wide UAA differs from the Ops Manager internal UAA, which only stores Ops Manager Admin accounts.
2. External authentication, through an existing identity provider accessed through SAML or LDAP protocol.

In either case, PAS user role settings are saved internally in the Cloud Controller Database, separate from the internal or external user store.

Org and Space Managers then use Apps Manager to invite and manage additional PAS users within their orgs and spaces. PAS users with proper permissions can also use the cf CLI to assign user roles.

Operators can log into Apps Manager by using the **UAA Administrator User** credentials under the **Credentials** tab of the PAS tile. These UAA Admin credentials grant them the role of Org Manager within all orgs in the deployment. The UAA Admin can also use the UAAC to create new user accounts and the cf CLI to assign user roles.

## End Users

End users are the people who log into and use the apps hosted on PAS. They do not interact directly with PAS components or interfaces. Any interactions or roles they perform within the apps are defined by the apps themselves, not Pivotal Application Service.

## User Accounts and SSO

App developers can configure apps any way they want to grant end user access individually. In a deployment with [Single Sign-On Service for Pivotal Cloud Foundry](#) installed, they can also offer end users a single login that accesses multiple apps.

The Single Sign-On (SSO) service can save user account information in an external database accessed through SAML or LDAP, or in the internal PAS user store, along with PAS User accounts.

To make the SSO service available to developers, an operator creates service plans that give login access to specific groups of end users. A Space Manager then creates a local instance of the service plan, and registers apps with it. Apps registered to the plan instance then become available through SSO to all end users covered by the plan.

## User Types Summary

The following table summarizes PCF user types, their roles, the tools they use, the System of Record (SOR) that stores their accounts, and what accounts they can provision.

| User Type | Available Roles                                                                                                                                                                                                   | Tools They Use                                                                                                                                                                     | Account SOR                                                                    | Accounts They Can Provision                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------|
| Operators | Admin (UAA Admin, SSO Plan Admin, other system admins)                                                                                                                                                            | <ul style="list-style-type: none"> <li>IaaS UI</li> <li>PivNet</li> <li>Ops Manager</li> <li>cf CLI</li> <li>UAA CLI (UAAC)</li> <li>SSO Dashboard</li> <li>Marketplace</li> </ul> | Ops Manager user store through UAA<br><i>or</i><br>External store through SAML | Operators and PAS Users                                   |
| PAS Users | <ul style="list-style-type: none"> <li>UAA Administrator</li> <li>Org Manager</li> <li>Org Auditor</li> <li>Org Billing Manager</li> <li>Space Manager</li> <li>Space Developer</li> <li>Space Auditor</li> </ul> | <ul style="list-style-type: none"> <li>cf CLI</li> <li>CAPI</li> <li>Apps Manager</li> <li>PCF Metrics</li> <li>Marketplace</li> </ul>                                             | PAS user store through UAA<br><i>or</i><br>External store through SAML or LDAP | PAS Users within permitted orgs and spaces, and End Users |

|           |                          |             |                                                            |  |
|-----------|--------------------------|-------------|------------------------------------------------------------|--|
|           |                          |             |                                                            |  |
| End Users | Defined by apps they use | Hosted apps | Individual apps<br><i>or</i><br>PAS user store through SSO |  |



## Retrieving Credentials from Your Deployment

Page last updated:

This topic describes how the credentials for your Pivotal Cloud Foundry (PCF) deployment are stored and how you can access them.

- **What credentials does PCF store?**
  - Many PCF components use credentials to authenticate connections, and PCF installations often have hundreds of active credentials. This includes certificates, virtual machine (VM) credentials, and credentials for jobs running on the VMs.
- **Where does PCF store these credentials?**
  - PCF stores credentials in either the Ops Manager database or [BOSH CredHub](#). In PCF v1.11 and later, the BOSH Director VM includes a co-located CredHub instance. Ops Manager, Pivotal Application Service (PAS), and service tiles running on PCF can use this CredHub instance to store their credentials. For example, in PCF v1.12, PAS began migrating its credentials to CredHub. See the [PAS Release Notes](#) for a full list.
- **When do I need to access these credentials?**
  - You may need to access credentials for Ops Manager, PAS, and service tiles as part of regular administrative tasks in PCF, including troubleshooting. Many procedures in this documentation require you to retrieve credentials.
- **How can I retrieve credentials?**
  - The workflow for retrieving credentials depends on where they are stored. See the procedures below.

## Retrieve Credentials Stored in BOSH CredHub

To retrieve credentials from CredHub using the Ops Manager API, do the following:

1. Perform the procedures in the [Using the Ops Manager API](#) topic to authenticate and access the Ops Manager API.
2. Use the Ops Manager API to retrieve a list of deployed products:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Replace `UAA-ACCESS-TOKEN` with the access token recorded in the previous step.

3. In the response to the above request, locate the `guid` for the product from which you want to retrieve credentials. For example, if you want to retrieve PAS credentials, find the `installation_name` starting with `cf-` and copy its `guid`.
4. Run the following `curl` command to list the names of the credentials stored in CredHub for the product you selected. If you already know the name of the credential, you can skip this step.

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products/PRODUCT-GUID/variables" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Replace `PRODUCT-GUID` with the value of `guid` from the previous step.

5. Run the following `curl` command to view the credential:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products/PRODUCT-GUID/variables?name=VARIABLE-NAME" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Replace `VARIABLE-NAME` with the name of the credential you want to retrieve.

## Retrieve Credentials Stored in the Ops Manager Database

To retrieve credentials stored in the Ops Manager database and not CredHub, use the Ops Manager UI or API as outlined in the procedures below.

## Retrieve Credentials Using the Ops Manager UI

1. From Ops Manager, select the product tile for which you want to retrieve credentials.
2. Click the **Credentials** tab.
3. Locate the credential that you need and click **Link to Credential**.

## Retrieve Credentials Using the Ops Manager API

1. Perform the procedures in the [Using the Ops Manager API](#) topic to authenticate and access the Ops Manager API.
2. Use the Ops Manager API to retrieve a list of deployed products:

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Replace `UAA-ACCESS-TOKEN` with the access token recorded in the previous step.

3. In the response to the above request, locate the `guid` for the product from which you want to retrieve credentials. For example, if you want to retrieve PAS credentials, find the `installation_name` starting with `cf-` and copy its `guid`.
4. Run the following `curl` command to list references for the credentials stored in Ops Manager for the product you selected. If you already know the reference for the credential, you can skip this step.

```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products/PRODUCT-GUID/credentials" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Replace `PRODUCT-GUID` with the value of `guid` from the previous step.

5. Run the following `curl` command to view the credential:

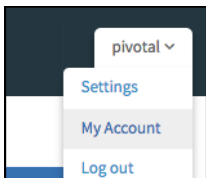
```
$ curl "https://OPS-MAN-FQDN/api/v0/deployed/products/PRODUCT-GUID/credentials/CREDENTIAL-REFERENCE" \
-X GET \
-H "Authorization: Bearer UAA-ACCESS-TOKEN"
```

Replace `CREDENTIAL-REFERENCE` with the name of the credential you want to retrieve.

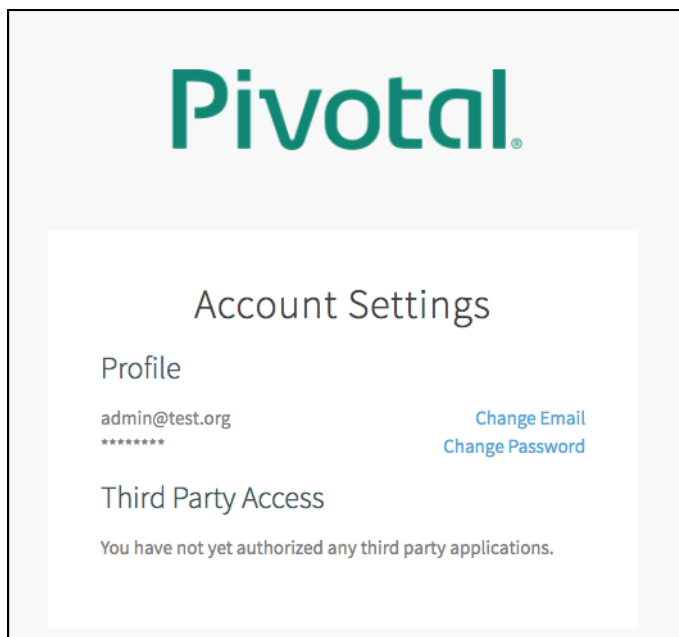
## Changing Ops Manager Credentials

### Ops Manager Password

1. Log in to Ops Manager and navigate to **My Account**. You can access this at <https://OPS-MAN-FQDN/uaa/profile>.



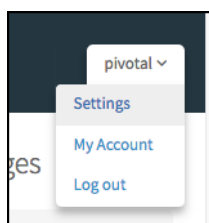
2. Navigate to **Change Password**. You can access this at [https://OPS-MAN-FQDN/uaa/change\\_password](https://OPS-MAN-FQDN/uaa/change_password).
3. Enter your current password and a new password.



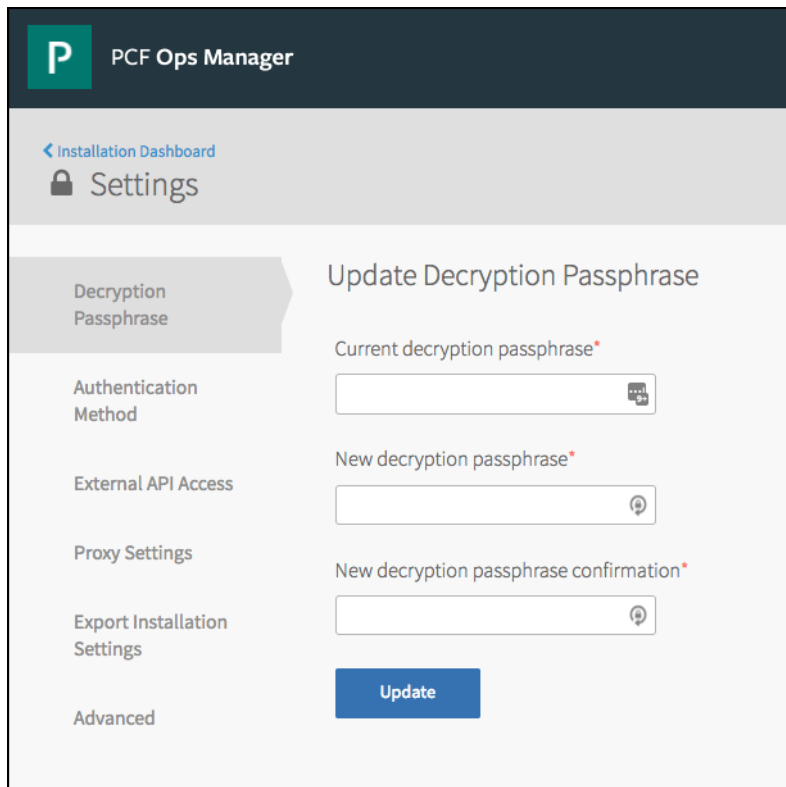
## Ops Manager Decryption Passphrase

You must have the existing passphrase to update the decryption passphrase.

1. Log in to Ops Manager, and navigate to **Settings**. You can access this at [https://OPS-MAN-FQDN/encryption\\_passphrase/edit](https://OPS-MAN-FQDN/encryption_passphrase/edit).



2. In the **Decryption Passphrase** panel, enter your current decryption passphrase and the new decryption passphrase, then click **Save**.



The screenshot shows the PCF Ops Manager interface. At the top is a dark blue header with the Pivotal 'P' logo and the text 'PCF Ops Manager'. Below the header is a light gray navigation bar containing a back arrow and the text 'Installation Dashboard', followed by a lock icon and the word 'Settings'. On the left side, there is a vertical sidebar with several settings categories: 'Decryption Passphrase' (which is highlighted with a gray arrow pointing right), 'Authentication Method', 'External API Access', 'Proxy Settings', 'Export Installation Settings', and 'Advanced'. The main content area on the right is titled 'Update Decryption Passphrase'. It contains three input fields: 'Current decryption passphrase\*' with a password icon, 'New decryption passphrase\*' with a password icon, and 'New decryption passphrase confirmation\*' with a password icon. At the bottom of this section is a blue button labeled 'Update'.

## S3 Compatible Blobstore Credentials

If you use an S3 compatible blobstore, you can rotate your blobstore credentials from the **Director Config** panel of the BOSH Director tile. After entering new credentials and clicking **Apply Changes**, BOSH recreates the VMs in your deployment to apply the new credentials.


1. From a browser, navigate to <https://OPS-MAN-FQDN/> and log in to Ops Manager.
2. From the Installation Dashboard, click the BOSH Director tile.
3. From the **Director Config** panel, select the **Recreate all VMs** checkbox.

## Director Config

---

NTP Servers (comma delimited)\*

169.254.169.254



JMX Provider IP Address

Bosh HM Forwarder IP Address

☐ Enable VM Resurrector Plugin

☐ Enable Post Deploy Scripts

☐ Recreate all VMs

This will force BOSH to recreate all VMs on the next deploy. Persistent disk will be preserved

4. For **Access Key**, enter a new access key.

Blobstore Location

☒ Internal


☐ S3 Compatible Blobstore

S3 Endpoint\*

Bucket Name\*

Access Key\*

Secret Key\*



☒ V2 Signature

☐ V4 Signature

Region\*

5. For **Secret Key**, enter a new secret key.
6. Click **Apply Changes**.
7. Clear the **Recreate all VMs** checkbox.

## CredHub

### Overview

CredHub is a component designed for centralized credential management in Pivotal Cloud Foundry (PCF). It is a single component that can address several scenarios in the PCF ecosystem. At the highest level, CredHub centralizes and secures credential generation, storage, lifecycle management, and access.

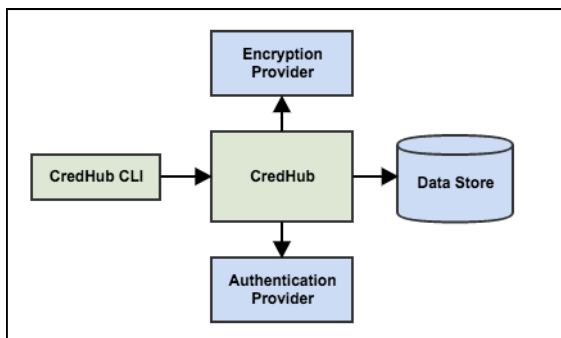
### What Can CredHub Do?

CredHub performs a number of different functions to help generate and protect the credentials in your PCF deployment.

- Securing data for storage
- Authentication
- Authorization
- Access and change logging
- Data typing
- Credential generation
- Credential metadata
- Credential versioning

### Application Architecture

CredHub consists of a REST API and a CLI. The REST API conforms to the Config Server API spec. CredHub is an OAuth2 resource server that integrates with User Account Authentication (UAA) to provide core authentication and federation capabilities.



### CredHub in PCF

A PCF deployment stores credentials in the following locations:

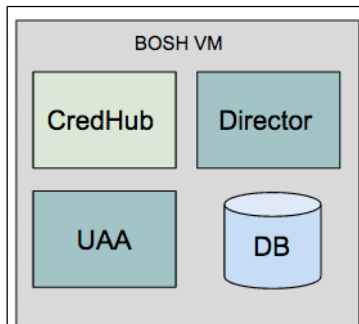
- **BOSH CredHub:** Colocated with the BOSH Director on a single VM. This CredHub instance stores credentials for the BOSH Director.
- **Runtime CredHub:** Deployed as an independent service and stores service instance credentials.

### BOSH CredHub

In PCF, BOSH Director VM includes a CredHub job. This provides a lightweight credential storage instance for the BOSH Director. The BOSH Director, Pivotal Application Service (PAS), and other tiles store credentials in BOSH CredHub. For more information, see [Retrieving Credentials from Your Deployment](#).

 **Note:** This configuration does not provide high availability.

In this colocated deployment architecture, the BOSH Director, CredHub, UAA, and the Director database are all installed on a single BOSH VM, as shown in the following diagram:

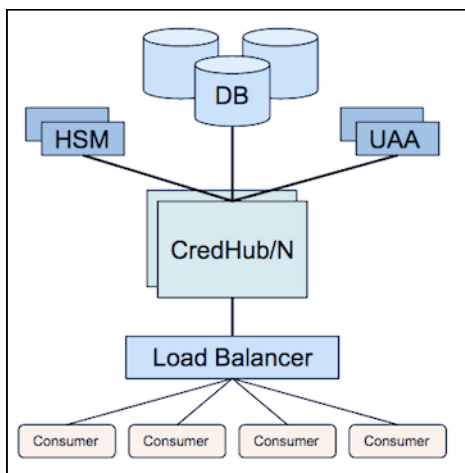


## Runtime CredHub

The PAS tile deploys CredHub as an independent service on its own VM. This provides a highly available credential storage instance for securing service instance credentials. For more information, see [Securing Service Instance Credentials with Runtime CredHub](#).

CredHub is a stateless application, so you can scale it to multiple instances that share a common database cluster and encryption provider.

With CredHub as a service, the load balancer and external databases communicate directly with the CredHub VMs, as shown in the following diagram:



## Using CredHub to Store Credentials for Service Tiles

If you develop a service tile for PCF and want to store its credentials in BOSH CredHub, see the [CredHub](#) section of the *Tile Developer Guide*.

## CredHub Credential Types

Credentials exist in multiple places in the PCF ecosystem. PCF components use credentials to authenticate connections between components. PCF installations often have hundreds of active credentials. Leaked credentials are common causes of data and security breaches, so managing them securely is very important.

For more information, read [CredHub Credential Types](#).

## Backing Up and Restoring CredHub Instances

The CredHub application does not hold state, but you must ensure its dependent components are backed up. Redundant backups can help prevent data loss if an individual component fails. For more information, read [Backing Up and Restoring CredHub Instances](#).





## CredHub Credential Types

This topic describes the different credential types supported by CredHub.

CredHub supports different types of credentials to simplify generating and managing multi-part credentials. For example, a TLS certificate contains three parts: the root certificate authority (CA), the certificate, and the private key. CredHub supports all three parts, which helps keep connection requests from being rejected erroneously.

CredHub supports the following credential types:









| Type                     | Description                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>value</code>       | A single string value for arbitrary configurations and other non-generated or validated strings.                                                                                                                |
| <code>json</code>        | An arbitrary JSON object for static configurations with many values.                                                                                                                                            |
| <code>user</code>        | Three string values for username, password, and password hash.                                                                                                                                                  |
| <code>password</code>    | A single string value for passwords and other random string credentials. Values for this type can be automatically generated.                                                                                   |
| <code>certificate</code> | An object containing a root CA, certificate, and private key. Use this type for key pair applications that utilize a certificate, such as TLS connections. Values for this type can be automatically generated. |
| <code>rsa</code>         | An object containing an RSA public key and private key without a certificate. Values for this type can be automatically generated.                                                                              |
| <code>ssh</code>         | An object containing an SSH-formatted public key and private key. Values for this type can be automatically generated.                                                                                          |

Each credential type supports distinct parameters for customizing how credentials are generated. These include minimum password lengths, required characters, and certificate fields. For more information, see the [Generate Credentials](#) section of the CredHub API documentation.

For every credential type, secret values are encrypted before storage. For instance, the private key of a certificate-type credential and the password of a user-type credential are encrypted before storage. For JSON and Value type credentials, the full contents are encrypted before storage.

## Security for Apps and Services

This topic links to topics that describe how PCF and PCF users manage security for apps and service instances.

- [Application Security Groups](#) : Describes how ASGs work and how to manage them in all versions of Cloud Foundry, including PCF.
- [Configuring SSH Access for PCF](#) : Explains how to configure PCF to allow SSH access to app instances, for debugging.
- [Restricting App Access to Internal PCF Components](#) : Details how to create Application Security Groups (ASGs), rules that allow internal outgoing communications from all apps in PCF, or the apps running in the same space.
- [Configuring Application Security Groups for Email Notifications](#) : Describes how to define an ASG to enable app-generated notifications.
- [Trusted System Certificates](#) : Explains where applications can find trusted system certificates.
- [Managing Access to Service Plans](#) : Describes how to enable or disable access to service plans for a subset of users.
- [Delivering Service Credentials to an Application](#) : Provides documentation on how to bind apps to service instances, which generate the credentials that enable the apps to use the service.
- [Managing Service Keys](#) : Explains to create and manage service keys that enable apps to use service instances.

## Compliance and Other Security-Related Topics

This section contains topics related to compliance and securing Pivotal Cloud Foundry (PCF) deployments.

### Compliance

- [NIST Controls and PCF](#): Provides a dedicated site that assesses Pivotal Cloud Foundry against NIST SP 800-53(r4) Controls.
- [General Data Protection Regulation](#) [↗](#): Provides an overview of the General Data Protection Regulation (GDPR) and where Pivotal Cloud Foundry (PCF) may store personal data

### Other Security-Related Topics

- [Security-Related PCF Tiles and Add-ons](#) [↗](#): Provides links to other security-related services available for PCF deployments.
- [Security Guidelines for Your IaaS Provider](#): Provides links to security-related documentation related to different IaaS providers. The topics may come from third party providers, and are not necessarily owned or maintained by Pivotal. Pivotal provides them for your convenience, but cannot guarantee the accuracy or currency of these documents.

## Assessment of Pivotal Cloud Foundry against NIST SP 800-53(r4) Controls

Page last updated:

Many organizations are required to reference a standardized control framework when assessing the security and compliance of their information systems. Standardized control frameworks are intended to provide a model for how to protect information and data systems from threats, including malicious third parties, structural failures, and human error. One very comprehensive and commonly referenced framework is NIST Special Publication 800-53(r4). Adherence to these controls is required for many government agencies in the United States, as well as for many private enterprises that operate within regulated markets, such as healthcare or finance. For example, the HIPAA regulations that govern the required protections for Personal Health Information (PHI) may be cross-referenced to the NIST SP 800-53(r4) control set.

These pages provide an assessment of the Pivotal Cloud Foundry PAS platform against the NIST SP 800-53(r4) controls, and provides guidance for how deployers may achieve compliance when using a shared responsibility model. Responsibility for any particular control may be assigned to the underlying IaaS infrastructure, the PAS platform, the deployed application, or the organization.

This document covers the Pivotal Cloud Foundry PAS, and assumes the use of BOSH and Ops Manager. In addition, we assume the platform has been deployed in a manner consistent with the corresponding IaaS reference architecture.

### Control Families

- [AC - Access Control](#)
- [AU - Audit and Accountability](#)
- [AT - Awareness and Training](#)
- [CM - Configuration Management](#)
- [CP - Contingency Planning](#)
- [IA - Identification and Authentication](#)
- [IR - Incident Response](#)
- [MA - Maintenance](#)
- [MP - Media Protection](#)
- [PS - Personnel Security](#)
- [PE - Physical and Environmental Protection](#)
- [PL - Planning](#)
- [PM - Program Management](#)
- [RA - Risk Assessment](#)
- [CA - Security Assessment and Authorization](#)
- [SC - System and Communications Protection](#)
- [SI - System and Information Integrity](#)
- [SA - System and Services Acquisition](#)

## General Data Protection Regulation

This topic provides an overview of the General Data Protection Regulation (GDPR) and where Pivotal Cloud Foundry (PCF) may store personal data.

### Overview

GDPR came into effect on May 25, 2018 and impacts any company processing the data of EU citizens or residents, even if the company is not EU-based. The GDPR sets forth how companies should handle privacy issues, securely store data, and respond to security breaches.

### Understand Personal Data

The GDPR grants data subjects certain rights, such as the right to obtain a copy of their personal data, object to the processing of personal data, and the right to have their personal data erased. Organizations subject to GDPR need to ensure that they can address and respond to requests by data subjects if they are processing their personal data.

Article 4, Section 1 of the GDPR defines personal data as follows:

‘personal data’ means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

For more information, see the GDPR [text](#).

Personal data can be collected, stored, and processed in a PCF deployment. Pivotal has performed a review of PCF components and determined that personal data may reside in the following areas:

- [User Account and Authentication \(UAA\)](#)
- [Cloud Foundry API](#)
- [Routing](#)
- [Diego](#)
- [Notifications Service](#)

### Where Personal Data May Reside

The following sections explain how different PCF components collect personal data.

#### User Account and Authentication (UAA)

UAA is an open-source Cloud Foundry component that provides identity management features and identity-based security for applications and APIs. For more information, see [User Account and Authentication](#).

| GDPR | Workflow       | What personal data is collected?                                                                                                                                                                | When is it collected?        | Where is it stored? | How is it processed? | Who has access to it?                                                                      |
|------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|---------------------|----------------------|--------------------------------------------------------------------------------------------|
|      | User registers | <ul style="list-style-type: none"> <li>• Username</li> <li>• Email address</li> <li>• First name (optional)</li> <li>• Last name (optional)</li> <li>• User ID (UAA GUID, generated)</li> </ul> | User registration submission | UAA DB              | Stored in UAA DB     | <ul style="list-style-type: none"> <li>• End user</li> <li>• UAA administrators</li> </ul> |
|      |                | <ul style="list-style-type: none"> <li>• Username</li> <li>• Email address</li> </ul>                                                                                                           |                              |                     |                      |                                                                                            |

|                     |                                                      |                                                                                                                                                                                                                                                     |                              |              |                                                                    |                                                                                        |
|---------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|--------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Business Initiation | Just-in-time provisioning: create user on user login | <ul style="list-style-type: none"> <li>First name (optional)</li> <li>Last name (optional)</li> <li>User ID (UAA GUID, generated)</li> <li>Additional attributes as defined by the organization</li> </ul>                                          | User login                   | UAA DB       | Stored in UAA DB                                                   | UAA administrators                                                                     |
|                     | Admin user makes a creation API call                 | <ul style="list-style-type: none"> <li>Username</li> <li>Email address</li> <li>First name (optional)</li> <li>Last name (optional)</li> <li>User ID (UAA GUID, generated)</li> <li>Additional attributes as defined by the organization</li> </ul> | Admin API call               | UAA DB       | Stored in UAA DB                                                   | UAA administrators                                                                     |
| Business Execution  | User self-updates profile                            | <ul style="list-style-type: none"> <li>Email address</li> <li>First name (optional)</li> <li>Last name (optional)</li> </ul>                                                                                                                        | User registration submission | UAA DB       | Stored in UAA DB                                                   | <ul style="list-style-type: none"> <li>End user</li> <li>UAA administrators</li> </ul> |
|                     | Just-in-time provisioning: user update               | <ul style="list-style-type: none"> <li>Email address</li> <li>First name (optional)</li> <li>Last Name (optional)</li> <li>Additional attributes as defined by the organization</li> </ul>                                                          | User login                   | UAA DB       | Stored in UAA DB                                                   | UAA administrators                                                                     |
|                     | User logs in                                         | <ul style="list-style-type: none"> <li>Current account cookie (generated)</li> <li>Saved account cookie (generated)</li> </ul>                                                                                                                      | User login                   | User browser | By UAA                                                             | <ul style="list-style-type: none"> <li>End user</li> <li>UAA login page</li> </ul>     |
|                     | Admin user makes an update API call                  | <ul style="list-style-type: none"> <li>Email address</li> <li>First name (optional)</li> <li>Last name (optional)</li> <li>Additional attributes as defined by the organization</li> </ul>                                                          | Admin API call               | UAA DB       | Stored in UAA DB                                                   | UAA administrators                                                                     |
| Delete User Flow    | Admin user makes a hard delete API call              | n/a                                                                                                                                                                                                                                                 | n/a                          | n/a          | Deleted from UAA DB                                                | UAA administrators                                                                     |
|                     | Admin user makes a deactivation API call             | n/a                                                                                                                                                                                                                                                 | n/a                          | n/a          | Soft delete (records still held in database but user cannot login) | UAA administrators                                                                     |
| Reports/Logs        | Event or debug logs                                  | Any information                                                                                                                                                                                                                                     | When event happens           | UAA logs     | Depends on setup of <a href="#">Loggregator</a> and log forwarding | BOSH administrators                                                                    |

## Cloud Foundry API

The Cloud Foundry API release contains several components, including the Cloud Controller. For more information, see the Cloud Foundry API release [README](#).

|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|

| GDPR                       | Workflow                                | What personal data is collected?                                                                                       | When is it collected?                                       | Where is it stored?                                                                                                         | How is it processed?                            | Who has access to it?                                                                                                               | How long is it kept?                                                                                                                        |
|----------------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Business Initiation</b> | User makes a request for the first time | User ID                                                                                                                | The first time a user makes a request to the API            | Cloud Controller DB                                                                                                         | It is used to identify permissions for the user | PCF operator                                                                                                                        | As long as the user is part of the system                                                                                                   |
| <b>Business Execution</b>  | Troubleshooting API requests            | <ul style="list-style-type: none"> <li>User ID</li> <li>User agent</li> <li>IP address</li> </ul>                      | On each request                                             | <ul style="list-style-type: none"> <li>Local VM: component and logs</li> <li>Log aggregator used by PCF operator</li> </ul> | n/a                                             | PCF operator                                                                                                                        | <ul style="list-style-type: none"> <li>Local VM: 4 week maximum by default</li> <li>Log aggregator as configured by PCF operator</li> </ul> |
| <b>Audit Trails</b>        | Audit what changes a user makes         | <ul style="list-style-type: none"> <li>Name</li> <li>User ID</li> <li>Email address</li> </ul>                         | On specific API requests that mutate the state of resources | Audit Event Table in the Cloud Controller DB                                                                                | n/a                                             | <ul style="list-style-type: none"> <li>PCF operator</li> <li>Users that can view the resource that had an audited change</li> </ul> | 31 days                                                                                                                                     |
|                            | Audit what changes a user makes         | <ul style="list-style-type: none"> <li>IP Address</li> <li>Email address</li> <li>User ID</li> <li>Username</li> </ul> | On each request                                             | <ul style="list-style-type: none"> <li>Local VM: CEF logs</li> <li>Log aggregator used by PCF operator</li> </ul>           | n/a                                             | PCF operator                                                                                                                        | <ul style="list-style-type: none"> <li>Local VM: 4 week maximum by default</li> <li>Log aggregator as configured by PCF operator</li> </ul> |
|                            | Audit what user created a resource      | <ul style="list-style-type: none"> <li>Name</li> <li>User ID</li> <li>Email address</li> </ul>                         | When API resources are created                              | As part of the resource row in Cloud Controller DB                                                                          | n/a                                             | <ul style="list-style-type: none"> <li>PCF operator</li> <li>Users that can view the resource</li> </ul>                            | As long as the resource exists                                                                                                              |

## Routing

By default, the [Gorouter](#) logs include the `X-Forwarded-For` header, which may include the originating client IP. Under GDPR, client IP addresses should be considered personal data.

### Disable Client IP Logging

In Pivotal Application Service (PAS) v2.0 and later and Elastic Runtime v1.12, operators can disable logging of client IP addresses in the Gorouter.

To disable logging of client IP addresses, do the following:

1. Navigate to the Ops Manager Installation Dashboard and click the PAS or Elastic Runtime tile.
2. Click **Networking**.
3. Under **Logging of Client IPs in CF Router**, select one of the two options:
  - If the source IP address exposed by your load balancer is its own IP address, select **Disable logging of X-Forwarded-For header only**.
  - If the source IP address exposed by your load balancer belongs to the downstream client, select **Disable logging of both source IP and X-Forwarded-For header**.
4. Click **Save**.



5. Return to the Ops Manager Installation Dashboard and click **Apply Changes** to redeploy.

## Diego

Diego is the container management system for PCF. For more information, see [Diego Components and Architecture](#).

| GDPR               | Workflow                                     | What personal data is collected?                                                                                                                                     | When is it collected?                                                                                                                                                                   | Where is it stored?                                                                                                                                                                             | How is it processed?                                                                                                                                                                             | Who has access to it?                                                                                                                                                    | How can I delete it?                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Business Execution | Executing apps and tasks                     | No personal data is collected explicitly, but personal data may be encoded in app file contents or runtime metadata such as environment variables or start commands. | Runtime metadata is collected when Cloud Controller submits work specification to the Diego BBS API. File contents are collected when Diego schedules an app or a task on a Diego cell. | Runtime metadata is stored in the Diego BBS DB. App file contents are cached on Diego cells.                                                                                                    | Runtime metadata is used to start processes inside app instance containers and to configure their environment. App file contents are presented as part of the app instance container filesystem. | Platform operators and other developers with access to the Cloud Controller space containing that app can view the data.                                                 | <ul style="list-style-type: none"> <li>To delete the runtime metadata stored in the Diego BBS DB, stop the app or cancel the task that includes that data.</li> <li>To delete the app file contents stored in the running app and task containers, stop the app or cancel the task to destroy the containers. To destroy the app file contents stored in the download cache on the Diego cells, recreate the Diego cell VMs.</li> </ul>                           |
| Reports/Logs       | SSH proxy logs<br>Cloud Foundry user access. | UAA user name and ID                                                                                                                                                 | When the user authenticates for SSH access to an app.                                                                                                                                   | The data is stored in a log file collocated with the SSH proxy instance handling the authentication request. This log file may also have its contents forwarded to a remote syslog destination. | No processing of the local log file is done automatically. If the log file contents are forwarded to a log aggregation service, they may be parsed and processed arbitrarily.                    | Only platform operators have access to the local log file. Platform operators or auditors may have access to these log contents in a downstream log aggregation service. | <p>To delete the log lines containing the user ID, perform the following steps:</p> <ol style="list-style-type: none"> <li>Run <code>bosh recreate</code> on the VMs hosting the SSH proxy processes to remove all the logs on ephemeral disk.</li> <li><code>bosh ssh</code> into the VMs hosting the SSH proxy processes and remove specific log lines containing user IDs.</li> <li>Scrub corresponding log lines from any log aggregation service.</li> </ol> |

## Notifications Service

The Notifications Service enables operators to configure components of Cloud Foundry to send emails to end users. For more information, see [Getting Started with the Notifications Service](#).

| GDPR               | Workflow                                            | What personal data is collected? | When is it collected?          | Where is it stored?                                                      | How is it processed?                 | Who has access to it?                          |
|--------------------|-----------------------------------------------------|----------------------------------|--------------------------------|--------------------------------------------------------------------------|--------------------------------------|------------------------------------------------|
| Business Execution | Sending email to UAA users                          | User ID                          | First email sent               | The <code>receipts</code> table in the Notifications database            | Stored in the Notifications database | Notifications operator making a database query |
|                    | UAA user unsubscribes globally                      | User ID                          | When the UAA user unsubscribes | The <code>global_unsubscribes</code> table in the Notifications database | Stored in the Notifications database | Notifications operator making a database query |
|                    | UAA user unsubscribes from a specific kind of email | User ID                          | When the UAA user unsubscribes | The <code>unsubscribes</code> table in the Notifications database        | Stored in the Notifications database | Notifications operator making a database query |
|                    | UAA user unsubscribes from a campaign in the v2 API | User ID                          | When the UAA user unsubscribes | The <code>unsubscribes</code> table in the Notifications database        | Stored in the Notifications database | Notifications operator making a database query |
| Reports/Logs       | UAA user unsubscribes                               | User email address               | When the UAA user unsubscribes | Log output                                                               | <a href="#">Loggregator</a>          | Loggregator Firehose users                     |

## Security-Related PCF Tiles and Add-ons

This section provides links to other security-related services available for Pivotal Cloud Foundry (PCF) deployments.

For information about other security-related tiles provided by Pivotal partners, refer to [Pivotal Network](#) and [Pivotal Documentation](#).

### Tiles

This section provides links to security-related tiles available for Pivotal Cloud Foundry (PCF) deployments.

- [Single Sign-On \(SSO\)](#): Provides support for native authentication, federated single sign-on, and authorization.
- [CredHub Service Broker](#): Allows apps running on Pivotal Application Service (PAS) to access secure credentials in CredHub.

### Add-ons

This section provides links to security-related BOSH add-ons available for Pivotal Cloud Foundry (PCF) deployments.

- [File Integrity Monitoring Add-on for PCF](#): Provides File Integrity Monitoring (FIM) protection within the PCF environment. This monitoring is sometimes required for compliance purposes.
- [IPsec Add-on for PCF](#): Describes the IPsec Add-on for PCF, which secures data transmissions inside Pivotal Cloud Foundry (PCF)
- [ClamAV Add-on](#): Provides antivirus protection within the PCF environment. This protection is sometimes required for compliance purposes.

## Security Guidelines for Your IaaS Provider

Pivotal Cloud Foundry supports a variety of Infrastructure as a Service (IaaS) providers. Different IaaS providers require different configuration steps to secure user data, identity information, and credentials.

Security requirements can vary broadly based on the unique configuration and infrastructure of each organization. Rather than provide specific guidance that may not apply to all use cases, Pivotal has collected links to IaaS providers' security and identity management documentation. The documents below may help you understand how your IaaS' security requirements impact your PCF deployment.

Pivotal does not endorse these documents for accuracy or guarantee that their contents apply to all PCF installations.



### How to Use This Topic

Find your IaaS provider in the list below. The documentation items linked for each IaaS may help you configure and secure your installation infrastructure.

## Amazon Web Services (AWS)

- [AWS Identity and Access Management guide](#) 

This guide is a reference for AWS' Identity and Access Management (IAM) features. If you're new to AWS, start here.

- [AWS identity documentation](#) 
- [AWS credential documentation](#) 

This documentation provides a general definition of IAM terms and provide best practices to help you manage IaaS users and permissions.

## Google Cloud Platform (GCP)

- [GCP authentication documentation](#) 




This developer-facing documentation explains general authentication guidelines for GCP.

## Microsoft Azure

- [Azure security documentation](#) 

This site has documentation on Azure security tools. It provides a general guide to how to manage IaaS users and credentials.

## OpenStack

- [OpenStack credential configuration](#) 
- [OpenStack credential creation](#) 
- [OpenStack deployment configuration](#) 

These documents provide a general reference for OpenStack service credential management.

## VMware vSphere

- [vSphere Security guide \(PDF\)](#) 



This guide contains best practices for securing and managing a vSphere installation.

## Buildpacks

Page last updated:

Buildpacks provide framework and runtime support for apps. Buildpacks typically examine your apps to determine what dependencies to download and how to configure the apps to communicate with bound services.

When you push an app, Cloud Foundry automatically detects an appropriate buildpack for it. This buildpack is used to compile or prepare your app for launch.













 **Note:** Cloud Foundry deployments often have limited access to dependencies. This limitation occurs when the deployment is behind a firewall, or when administrators want to use local mirrors and proxies. In these circumstances, Cloud Foundry provides a [Buildpack Packager](#)  app.


## About Buildpacks

For general information about buildpacks, see [About Buildpacks](#).

## System Buildpacks

Cloud Foundry includes a set of system buildpacks for common languages and frameworks. This table lists the system buildpacks.

| Name                       | Supported Languages, Frameworks, and Technologies                  | GitHub Repository                                                                                                       |
|----------------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Binary</a>     | <i>n/a</i>                                                         | <a href="#">Binary source</a>      |
| <a href="#">Go</a>         | Go                                                                 | <a href="#">Go source</a>          |
| <a href="#">HWC</a>        | HWC                                                                | <a href="#">HWC source</a>         |
| <a href="#">Java</a>       | Grails, Play, Spring, or any other JVM-based language or framework | <a href="#">Java source</a>        |
| <a href="#">.NET Core</a>  | .NET Core                                                          | <a href="#">.NET Core source</a>   |
| <a href="#">NGINX</a> *    | NGINX                                                              | <a href="#">NGINX source</a>       |
| <a href="#">Node.js</a>    | Node or JavaScript                                                 | <a href="#">Node.js source</a>     |
| <a href="#">PHP</a>        | Cake, Symfony, Zend, NGINX, or HTTPD                               | <a href="#">PHP source</a>         |
| <a href="#">Python</a>     | Django or Flask                                                    | <a href="#">Python source</a>      |
| <a href="#">R</a> *        | R                                                                  | <a href="#">R source</a>           |
| <a href="#">Ruby</a>       | Ruby, JRuby, Rack, Rails, or Sinatra                               | <a href="#">Ruby source</a>        |
| <a href="#">Staticfile</a> | HTML, CSS, JavaScript, or NGINX                                    | <a href="#">Staticfile source</a>  |

\* This buildpack is not distributed as part of Pivotal Application Service (PAS) v2.4. However, it is supported for use with PAS. You can download an offline version of this buildpack from [Pivotal Network](#) .

## Community Buildpacks

You can find a list of unsupported, community-created buildpacks here: [cf-docs-contrib](#) [↗](#).

## Customizing and Developing Buildpacks

For information about customizing existing buildpacks and developing new buildpacks, see [Customizing and Developing Buildpacks](#).

For information about updating and releasing a new version of a Cloud Foundry buildpack through the Cloud Foundry Buildpacks Team Concourse pipeline, see [Using CI for Buildpacks](#). You can use this as a model when working with Concourse to build and release new versions of your own buildpacks.

## About Buildpacks

Page last updated:

This topic provides links to additional information about using buildpacks. Each of the following are applicable to all supported buildpack languages and frameworks:

- [Buildpacks](#)
- [Stack Association](#)
- [Pushing an Application with Multiple Buildpacks](#)
- [Using a Proxy](#)
- [Supported Binary Dependencies](#)
- [Production Server Configuration](#)

## Buildpacks

Page last updated:

This topic describes how buildpacks work in Cloud Foundry.


## Buildpack Scripts


A buildpack repository may contain the following five scripts in the `bin` directory:


- `bin/detect` determines whether or not to apply the buildpack to an app.
- `bin/supply` provides dependencies for an app.
- `bin/finalize` prepares the app for launch.
- `bin/release` provides feedback metadata to Cloud Foundry indicating how the app should be executed.
- `bin/compile` is a deprecated alternative to `bin/supply` and `bin/finalize`.

The `bin/supply` and `bin/finalize` scripts replace the deprecated `bin/compile` script. Older buildpacks may still use `bin/compile` with the latest version of Cloud Foundry. In this case, applying multiple buildpacks to a single app is not supported. Similarly, newer buildpacks may still provide `bin/compile` for compatibility with Heroku and older versions of Cloud Foundry.

The `bin/supply` script is required for non-final buildpacks. The `bin/finalize` (or `bin/compile`) script is required for final buildpacks.

 **Note:** In this document, the terms *non-final buildpack* and *final buildpack*, or *last buildpack*, are used to describe the process of applying multiple buildpacks to an app. See the following example: `cf push APP-NAME -b FIRST-BUILDPACK -b SECOND-BUILDPACK -b FINAL-BUILDPACK`.

 **Note:** If you use only one buildpack for your app, this buildpack behaves as a final, or last, buildpack.

 **Note:** When using multi-buildpack support, the last buildpack in order is the final buildpack, and is able to make changes to the app and determine a start command. All other specified buildpacks are non-final and only supply dependencies.

### bin/detect

The `detect` script determines whether or not to apply the buildpack to an app. The script is called with one argument, the `build` directory for the app. The `build` directory contains the app files uploaded when a user performs a `cf push`.

The `detect` script returns an exit code of `0` if the buildpack is compatible with the app. In the case of system buildpacks, the script also prints the buildpack name, version, and other information to `STDOUT`.

The following is an example `detect` script that checks for a Ruby app based on the existence of a `Gemfile`:

```
#!/usr/bin/env ruby

gemfile_path = File.join ARGV[0], "Gemfile"


if File.exist?(gemfile_path)
 puts "Ruby"
 exit 0
else
 exit 1
end
```

Optionally, the buildpack `detect` script can output additional details provided by the buildpack developer. This includes buildpack versioning information and a list of configured frameworks and their associated versions.

The following is an example of the detailed information returned by the Java buildpack:

```
java-buildpack=v3.0-https://github.com/cloudfoundry/java-buildpack.git#3bd15e1 open-jdk-jre=1.8.0_45 spring-auto-reconfiguration=1.7.0_RELEASE tomcat-access-logging-support=2.4.0_RELEASE tomcat-in-
```



 **Note:** Cloud Foundry detects only one buildpack by default. When multiple buildpacks are desired, you must explicitly specify them.

For more information, see the [Buildpack Detection](#) section below.

## bin/supply

The `supply` script provides dependencies for the app and runs for all buildpacks. All output sent to `STDOUT` is relayed to the user through the Cloud Foundry Command Line Interface (cf CLI).

The script is run with four arguments:

- The `build` directory for the app
- The `cache` directory, which is a location the buildpack can use to store assets during the build process
- The `deps` directory, which is where dependencies provided by all buildpacks are installed
- The `index`, which is a number that represents the ordinal position of the buildpack

The `supply` script stores dependencies in `deps / index`. It may also look in other directories within `deps` to find dependencies supplied by other buildpacks.

The `supply` script must not modify anything outside of the `deps / index` directory. Staging may fail if such modification is detected.

The `cache` directory provided to the `supply` script of the final buildpack is preserved even when the buildpack is upgraded or otherwise changes. The `finalize` script also has access to this cache directory.

The `cache` directories provided to the `supply` scripts of non-final buildpacks are cleared if those buildpacks are upgraded or otherwise change.

The following is an example of a simple `supply` script:

```
#!/usr/bin/env ruby

#sync output

Stdout.sync = true

build_path = ARGV[0]
cache_path = ARGV[1]
deps_path = ARGV[2]
index = ARGV[3]

install_ruby

private

def install_ruby
 puts "Installing Ruby"

 # !!! build tasks go here !!!
 # download ruby
 # install ruby
end
```

## bin/finalize

The `finalize` script prepares the app for launch and runs only for the last buildpack. All output sent to `STDOUT` is relayed to the user through the cf CLI.

The script is run with four arguments:

- The `build` directory for the app
- The `cache` directory, which is a location the buildpack can use to store assets during the build process
- The `deps` directory, which is where dependencies provided by all buildpacks are installed
- The `index`, which is a number that represents the ordinal position of the buildpack

The `finalize` script may find dependencies installed by the `supply` script of the same buildpack in `deps / index`. It may also look in other directories within `deps` to find dependencies supplied by other buildpacks.

The `cache` directory provided to the `finalize` script is preserved even when the buildpack is upgraded or otherwise changes. The `supply` script of the same buildpack also has access to this cache directory.

The following is an example of a simple `finalize` script:

```
#!/usr/bin/env ruby

#sync output

Sstdout.sync = true

build_path = ARGV[0]
cache_path = ARGV[1]
deps_path = ARGV[2]
index = ARGV[3]

setup_ruby

private

def setup_ruby
 puts "Configuring your app to use Ruby"

 # !!! build tasks go here !!!
 # setup ruby
end
```

## bin/compile (Deprecated)

The `compile` script is deprecated. It encompasses the behavior of the `supply` and `finalize` scripts for single buildpack apps by using the `build` directory to store dependencies.

The script is run with two arguments:

- The `build` directory for the app
- The `cache` directory, which is a location the buildpack can use to store assets during the build process

During the execution of the `compile` script, all output sent to `STDOUT` is relayed to the user through the cf CLI.

## bin/release

The `release` script provides feedback metadata to Cloud Foundry indicating how the app should be executed. The script is run with one argument, the `build` directory. The script must generate a YAML file in the following format:

```
default_process_types:
 web: start_command.filetype
```


`default_process_types` indicates the type of app being run and the command used to start it. This start command is used if a start command is not specified in the `cf push` or in a Procfile.

At this time, only the `web` type of apps is supported.

 **Note:** To define environment variables for your buildpack, add a Bash script to the `.profile.d` directory in the root folder of your app.

The following example shows what a `release` script for a Rack app might return:

```
default_process_types:
 web: bundle exec rackup config.ru -p $PORT
```

 **Note:** The `web` command runs as `bash -c COMMAND` when Cloud Foundry starts your app. Refer to [the command attribute](#) section for more information about custom start commands.

## Droplet Filesystem

The buildpack staging process extracts the droplet into the `/home/vcap` directory inside the instance container and creates the following filesystem tree:

```
app/
deps/
logs/
tmp/
staging_info.yml
```

The `app` directory includes the contents of the `build` directory, and `staging_info.yml` contains the staging metadata saved in the droplet.

## Buildpack Detection

When you push an app, Cloud Foundry uses a detection process to determine a single buildpack to use. For general information about this process, see [How Apps Are Staged](#).

During staging, each buildpack has a position in a priority list. You can retrieve this position by running `cf buildpacks`.

Cloud Foundry checks if the buildpack in position 1 is a compatible buildpack. If the position 1 buildpack is not compatible, Cloud Foundry moves on to the buildpack in position 2. Cloud Foundry continues this process until the correct buildpack is found.

If no buildpack is compatible, the `cf push` command fails with the following error:

```
None of the buildpacks detected a compatible application
Exit status 222
Staging failed: Exited with status 222

FAILED
NoAppDetectedError
```

For a more detailed account of how Cloud Foundry interacts with the buildpack, see the [Sequence of Interactions](#) section below.

## Sequence of Interactions

This section describes the sequence of interactions between the Cloud Foundry platform and the buildpack. The sequence of interactions differs depending on whether the platform [skips](#) or [performs](#) buildpack detection.

### No Buildpack Detection

Cloud Foundry skips buildpack detection if the developer specifies one or more buildpacks in the app manifest or in the

```
cf push APP-NAME -b BUILDPACK-NAME
```

cf CLI command.

If you explicitly specify buildpacks, Cloud Foundry performs the following interactions:


1. For each buildpack except the last buildpack, the platform does the following:
  - a. Creates the `deps / index` directory
  - b. Runs `/bin/supply` with the `build`, `cache`, and `deps` directories and the buildpack `index`
  - c. Accepts any modification of the `deps / index` directory
  - d. Accepts any modification of the `cache` directory
  - e. May disallow modification of any other directories
2. For the last buildpack, the platform does the following:
  - a. If `/bin/finalize` is present:
    - i. Creates the `deps / index` directory if it does not exist
    - ii. If `/bin/supply` is present, runs `/bin/supply` with the `build`, `cache`, and `deps` directories and the buildpack `index`
    - iii. Accepts any modification of the `deps / index` directory

- iv. May disallow modification of the `build` directory
  - v. Runs `/bin/finalize` with the `build`, `cache`, and `deps` directories and the buildpack `index`
  - vi. Accepts any modification of the `build` directory
- b. If `/bin/finalize` is not present:
    - i. Runs `/bin/compile` with the `build` and `cache` directories
    - ii. Accepts any modification of the `build` directory
  - c. Runs `/bin/release` to determine staging information

At the end of this process, the `deps` directory is included at the root of the droplet, adjacent to the `app` directory.

## Buildpack Detection

Cloud Foundry performs buildpack detection if the developer does not specify one or more buildpacks in the app manifest or in the `cf push APP-NAME -b BUILDPACK-NAME` cf CLI command.

 **Note:** Cloud Foundry detects only one buildpack to use with the app.


If the platform performs detection, it does the following:


1. Runs `/bin/detect` for each buildpack
2. Selects the first buildpack with a `/bin/detect` script that returns a zero exit status
3. If `/bin/finalize` is present:
  - a. Creates the `deps / index` directory if it does not exist
  - b. If `/bin/supply` is present, runs `/bin/supply` with the `build`, `cache`, and `deps` directories and the buildpack `index`
  - c. Accepts any modification of the `deps / index` directory
  - d. May disallow modification of the `build` directory
  - e. Runs `/bin/finalize` on the `build`, `cache`, and `deps` directories
  - f. Accepts any modification of the `build` directory
4. If `/bin/finalize` is not present:
  - a. Runs `/bin/compile` on the `build` and `cache` directories
  - b. Accepts any modification of the `build` directory
5. Runs `/bin/release` to determine staging information

At the end of this process, the `deps` directory is included at the root of the droplet, adjacent to the `app` directory.

## Stack Association

This topic describes the stack association feature for Pivotal Cloud Foundry (PCF) buildpacks.

 **Note:** This functionality is supported as of CAPI [v1.58.0](#) and cf CLI [v6.39.0](#).

 **warning:** To avoid security exposure, ensure that you migrate your apps and custom buildpacks to use the `cflinuxfs3` stack based on Ubuntu 18.04 (Bionic Beaver). `cflinuxfs2` is based on Ubuntu 14.04 (Trusty Tahr), which reaches end of general support (EOGS) in April 2019.

## Overview

Each buildpack in your PCF deployment is associated with a stack. You can see this when you run `cf buildpacks`: there is a `stack` column in the output that shows a corresponding stack for each buildpack. See the following example:

```
$ cf buildpacks
Getting buildpacks...

buildpack position enabled locked filename stack
staticfile_buildpack 1 true false staticfile_buildpack-cached-cflinuxfs2-v1.4.29.zip cflinuxfs2
java_buildpack_offline 2 true false java-buildpack-offline-cflinuxfs2-v4.12.1.zip cflinuxfs2
ruby_buildpack 3 true false ruby_buildpack-cached-cflinuxfs2-v1.7.21.zip cflinuxfs2
...
```

Because of this stack association, buildpacks do not have to be uniquely named. This helps in managing similar buildpacks that are compatible with different stacks.

The [buildpack packager](#) includes a `--stack` option. If you use this option and upload a buildpack to PCF, the Cloud Controller detects the stack association and creates a stack record for the buildpack.

## Buildpacks without a Stack Record

Some buildpacks may have a missing stack record. For example, if you uploaded a custom buildpack before PCF introduced stack association. The output of `cf buildpacks` shows a blank `stack` column if the buildpack does not have a stack record.

In this case, you must manually assign a stack to the buildpack. To do this, run `cf update-buildpack BUILDPACK-NAME --assign-stack stack`.

Buildpacks with a missing stack record will continue to work, but are more manageable when the stack record is present.

Consider the following behavior when pushing apps to a deployment that has buildpacks with a missing stack record:

- If you push an app and specify a stack with `cf push app-name -s stack`, PCF uses that stack. Otherwise, it uses the system default, `cflinuxfs2`.
- You may see additional logging in the buildpack detection output of the `cf push` command when PCF detects buildpacks without a stack record.

## Managing Stack Association with the cf CLI

The cf CLI commands for managing buildpacks include functionality to support association between buildpacks and stacks. The `update-buildpack`, `rename-buildpack`, and `delete-buildpack` commands all include a `-s` flag for specifying a stack.

When operating on buildpacks with the cf CLI, consider the following:

- You cannot upload a buildpack with `cf create-buildpack` if a buildpack of the same name already exists and it has a missing stack record.
- When using `cf create-buildpack`, you may inadvertently create a duplicate buildpack with a `nil` stack. `cf create-buildpack` does not disallow creation of buildpacks with no stack association.
- The `-s` flag is required when there are two buildpacks with the same name. If you are operating on a uniquely named buildpack, you do not need to specify its stack.

- If you have two buildpacks of the same name, one with a stack record and one without, running cf CLI commands without `-s` operates on the buildpack with the missing stack record.

## Example Scenarios

See the following examples of managing buildpacks with the cf CLI, which are applicable when running `cf update-buildpack`, `cf rename-buildpack`, or



```
cf delete-
buildpack
```

- **Updating, renaming, or deleting a uniquely-named buildpack:**
  - You have a single buildpack named `my-buildpack`, and it is associated with `stack_a`. If you want to delete the buildpack, you can run `cf delete-buildpack my-buildpack`.
  - You can also provide `-s stack_a`, but the option is not required if you have a uniquely-named buildpack.
- **Updating, renaming, or deleting a uniquely-named buildpack that has a `nil` stack:**
  - You have a single buildpack named `my-buildpack`, and it is not associated with a stack. If you want to delete the buildpack, you can run `cf delete-buildpack my-buildpack`.
- **Updating, renaming, or deleting a buildpack when another buildpack exists with the same name, and both buildpacks have stack associations:**
  - You have two buildpacks named `my-buildpack`, one that is associated with `stack_a` and the other associated with `stack_b`. If you want to delete the buildpack that uses `stack_a`, you can run `cf delete-buildpack my-buildpack -s stack_a`.
- **Updating, renaming, or deleting a buildpack when another buildpack exists with the same name. One buildpack has a stack association, and the other buildpack has a `nil` stack:**
  - You have two buildpacks named `my-buildpack`, one associated with `stack_a` and the other associated with no (`nil`) stack association:
    - If you want to delete the buildpack that uses `stack_a`, you can run `cf delete-buildpack my-buildpack -s stack_a`.
    - If you want to delete the buildpack that is associated with the `nil` stack, run `cf delete-buildpack my-buildpack`.

## Pushing an Application with Multiple Buildpacks

Page last updated:


This topic describes how developers can push an application with multiple buildpacks.

 **Note:** As an alternative to the cf CLI procedure below, you can specify multiple buildpacks in your [application manifest](#). This is not compatible with [Deprecated App Manifest Features](#) .

For more information about pushing applications to Pivotal Application Service, see the [Deploy an Application](#) topic.

## Specifying Buildpacks with the cf CLI

To push an application with multiple buildpacks using the Cloud Foundry Command Line Interface (cf CLI), perform the following procedure:

 **Note:** You must use cf CLI v6.38 or later.

1. Run the following command to ensure that you are using the cf CLI v6.38 or later:

```
$ cf version
```

For more information about upgrading the cf CLI, see [Installing the cf CLI](#).


2. To push your app with multiple buildpacks, specify each buildpack with a `-b` flag:

```
$ cf push YOUR-APP -b BUILDPACK-NAME-1 -b BUILDPACK-NAME-2 ... -b FINAL-BUILDPACK-NAME
```

The last buildpack you specify is the **final buildpack**, which can modify the launch environment and set the start command.

To see a list of available buildpacks, run `cf buildpacks`.

For more information on multi-buildpack order, see the [Buildpacks](#) topic.

For more information about using the cf CLI, see the [Cloud Foundry Command Line Interface](#)  topic.

## Using a Proxy

Page last updated:

This topic describes how developers can use a proxy with the buildpacks for their application.

### Use a Proxy

Buildpacks can use proxies using the `http_proxy` and `https_proxy` environment variables. You should set these to the proxy hostname or port.

All of the buildpacks automatically use these proxy environment variables correctly. If any buildpacks contacts the Internet during staging, it does so through the proxy host. The binary buildpack does not use a proxy because it does not use the Internet during staging.

To set a proxy for buildpacks to use during staging, perform one of the following procedures:

- Set the environment variables by adding the following section to the `env` block of the application manifest:

```

env:
 http_proxy: http://YOUR-HTTP-PROXY:PORT
 https_proxy: https://YOUR-HTTPS-PROXY:PORT
```

- Set the environment variables with the Cloud Foundry Command Line Interface (cf CLI) using the `cf set-env` command:

```
$ cf set-env YOUR-APP http_proxy "http://YOUR-HTTP-PROXY:PORT"
$ cf set-env YOUR-APP https_proxy "https://YOUR-HTTPS-PROXY:PORT"
```



**Note:** While many apps use the `http_proxy` and `https_proxy` environment variables at runtime, some do not. The buildpack does not add extra functionality to make proxies work at runtime.



## Supported Binary Dependencies

Page last updated:

Each buildpack only supports the stable patches for each dependency listed in the buildpack's `manifest.yml` and also in its GitHub releases page. For example, see the [php-buildpack releases page](#).

If you try to use an unsupported binary, staging your app fails with the following error message:

```
Could not get translated url, exited with: DEPENDENCY_MISSING_IN_MANIFEST:
...
!
! exit
!
Staging failed: Buildpack compilation step failed
```

## Production Server Configuration

Page last updated:

This topic describes how to configure a production server for your apps.

When you deploy an app, PAS determines the command used to start the app through the following process:

1. If the developer uses the command `cf push -c COMMAND`, then PAS uses `COMMAND` to start the app.
2. If the developer creates a file called a Procfile, PAS uses the Procfile to configure the command that launches the app. See the [About Procfiles](#) section below for more information.
3. If the developer does not use `cf push -c COMMAND` and does not create a Procfile, then PAS does one of the following, depending on the buildpack:
  - Uses a default start command.
  - Fails to start the app and shows a warning that the app is missing a Procfile.

## About Procfiles

One reason to use a Procfile is specify a start command for buildpacks where a default start command is not provided. Some buildpacks, such as Python, that work on a variety of frameworks, do not attempt to provide a default start command.

Another reason to use a Procfile is to configure a production server for web apps.

A Procfile enables you to declare required runtime processes, called process types, for your web app. Process managers in a server use the process types to run and manage the workload. In a Procfile, you declare one process type per line and use the following syntax:

```
PROCESS_TYPE: COMMAND
```

- `PROCESS_TYPE` is `web`. A `web` process handles HTTP traffic.
- `COMMAND` is the command line to launch the process.

For example, a Procfile with the following content starts the launch script created by the build process for a Java app:

```
web: build/install/MY-PROJECT-NAME/bin/MY-PROJECT-NAME
```

## Specify a Web Server

Follow these steps to specify a web server using a Procfile. For more information about configuring a web server for Rails apps, see the [Configure a Ruby Web Server](#) section of this topic.

1. Create a blank file with a command line for a `web` process type.
2. Save it as a file named `Procfile` with no extension in the root directory of your app.
3. Push your app.

## Configure a Ruby Web Server

PAS uses the default standard Ruby web server library WEBrick for Ruby and Ruby on Rails apps. However, PAS can support a more robust production web server, such as Phusion Passenger, Puma, Thin, or Unicorn.

To instruct PAS to use a web server other than WEBrick, perform the following steps:

1. Add the gem for the web server to your Gemfile.
2. In the `config` directory of your app, create a new configuration file or modify an existing file. Refer to your web server documentation for how to configure this file. The following example uses the Puma web server:

```
config/puma.rb
threads 8,32
workers 3

on_worker_boot do
 # things workers do
end
```

3. In the root directory of your app, create a Procfile and add a command line for a `web` process type that points to your web server. For information about configuring the specific command for a process type, see your web server documentation.

The following example shows a command that starts a Puma web server and specifies the app runtime environment, TCP port, and paths to the server state information and configuration files:

```
web: bundle exec puma -e $RAILS_ENV -p 1234 -s ~/puma -C config/puma.rb
```

## Binary Buildpack

Page last updated:

Use the binary buildpack for running arbitrary binary web servers.

### Push an App

Specify the binary buildpack to stage an app as a binary file. On a command line, use `cf push APP-NAME` with the `-b` option to specify the buildpack.

For example:

```
$ cf push my_app -b https://github.com/cloudfoundry/binary-buildpack.git
```

You can provide Cloud Foundry with the shell command to execute your binary in the following two ways:

- **Procfile:** In the root directory of your app, add a `Procfile` that specifies a `web` task:

```
web: ./app
```

- **Command line:** Use `cf push APP-NAME` with the `-c` option:

```
$ cf push my_app -c './app' -b binary_buildpack
```

### Compile your Binary

Cloud Foundry expects your binary to bind to the port specified by the `PORT` environment variable.

The following example in [Go](#) binds a binary to the `PORT` environment variable:

```
package main

import (
 "fmt"
 "net/http"
 "os"
)

func handler(w http.ResponseWriter, r *http.Request) {
 fmt.Fprintf(w, "Hello, %s", "world!")
}

func main() {
 http.HandleFunc("/", handler)
 http.ListenAndServe(":"+os.Getenv("PORT"), nil)
}
```

Your binary should run without any additional runtime dependencies on the `cflinuxfs2` or `lucid64` root filesystem (rootfs). Any such dependencies should be statically linked to the binary.

To boot a Docker container running the `cflinuxfs3` filesystem, run the following command:

```
$ docker run -it cloudfoundry/cflinuxfs2 bash
```

To boot a Docker container running the `lucid64` filesystem, run the following command:

```
$ docker run -it cloudfoundry/lucid64 bash
```

To compile the above Go application on the rootfs, `golang` must be installed. `apt-get install golang` and `go build app.go` will produce an `app` binary.

When deploying your binary to Cloud Foundry, use `cf push` with the `-s` option to specify the root filesystem it should run against.

```
$ cf push my_app -s (cflinuxfs2/lucid64)
```

## BOSH Configured Custom Trusted Certificate Support

Your platform operator can configure the platform to add the custom certificates into the application container. The custom trusted certificates are added to the `/etc/ssl/certs` directory and can be used by binary applications.

For more information, see [Configuring Trusted System Certificates for Applications](#).

## .NET Apps

If you are pushing a .NET Console app using the binary buildpack, see [Console Applications](#) in the *.NET Cookbook* for more information.

You can deploy .NET Core apps to a Windows stack using the binary buildpack. Build it as a self-contained app and push it with the binary buildpack, specifying the `windows2016` stack with a custom start command.

For information about deploying different types of .NET apps, follow the links in the table below.

| Type of .NET App                                                                                  | Buildpack                 |
|---------------------------------------------------------------------------------------------------|---------------------------|
| ASP.NET MVC<br>ASP.NET Web Forms<br>ASP.NET WebAPI Apps<br>Windows Communication Foundation (WCF) | <a href="#">HWC</a>       |
| .NET Core pushed to Linux stack                                                                   | <a href="#">.NET Core</a> |

## Help and Support

Join the #buildpacks channel in our [Slack community](#) if you need any further assistance.

For more information about using and extending the binary buildpack in Cloud Foundry, see the [binary-buildpack GitHub repository](#).

You can find current information about this buildpack on the binary buildpack [release page](#) in GitHub.

## Go Buildpack

Page last updated:

## Supported Versions

Supported Go versions can be found [in the release notes](#).

## Push an App

The Go buildpack will be automatically detected in the following circumstances:

- Your app has been packaged with [godep](#) using `godep save`.
- Your app has a `vendor/` directory and has any files ending with `.go`.
- Your app has a `GOPACKAGE` environment variable specified and has any files ending with `.go`.
- Your app has a `glide.yml` file and is using [glide](#), starting in buildpack version [1.7.9](#).
- Your app has a `Gopkg.toml` file and is using [dep](#), starting in buildpack version [1.8.9](#).

If your Cloud Foundry deployment does not have the Go Buildpack installed, or the installed version is out of date, you can use the latest version with the command:

```
$ cf push my_app -b https://github.com/cloudfoundry/go-buildpack.git
```

When specifying versions, specify only major/minor versions, such as Go 1.6, rather than Go 1.6.0. This ensures you receive the most recent patches.

## Start Command

When pushing Go apps, you can specify a start command for the app. You can place the start command in the `Procfile` file in root directory of your app. For example, if the binary generated by your Go project is `my-go-server`, your `Procfile` could contain the following:

```
web: my-go-server
```

For more information about Procfiles, see the [Configuring a Production Server](#) topic.

You can also specify the start command for your app in the `manifest.yml` file in the root directory. For example, your `manifest.yml` could contain the following:

```

applications:
- name: my-app-name
 command: my-go-server
```

If you do not specify a start command in a `Procfile`, in the manifest, or with the `-c` flag for `cf push`, the generated binary will be used as the start command. Example: `my-go-server`

## Push an App with godep

If you are using [godep](#) to package your dependencies, make sure that you have created a valid `Godeps/Godeps.json` file in the root directory of your app by running `godep save`.


When using godep, you can fix your Go version in `GoVersion` key of the `Godeps/Godeps.json` file.

- [Sample Go 1.6 app](#) 

An example `Godeps/Godeps.json` :

```
{
 "ImportPath": "go_app",
 "GoVersion": "go1.6",
 "Deps": []
}
```

## Push an App with Glide

If you use [glide](#)  to specify or package your dependencies, make sure that you have created a valid `glide.yml` file in the root directory of your app by running `glide init` .

To vendor your dependencies before pushing, run `glide install` . This will generate a `vendor` directory and a `glide.lock` file specifying the latest compatible versions of your dependencies. You must have a `glide.lock` file when pushing a vendored app. You do not need a `glide.lock` file when deploying a non-vendored app.

### Glide

- [Sample Go app with Glide](#) 

An example `glide.yml` file:


```
package: go_app_with_glide
import:
- package: github.com/ZiCog/shiny-thing
 subpackages:
 - foo
```

You can specify Go version in the `manifest.yml` file:

```

applications:
- name: my-app-name
 env:
 GOVERSION: go1.8
```

## Push an App with dep

If you use [dep](#)  to specify or package your dependencies, make sure that you have created a valid `Gopkg.toml` file in the root directory of your app by running `dep init` .

To vendor your dependencies before pushing, run `dep ensure` . This will generate a `vendor` directory and a `Gopkg.lock` file specifying the latest compatible versions of your dependencies. You must have a `Gopkg.lock` file when pushing a vendored app. You do not need a `Gopkg.lock` file when deploying a non-vendored app.

### dep

- [Sample Go app with dep](#) 

An example `Gopkg.toml` file:

```
[[constraint]]
branch = "master"
name = "github.com/ZiCog/shiny-thing"
```

You can specify Go version in the `manifest.yml` file:

```

applications:
- name: my-app-name
 env:
 GOVERSION: go1.8
```

## Push an App with Native Go Vendoring

If you use the native Go vendoring system, which packages all local dependencies in the `vendor/` directory, you must specify your app's package name in the `GOPACKAGENAME` environment variable.

An example `manifest.yml` :

```

applications:
- name: my-app-name
 command: go-online
 env:
 GOPACKAGENAME: example.com/user/app-package-name
```

### Go 1.6

- [Sample Go 1.6 app with native vendoring](#) ↗.

Go 1.6 has vendoring enabled by default. Set the `GO15VENDOREXPERIMENT` environment variable to `0` to disable vendoring.

An example `manifest.yml` file:

```

applications:
- name: my-app-name
 command: example-project
 env:
 GOVERSION: go1.6
 GOPACKAGENAME: example.com/user/app-package-name
```

### Go 1.7 and Later

- [Sample Go 1.7 app with native vendoring](#) ↗.

Go 1.7 and later always has vendoring enabled, and you cannot disable it with an environment variable.

An example `manifest.yml` :

```

applications:
- name: my-app-name
 command: example-project
 env:
 GOVERSION: go1.8
 GOPACKAGENAME: example.com/user/app-package-name
```

## Pass a Symbol and String to the Linker

The Go buildpack supports the Go [linker's](#) ↗ ability, `-X symbol value`, to set the value of a string at link time. Set the `GO_LINKER_SYMBOL` and `GO_LINKER_VALUE` in the application's configuration before pushing code.

This can be used to embed the commit SHA or other build-specific data directly into the compiled executable.

For a sample Go app, see the [go-buildpack](#) ↗ repository on GitHub.



## C Dependencies

The Go buildpack supports building with C dependencies using [cgo](#). You can set config vars to specify cgo flags to, for example, specify paths for vendored dependencies. As an example, to build [gopgsqldriver](#), add the config var `CGO_CFLAGS` with the value `-I/app/code/vendor/include/postgresql` and include the relevant Postgres header files in `vendor/include/postgresql/` in your app.

## Proxy Support

If you need to use a proxy to download dependencies during staging, you can set the `http_proxy` and/or `https_proxy` environment variables. For more information, see the [Proxy Usage](#) topic.

## BOSH Configured Custom Trusted Certificate Support

Go uses certificates stored in `/etc/ssl/certs`. Your platform operator can configure the platform to [add the custom certificates into the application container](#).

## Help and Support

Join the #buildpacks channel in our [Slack community](#) if you need any further assistance.

For more information about using and extending the Go buildpack in Cloud Foundry, see the [go-buildpack GitHub repository](#).

You can find current information about this buildpack on the Go buildpack [release page](#) in GitHub.

## HWC Buildpack

Page last updated:

This topic describes how to configure your .NET Framework apps for use with the HWC buildpack and how to push your .NET Framework apps to Pivotal Application Service for Windows (PASW).

The HWC buildpack provides a runtime server that uses the Hosted Web Core API for running .NET Framework applications in Windows Server containers. For more information, see [Hosted Web Core API Reference](#) in the Microsoft documentation.

The HWC buildpack provides access to .NET Framework 4.5.1 and later, made available by the Windows root file system (rootfs). Using the HWC buildpack requires deploying Windows cells with PASW.

The HWC buildpack supports the following common app types by default:

- ASP.NET MVC
- ASP.NET Web Forms
- ASP.NET WebAPI Apps
- Windows Communication Foundation (WCF)

For information about deploying different types of .NET apps, follow the links in the table below.

| Type of .NET App                  | Buildpack                 |
|-----------------------------------|---------------------------|
| .NET Console                      | <a href="#">Binary</a>    |
| .NET Core pushed to Linux stack   | <a href="#">.NET Core</a> |
| .NET Core pushed to Windows stack | <a href="#">Binary</a>    |

Before you push your first app using the HWC buildpack, see the [Getting Started](#) guide in the *.NET Cookbook*.

## Configure HWC

HWC relies on a `Web.config` configuration file for configuring the .NET applications.

Most `Web.config` files work out of the box with PASW, with the following constraints:

- Integrated Windows Authentication (IWA) is not yet supported on PASW.
- SQL server connection strings must use fully qualified domain names.
- Place connection string values in environment variables or [user-provided service instances](#).

The HWC buildpack includes a default configuration for the `applicationHost.config`, similar to IIS.

## Add a Global Error Handler

Before you push your app for the first time, add a global error handler. Without a global error handler, you will not receive any log information from your app if it crashes on startup.

To configure a global error handler that logs to `stdout`, see [Application Error Handling](#) in the *.NET Cookbook*.

## Push an App

Follow the steps below to push your application.

1. Build your app in Visual Studio. On the command line, navigate to the directory that contains the app files.
2. Run `cf push APP-NAME -s windows2016 -b hwc_buildpack` to push your app, where `APP-NAME` is the name you want to give your app. For example:

```
$ cf push my-app -s windows2016 -b hwc_buildpack
Creating app my-app in org sample-org / space sample-space as username@example.com...
OK
...
requested state: started
instances: 1/1
usage: 1GB x 1 instances
urls: my-app.example.com
```

- Find the URL of your app in the output from the push command and navigate to it to see your HWC app running. In the example above, `my-app.example.com` is the URL of your app.

## Features

Below are a set of features that can be used with HWC buildpack.

### Context Path Routing

Context path routing is a feature analogous to IIS virtual directories. It enables multiple applications to share the same route hostname.

HWC-hosted apps use the `VCAP_APPLICATION` environment variable to read out the bound app URIs. Any context path that exists underneath the root in the app's bound route corresponds to the `applicationHost.config`.

Run the following commands to define context path routing that makes `app2` accessible under `app1`'s URL. For example, `app1.example.com/app2`:

```
$ cf push app1 #find the URL for your app1
$ cf push app2 --no-start --no-route
$ cf map-route app2 example.com --hostname app1 --path app2
$ cf start app2
```

### Shadow Copy Setting

[Shadow Copy](#) is a hosting option that copies assemblies for an app in the `bin` directory to the app's temporary files directory. This features is turned off and unnecessary for apps running under Cloud Foundry. An app can override this setting in its `Web.config` file.

### URL Rewrite

The HWC buildpack supports the URL Rewrite module. It is preinstalled in the Windows file system.

### Profile Scripts

The HWC buildpack allows developers to provide `.profile.bat` scripts with their applications. You can use a `.profile.bat` script to perform app-specific initialization tasks, such as setting custom environment variables.

For information about configuring `.profile.bat` scripts, see the [Configure Pre-Runtime Hooks](#) section of *Deploy an Application*.

## Buildpack Support

A number of channels exist where you can get more help when using the HWC buildpack, or when developing your own HWC buildpack.

- HWC Buildpack Repository in GitHub:** Find more information about using and extending the HWC buildpack in the [HWC buildpack repository](#) in GitHub.
- Release Notes:** Find current information about this buildpack on the [HWC buildpack release page](#) in GitHub.
- Slack:** Join the #buildpacks channel in the [Cloud Foundry Slack community](#).



## Creating an Extension Buildpack for .NET Apps

This topic explains how to write extension buildpacks for .NET apps.

### Prerequisites

- Linux or MacOS development machine or virtual machine
- [Golang](#) v1.10 or later programming language
- [direnv](#) environment variable manager for your shell

### Initialize an Extension Buildpack

1. To install the `buildpack-packager` CLI tool, run the commands below. The [buildpack-packager](#) provides boilerplate code that you can use to start writing your buildpack.

```
go get github.com/cloudfoundry/libbuildpack/
go install github.com/cloudfoundry/libbuildpack/packager
```

2. To create your buildpack, run the following command:

```
buildpack-packager init --name MY-BUILDPACK-NAME --path=BUILDPACK-DIRECTORY
```

Where:

- `MY-BUILDPACK-NAME` is the name of the buildpack you are creating.
- `BUILDPACK-DIRECTORY` is the directory created by the command. This directory contains the boilerplate code.

For example:

```
$ buildpack-packager init --name my-example --path=my-example-buildpack
```


3. To activate direnv in your buildpack directory, run the following commands:

```
cd my-example-buildpack
direnv allow
```

## Create an Extension Buildpack to Supply Additional DLLs to a .NET Framework App

Most .NET Framework apps are pushed with the [Hosted Web Core \(HWC\) buildpack](#). The HWC buildpack contains an opinionated list of .NET dependencies and does not contain all the DLLs that every app could need.

If your app requires dependencies not contained in the HWC buildpack, we recommend that you create an extension buildpack. This extension buildpack references and supplies these dependencies to the app's container when you push the app.

 **Note:** You cannot add modules or extensions directly to HWC. HWC contains a number of built-in HWC features, like the URL Rewrite module and HTTP compression. Extensions should only provide additional functionality to your app. For more information about existing HWC features, see [Features](#) in *HWC Buildpack*.

To create an extension buildpack containing additional DLLs, follow the steps below:

1. Create a list of the dependencies that your published app requires.
2. Copy the DLLs for the dependencies into a zip file.
3. Upload the zip file containing your dependencies to a private web server that is accessible by Cloud Foundry. You can also use an S3 bucket or Azure Storage.

- On the command line, browse to the directory created by the `buildpack-packager init` command above.
- Edit the `manifest.yml` file by adding a `dependency` section that references the DLL zip file as follows:

```
dependencies:
- name: my-binary
 uri: http://s3.amazonaws.com/my-bucket/DLL-ZIP-FILE
 version: 0.0.1
 sha256: GENERATED-SHA-256
 cf_stacks:
 - windows2016
```

Where:

- `DLL-ZIP-FILE` is the name of your DLL zip file.
- `GENERATED-SHA-256` is a SHA generated by running the following command:

```
shasum -a256 DLL-ZIP-FILE
```

Where `DLL-ZIP-FILE` is the name of your DLL zip file.

- Ensure the `include_files` section of the manifest contains `bin/supply.exe`.
- Edit the supply script, `my-example-buildpack/src/my-example/supply.go`, to add dependencies to the container's `PATH` as follows:
  - Add a `stager.InstallDependency` for the `dependency` and `version` you have in your `manifest.yml` file.
  - Add a `stager.AddBinDependency` for every DLL file you want your app to be able to access. For example:

```
dep := libbuildpack.Dependency{Name: "my-binary", Version: "0.0.1"}
if err := s.Installer.InstallDependency(dep, s.Stager.DepDir()); err != nil {
 return err
}
if err := s.Stager.AddBinDependencyLink(filepath.Join(s.Stager.DepDir(), "MyBinary.dll"), "MyBinary.dll"); err != nil {
 return err
}
```


- Edit `scripts/build.sh` to cross-compile as follows:

```
GOOS=windows go build -ldflags="-s -w" -o bin/supply.exe mysql/supply/cli
```

## Complete Extension Buildpack

- To build a cached buildpack artifact, run the following command:

```
buildpack-packager build -cached -stack windows2016
```

 **Note:** If the buildpack code contains a mistake, `buildpack-packager` throws an error. Once all local errors are corrected, you must push your app to with the new extension buildpack to determine whether the new buildpack functions as intended.

- Upload the buildpack to a private web server accessible to Cloud Foundry. You can also use an S3 bucket or Azure Storage. You can upload the finished buildpack to the same web server as your dependencies.
- To deploy your app with the extension buildpack, run the following command:

```
cf push my-app -s windows2016 -b BUILDPACK-URL -b hwc_buildpack
```

Where `BUILDPACK-URL` is the URL where you uploaded the buildpack. For example:

```
$ cf push my-app -s windows2016 -b http://s3.amazonaws.com/my-bucket/my-example-buildpack.zip -b hwc_buildpack
```

If your extension buildpack does not include the correct dependencies, you will receive an error message.

## Combine Extension Buildpack with Other Features

If your extension buildpack has executables or scripts that need to be run, you can reference them either in the start command or in profile scripts.

- For more information about the start command, see [command](#) in *Deploying with Application Manifests*.
- For more information about profile scripts, see [Configure Pre-Runtime Hooks](#) in *Deploy an Application*.

## Tips for .NET Developers

This topic lists resources for developing .NET apps that run on Pivotal Application Service (PAS) for Windows, and describes how to push .NET apps to PAS for Windows cells.

For how to develop .NET microservices for .NET apps using Steeltoe, see the [Steeltoe documentation](#).

### Overview

After operators install and configure the PAS for Windows tile, developers can push .NET apps to the Windows cell. For documentation about installing the PAS for Windows tile, see the [Installing and Configuring PAS for Windows](#) topic. Developers can push both [OWIN](#) and non-OWIN apps, and can push apps that are served by [Hostable Web Core](#) or [self-hosted](#).

Operators must also install the Cloud Foundry Command Line Interface (cf CLI) to run the commands on this topic. For information about installing the cf CLI, see the [Installing the cf CLI](#) topic.

If you have upgraded to PAS for Windows and have apps that you want to migrate, see the [Upgrading Cells](#) topic.

## Develop .NET Apps

### .NET on PCF Cookbook

The [.NET Cookbook](#) has useful tips and recipes for developing .NET apps to run on PAS for Windows.

## Push a .NET App

By default, PCF serves .NET apps with Hostable Web Core (HWC). HWC is a lighter version of the Internet Information Services (IIS) server that contains the core IIS functionality.

Perform the following steps to push a .NET app to a Windows cell:

1. Run `cf api api.YOUR-SYSTEM-DOMAIN` to target the Cloud Controller of your PCF deployment:

```
$ cf api api.YOUR-SYSTEM-DOMAIN
```

2. Run one of the following commands to deploy your .NET app, replacing `APP-NAME` with the name of your app.

- If you want to deploy a .NET Framework app, run `cf push APP-NAME -s windows2016 -b hwc_buildpack`:

```
$ cf push APP-NAME -s windows2016 -b hwc_buildpack
```

- If you want to deploy an app with `.bat` or `.exe` files, run `cf push -s windows2016 -b binary_buildpack`:

```
$ cf push -s windows2016 -b binary_buildpack
```

The `-s windows2016` option instructs PCF to run the app in the Windows cell. If you are not pushing your app from its directory, use the `-p` option and specify the path to the directory that contains the app.

3. Wait for your app to stage and start. If you see an error message, refer to the [Troubleshoot App Errors](#) section of this topic.

## Context Path Routing Support for ASP.NET Apps



ASP.NET developers can host applications under a route path. Within Windows cells, you can have multiple routes to an app, but those routes cannot have different context paths.

For example, if you would like to route `APP-NAME-TWO` under `APP-NAME-ONE`, in order to create the `APP-NAME-ONE.example-domain.com/APP-NAME-TWO` path:

1. Run `cf push APP-NAME-ONE` to push the primary app.

```
$ cf push APP-NAME-ONE
```

2. Run `cf push APP-NAME-TWO --hostname APP-NAME-ONE --route-path APP-NAME-TWO` to map the route of the secondary app under the primary app.

```
$ cf push APP-NAME-TWO --hostname APP-NAME-ONE --route-path APP-NAME-TWO
```

If you need to use a non-default domain, add the domain option (`-d`) followed by your chosen domain address to the `cf-push` command from Step 2.

## Push a Self-Hosted App

Developers can choose to push a self-hosted app instead of using Hostable Web Core. Self-hosted apps combine server code with the app code.

Perform the following steps to push a self-hosted app:

1. Run `cf api api.YOUR-SYSTEM-DOMAIN` to target the Cloud Controller of your PCF deployment:

```
$ cf api api.YOUR-SYSTEM-DOMAIN
```

2. Run `cf push APP-NAME -s windows2016 -b binary_buildpack -c PATH-TO-BINARY` to push your .NET app from the app root. Replace `APP-NAME` with the name of your app and `PATH-TO-BINARY` with the path to your executable.

```
$ cf push APP-NAME -s windows2016 -b binary_buildpack -c PATH-TO-BINARY
```

3. Wait for your app to stage and start. If you see an error message, refer to the [Troubleshoot App Errors](#) section of this topic.

## Push a SOAP Service

Developers can push Simple Object Access Protocol (SOAP) web services to their PCF deployment by following the procedures in the sections below.

### Step 1: Deploy Your Web Service

Perform the following steps to deploy a SOAP web service:

1. Develop the service as an ASMX web service in Microsoft Visual Studio.
2. Publish the service to your local file system.
3. Run `cf push SERVICE-NAME -s windows2016 -b hwc_buildpack -u none` to push your service from the directory containing the published web service. Replace `SERVICE-NAME` with the name of your service:

```
$ cf push SERVICE-NAME -s windows2016 -b hwc_buildpack -u none
```

The push command must include the `-s` flag to specify the stack as `windows2016`, which instructs PCF to run the app in the Windows cell.

The push command can include the following optional flags:

- If you are not pushing your service from the directory containing the published web service, use the `-p` flag to specify the path to the directory that contains the published web service.
- If you do not have a route serving `/`, use the `-u none` flag to disable the health check.

4. Locate the section of the terminal output that displays the URL of the web service:

```
requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: YOUR-WEB-SERVICE.YOUR-DOMAIN
last uploaded: Thu Nov 17 19:18:19 UTC 2016
stack: windows2016
buildpack: hwc_buildpack
```

## Step 2: Modify the WSDL File

Your SOAP web service is now deployed on PCF, but the service's WSDL file contains the incorrect port information. Before an application can consume your web service, either you or the application developer must modify the WSDL file.

Examine the following portion of an example WSDL file:

```
<?xml version='1.0' encoding='utf-8'>
<wsdl:service name="WebService1">
 <wsdl:port name="WebService1Soap" binding="tns:WebService1Soap">
 <soap:address location="http://webservice.example.com:62492/WebService1.asmx"/>
 </wsdl:port>
 <wsdl:port name="WebService1Soap12" binding="tns:WebService1Soap12">
 <soap12:address location="http://webservice.example.com:62492/WebService1.asmx"/>
 </wsdl:port>
</wsdl:service>
```

The WSDL file provides the port number for the SOAP web service as `62492`. This is the port that the web service listens on in the [Garden container](#), but external applications cannot access the service on this port. Instead, external applications must use port `80`, and the [Gorouter](#) routes requests to the web service in the container.

The URL of the web service in the WSDL file must be modified to remove `62492`. With no port number, the URL defaults to port `80`. In the example above, the modified URL would be `http://webservice.example.com/WebService1.asmx`.

SOAP web service developers can resolve this problem in one of two ways:

- Modify the WSDL file by following the instructions in [Modify a Web Service's WSDL Using a SoapExtensionReflector](#) from the Microsoft Developers Network.
- Instruct the developers of external applications that consume the web service to perform the steps in the [Consume the SOAP Web Service](#) section of this topic.

## Consume the SOAP Web Service

Developers of external applications that consume the SOAP web service can perform the following steps to use a modified version of the WSDL file:

1. In a browser, navigate to the WSDL file of the web service.

You can reach the WSDL of your web service by constructing the URL as follows: `YOUR-WEB-SERVICE.YOUR-DOMAIN/ASMX-FILE.asmx?wsdl`

See the following URL as an example: `https://webservice.example.com/WebService1.asmx?wsdl`

2. Download the WSDL file to your local machine.
3. Edit the WSDL file to eliminate the container port, as described in the [Modify the WSDL File](#) section of this topic.
4. In Microsoft Visual Studio, right-click on your application in the **Solution Explorer** and select **Add > Service Reference**.
5. Under **Address**, enter the local path to the modified WSDL file. For example, `C:\Users\example\wsdl.xml`.
6. Click **OK**. Microsoft Visual Studio generates a client from the WSDL file that you can use in your codebase.

## Context Path Routing Support for SOAP Web Services

Developers can push SOAP web services to their PCF deployment with context path routing. For more information, see the [Context Path Routing Support for ASP.NET Apps](#) section.

## Troubleshoot App Errors

If a .NET app fails to start, consult the following list of errors and their possible solutions:

- `NoCompatibleCell`: Your PCF deployment cannot connect to your Windows cell. See the [Troubleshooting Windows Cells](#) topic for information about troubleshooting your Windows cell configuration.
- `Start unsuccessful`: Your app may not contain the required DLL files and dependencies. Ensure that you are pushing from a directory containing your app dependencies, or specify the directory with the `-p` flag. Your app also may be misconfigured. Ensure that your app directory contains either a valid `.exe` binary or a valid `Web.config` file.

## Java Buildpack

You can use the Java buildpack with apps written in Grails, Play, Spring, or any other JVM-based language or framework.

See the following topics for more information:

- [Tips for Java Developers](#)
- [Getting Started Deploying Apps](#)
- [Configuring Service Connections](#)
- [Cloud Foundry Java Client Library](#)

See the [Java Buildpack Release Notes](#) for information about specific versions. You can find the source for the Java buildpack in the [Java buildpack repository](#) on GitHub:

## Buildpack and Application Logging

The Java buildpack only runs during the staging process, and therefore only logs staging information such as the downloaded components, configuration data, and work performed on your application by the buildpack.

The Java buildpack source documentation states the following:

- The Java buildpack logs all messages, regardless of severity, to `APP-DIRECTORY/java-buildpack.log`. The buildpack also logs messages to `$stderr`, filtered by a configured severity level.
- If the buildpack fails with an exception, the exception message is logged with a log level of `ERROR`. The exception stack trace is logged with a log level of `DEBUG`. This prevents users from seeing stack traces by default.

Once staging completes, the buildpack stops logging. The Loggregator handles application logging.

Your application must write to STDOUT or STDERR for its logs to be included in the Loggregator stream. For more information, see the [Application Logging in Cloud Foundry](#) topic.

## BOSH Custom Trusted Certificate Support

Versions 3.7 and later of the Java buildpack support BOSH-configured custom trusted certificates. For more information, see [Configuring Trusted Certificates](#) in the BOSH documentation.

The Java buildpack pulls the contents of `/etc/ssl/certs/ca-certificates.crt` and `$CF_INSTANCE_CERT/$CF_INSTANCE_KEY` by default.

The log output for Diego Instance Identity-based `KeyStore` appears as follows:

```
Adding System Key Manager
Adding Key Manager for /etc/cf-instance-credentials/instance.key and /etc/cf-instance-credentials/instance.crt
Start watching /etc/cf-instance-credentials/instance.crt
Start watching /etc/cf-instance-credentials/instance.key
Initialized KeyManager for /etc/cf-instance-credentials/instance.key and /etc/cf-instance-credentials/instance.crt
```

The log output for Diego Trusted Certificate-based `TrustStore` appears as follows:

```
Adding System Trust Manager
Adding TrustManager for /etc/ssl/certs/ca-certificates.crt
Start watching /etc/ssl/certs/ca-certificates.crt
Initialized TrustManager for /etc/ssl/certs/ca-certificates.crt
```

## Memory Constraints in Java Buildpack 4.0

The memory calculator in Java buildpack 4.0 accounts for the following memory regions:

- `-Xmx`: Heap
- `-XX:MaxMetaspaceSize`: Metaspace

- `-Xss` : Thread Stacks
- `-XX:MaxDirectMemorySize` : Direct Memory
- `-XX:ReservedCodeCacheSize` : Code Cache
- `-XX:CompressedClassSpaceSize` : Compressed Class Space

Applications which previously ran in 512 MB or smaller containers may no longer be able to. Most applications will run if they use the Cloud Foundry default container size of 1 G without any modifications. However, you can configure those memory regions directly as needed.

The Java buildpack optimizes for all non-heap memory regions first and leaves the remainder for the heap.

The Java buildpack prints a histogram of the heap to the logs when the JVM encounters a terminal failure.

The Cloud Foundry default Java buildpack is currently 3.x to allows time for apps to be upgrade to 4.x.

For more information, see [Java buildpack 4.0](#).

## Tips for Java Developers

Page last updated:

Cloud Foundry can deploy a number of different JVM-based artifact types. For a more detailed explanation of what it supports, see the [Java Buildpack documentation](#).

## Java Buildpack

For detailed information about using, configuring, and extending the Cloud Foundry Java buildpack, see [Java Buildpack documentation](#).

## Design

The Java Buildpack is designed to convert artifacts that run on the JVM into executable applications. It does this by identifying one of the supported artifact types (Grails, Groovy, Java, Play Framework, Spring Boot, and Servlet) and downloading all additional dependencies needed to run. The collection of services bound to the application is also analyzed and any dependencies related to those services are also downloaded.

As an example, pushing a WAR file that is bound to a PostgreSQL database and New Relic for performance monitoring would result in the following:

```
Initialized empty Git repository in /tmp/buildpacks/java-buildpack/.git/
--> Java Buildpack source: https://github.com/cloudfoundry/java-buildpack#0928916a2dd78e9fa9469c558046cef09f60e5d
--> Downloading Open Jdk JRE 1.7.0_51 from
 http://.../openjdk/lucid/x86_64/openjdk-1.7.0_51.tar.gz (0.0s)
 Expanding Open Jdk JRE to .java-buildpack/open_jdk_jre (1.9s)
--> Downloading New Relic Agent 3.4.1 from
 http://.../new-relic/new-relic-3.4.1.jar (0.4s)
--> Downloading PostgreSQL JDBC 9.3.1100 from
 http://.../postgresql-jdbc/postgresql-jdbc-9.3.1100.jar (0.0s)
--> Downloading Spring Auto Reconfiguration 0.8.7 from
 http://.../auto-reconfiguration/auto-reconfiguration-0.8.7.jar (0.0s)
 Modifying /WEB-INF/web.xml for Auto Reconfiguration
--> Downloading Tomcat 7.0.50 from
 http://.../tomcat/tomcat-7.0.50.tar.gz (0.0s)
 Expanding Tomcat to .java-buildpack/tomcat (0.1s)
--> Downloading Buildpack Tomcat Support 1.1.1 from
 http://.../tomcat-buildpack-support/tomcat-buildpack-support-1.1.1.jar (0.1s)
--> Uploading droplet (57M)
```

## Configuration

In most cases, the buildpack should work without any configuration. If you are new to Cloud Foundry, we recommend that you make your first attempts without modifying the buildpack configuration. If the buildpack requires some configuration, use [a fork of the buildpack](#).

## Java Client Library

The Cloud Foundry Client Library provides a Java API for interacting with a Cloud Foundry instance. This library, `cloudfoundry-client-lib`, is used by the Cloud Foundry Maven plugin, the Cloud Foundry Gradle plugin, and other Java-based tools.

For information about using this library, see the [Java Cloud Foundry Library](#) page.

## Grails

Grails packages applications into WAR files for deployment into a Servlet container. To build the WAR file and deploy it, run the following:

```
$ grails prod war
$ cf push my-application -p target/my-application-version.war
```

## Groovy

Groovy applications based on both [Ratpack](#) and a simple collection of files are supported.

## Ratpack

Ratpack packages applications into two different styles; Cloud Foundry supports the `distZip` style. To build the ZIP and deploy it, run the following:

```
$ gradle distZip
$ cf push my-application -p build/distributions/my-application.zip
```

## Raw Groovy

Groovy applications that are made up of a [single entry point](#) plus any supporting files can be run without any other work. To deploy them, run the following:

```
$ cf push my-application
```

## Java Main

Java applications with a `main()` method can be run provided that they are packaged as [self-executable JARs](#).

**Note:** If your application is not web-enabled, you must suppress route creation to avoid a “failed to start accepting connections” error. To suppress route creation, add `no-route: true` to the application manifest or use the `--no-route` flag with the `cf push` command.

For more information about the `no-route` attribute, see the [Deploying with Application Manifests](#) topic.

## Maven

A Maven build can create a self-executable JAR. To build and deploy the JAR, run the following:

```
$ mvn package
$ cf push my-application -p target/my-application-version.jar
```

## Gradle

A Gradle build can create a self-executable JAR. To build and deploy the JAR, run the following:

```
$ gradle build
$ cf push my-application -p build/libs/my-application-version.jar
```

## Play Framework

The [Play Framework](#) packages applications into two different styles. Cloud Foundry supports both the `staged` and `dist` styles. To build the `dist` style and deploy it, run the following:

```
$ play dist
$ cf push my-application -p target/universal/my-application-version.zip
```

## Spring Boot CLI

[Spring Boot](#) can run applications [comprised entirely of POGOs](#). To deploy then, run the following:

```
$ spring grab *.groovy
$ cf push my-application
```

## Servlet

Java applications can be packaged as Servlet applications.

## Maven

A Maven build can create a Servlet WAR. To build and deploy the WAR, run the following:

```
$ mvn package
$ cf push my-application -p target/my-application-version.war
```

## Gradle

A Gradle build can create a Servlet WAR. To build and deploy the JAR, run the following:

```
$ gradle build
$ cf push my-application -p build/libs/my-application-version.war
```

## Binding to Services

Information about binding apps to services can be found on the following pages:

- [Service Bindings for Grails Applications](#)
- [Service Bindings for Play Framework Applications](#)
- [Service Bindings for Spring Applications](#)

## Java and Grails Best Practices

### Provide JDBC driver

The Java buildpack does not bundle a JDBC driver with your application. If your application will access a SQL RDBMS, include the appropriate driver in your application.

### Allocate Sufficient Memory

If you do not allocate sufficient memory to a Java application when you deploy it, it may fail to start, or PAS may terminate it. You must allocate enough memory to allow for the following:

- Java heap
- Metaspace, if using Java 8
- PermGen, if using Java 7 or earlier
- Stack size per Thread



- JVM overhead

The `config/open_jdk_jre.yml` file of the [Cloud Foundry Java buildpack](#) contains default memory size and weighting settings for the JRE. See the [Open JDK JRE README](#) on GitHub for an explanation of JRE memory sizes and weightings and how the Java buildpack calculates and allocates memory to the JRE for your app.

To configure memory-related JRE options for your app, you either create a custom buildpack and specify this buildpack in your deployment manifest or you override the default memory settings of your buildpack as described in the <https://github.com/cloudfoundry/java-buildpack#configuration-and-extension> with the properties listed in the [Open JDK JRE README](#). For more information about configuring custom buildpacks and manifests, refer to the [Custom Buildpacks](#) and [Deploying with Application Manifests](#) topics.

When your app is running, you can use the `cf app APP-NAME` command to see memory utilization.

## Troubleshoot Out Of Memory

A Java app may crash because of insufficient memory on the Garden container or the JVM on which it runs. See the following sections for help diagnosing and resolving such issues.


### JVM

- **Error:** `java.lang.OutOfMemoryError`. See the following example:

```
$ cf logs APP-NAME --recent
2016-06-20T09:18:51.00+0100 [APP/0] OUT java.lang.OutOfMemoryError: Metaspace
```

- **Cause:** If the JVM cannot garbage-collect enough space to ensure the allocation of a data-structure, it fails with [java.lang.OutOfMemoryError](#). In the example above, JVM has an under-sized `metaspace`. You may see failures in other memory pools, such as `heap`.
- **Solution:** Configure the JVM correctly for your app. See [Allocate Sufficient Memory](#).

### Garden Container

 **Note:** The solutions in this section require configuring the memory calculator, which is a sub-project of the CF Java buildpack that calculates suitable memory settings for Java apps when you push them. See the [java-buildpack-memory-calculator](#) repository for more information. If you have questions about the memory calculator, you can ask them in the [#java-buildpack](#) channel of the [Cloud Foundry Slack organization](#).

- **Error:** The Garden container terminates the Java process with the `out of memory` event. See the following example:

```
$ cf events APP-NAME
time event actor description
2016-06-20T09:18:51.00+0100 app.crash app-name index: 0, reason: CRASHED, exit_description: out of memory, exit_status: 255
```

This error appears when the JVM allocates more OS-level memory than the quota requested by the app, such as [through the manifest](#).

- **Cause 1 - Insufficient native memory:** This error commonly means that the JVM requires more `native` memory. In the scope of the Java buildpack and the memory calculator, the term `native` means the memory required for the JVM to work, along with forms of memory not covered in the other classifications of the memory calculator. This includes the memory footprint of OS-level threads, [direct NIO buffers](#), code cache, program counters, and others.
- **Solution 1:** Determine how much `native` memory a Java app needs by [measuring it](#) with realistic workloads and fine-tuning it accordingly. You can then configure the Java buildpack using the `native` [setting](#) of the memory calculator, as in the example below:

```

applications:
- name: app-name
 memory: 1G
 env:
 JBP_CONFIG_OPEN_JDK_JRE: '{memory_calculator: {memory_sizes: {native: 150m}}}'
```

This example shows that `150m` of the overall available `1G` is reserved for anything that is not `heap`, `metaspace`, or `permgen`. In less common cases, this may come from companion processes started by the JVM, such as the [Process API](#).

- **Cause 2 - High thread count:** Java threads in the JVM can cause memory errors at the Garden level. When an app is under heavy load, it uses a high number of threads and consumes a significant amount of memory.

- **Solution 2:** Set the reserved memory for stack traces to the correct value for your app.

You can use the `stack` [setting](#) of the memory calculator to configure the amount of space the JVM reserves for each Java thread. You must multiply this value by the number of threads your app requires. Specify the number of threads in the `stack_threads` [setting](#) of the memory calculator. For example, if you estimate the max thread count for an app at `800` and the amount of memory needed to represent the deepest stacktrace of a Java thread is `512KB`, configure the memory calculator as follows:

```

applications:
- name: app-name
 memory: 1G
 env:
 JBP_CONFIG_OPEN_JDK_JRE: '[memory_calculator: {stack_threads: 800, memory_sizes: {stack: 512k}}]'
```

In this example, the overall memory amount reserved by the JVM for representing the stacks of Java threads is `800 * 512k = 400m`.

The correct settings for `stack` and `stack_threads` depend on your app code, including the libraries it uses. Your app may technically have no upper limit, such as in the case of [cavalier usage](#) of `CachedThreadPool` [executors](#). However, you still must calculate the depth of the thread stacks and the amount of space the JVM should reserve for each of them.

## Troubleshoot Failed Upload

If your application fails to upload when you push it to Cloud Foundry, it may be for one of the following reasons:

- **WAR is too large:** An upload may fail due to the size of the WAR file. Cloud Foundry testing indicates WAR files as large as 250 MB upload successfully. If a WAR file larger than that fails to upload, it may be a result of the file size.
- **Connection issues:** Application uploads can fail if you have a slow Internet connection, or if you upload from a location that is very remote from the target Cloud Foundry instance. If an application upload takes a long time, your authorization token can expire before the upload completes. A workaround is to copy the WAR to a server that is closer to the Cloud Foundry instance, and push it from there.
- **Out-of-date cf CLI client:** Upload of a large WAR is faster and hence less likely to fail if you are using a recent version of the cf CLI. If you are using an older version of the cf CLI client to upload a large WAR, and having problems, try updating to the latest version of the cf CLI.
- **Incorrect WAR targeting:** By default, `cf push` uploads everything in the current directory. For a Java application, `cf push` with no option flags uploads source code and other unnecessary files, in addition to the WAR. When you push a Java application, specify the path to the WAR:

```
$ cf push MY-APP -p PATH/TO/WAR-FILE
```

You can determine whether or not the path was specified for a previously pushed application by examining the application deployment manifest, `manifest.yml`. If the `path` attribute specifies the current directory, the manifest includes a line like the following:

```
path: .
```

To re-push just the WAR, do one of the following:

- Delete `manifest.yml` and run `cf push` again, specifying the location of the WAR using the `-p` flag.
- Edit the `path` argument in `manifest.yml` to point to the WAR, and re-push the application.

## Debug Java Apps on Cloud Foundry

Because of the way that Cloud Foundry deploys your applications and isolates them, it is not possible to connect to your application with the remote Java debugger. Instead, instruct the application to connect to the Java debugger on your local machine.

Here are the instructions for setting up remote debugging when using BOSH Lite or a Cloud Foundry installation.

1. Open your project in Eclipse.
2. Right-click on your project, go to **Debug as** and pick **Debug Configurations**.
3. Create a new **Remote Java Application**.
4. Make sure your project is selected, pick **Standard (Socket Listen)** from the **Connection Type** drop down and set a port. Make sure this port is open if you are running a firewall.
5. Click **Debug**.

The debugger should now be running. If you switch to the Debug perspective, you should see your application listed in the Debug panel and it should say

```
Waiting for vm to connect at
port
```

Next, push your application to Cloud Foundry and instruct Cloud Foundry to connect to the debugger running on your local machine using the following instructions:

1. Edit your `manifest.yml` file. Set the instances count to 1. If you set this greater than one, multiple applications try to connect to your debugger.
2. Also in `manifest.yml`, add the `env` section and create a variable called `JAVA_OPTS`.
3. Add the remote debugger configuration to the `JAVA_OPTS` variable:  

```
-agentlib:jdwp=transport=dt_socket,address=YOUR-IP-ADDRESS:YOUR-PORT
```
4. Save the `manifest.yml` file.
5. Run `cf push`.

Upon completion, you should see that your application has started and is now connected to the debugger running in your IDE. You can now add breakpoints and interrogate the application just as you would if it were running locally.

## Slow Starting Java or Grails Apps

Some Java and Grails applications do not start quickly, and the health check for an application can fail if an application starts too slowly.

The current Java buildpack implementation sets the Tomcat `bindOnInit` property to `false`. This prevents Tomcat from listening for HTTP requests until an application has fully deployed.

If your application does not start quickly, the health check may fail because it checks the health of the application before the application can accept requests. By default, the health check fails after a timeout threshold of 60 seconds.

To resolve this issue, use `cf push APP-NAME` with the `-t TIMEOUT-THRESHOLD` option to increase the timeout threshold. Specify `TIMEOUT-THRESHOLD` in seconds.

```
$ cf push my-app -t 180
```



**Note:** The timeout threshold cannot exceed 180 seconds. Specifying a timeout threshold greater than 180 seconds results in the following error:

```
Server error, status code: 400, error code: 100001, message: The app is invalid: health_check_timeout
maximum_exceeded
```

## Extension

The Java Buildpack is also designed to be easily extended. It creates abstractions for [three types of components](#) (containers, frameworks, and JREs) in order to allow users to easily add functionality. In addition to these abstractions, there are a number of [utility classes](#) for simplifying typical buildpack behaviors.

As an example, the New Relic framework looks like the following:

```
class NewRelicAgent < JavaBuildpack::Component::VersionedDependencyComponent

 # @macro base_component_compile
 def compile
 FileUtils.mkdir_p logs_dir

 download_jar
 @droplet.copy_resources
 end

 # @macro base_component_release
 def release
 @droplet.java_opts
 .add_javaagent(@droplet.sandbox + jar_name)
 .add_system_property('newrelic.home', @droplet.sandbox)
 .add_system_property('newrelic.config.license_key', license_key)
 .add_system_property('newrelic.config.app_name', "#{application_name}")
 .add_system_property('newrelic.config.log_file_path', logs_dir)
 end

 protected

 # @macro versioned_dependency_component_supports
 def supports?
 @application.services.one_service? FILTER, 'licenseKey'
 end

 private

 FILTER = /newrelic/.freeze

 def application_name
 @application.details['application_name']
 end

 def license_key
 @application.services.find_service(FILTER)['credentials']['licenseKey']
 end

 def logs_dir
 @droplet.sandbox + 'logs'
 end

end
```

## Environment Variables

You can access environments variable programmatically.

For example, you can obtain `VCAP_SERVICES` as follows:

```
System.getenv("VCAP_SERVICES");
```

See the [Cloud Foundry Environment Variables](#) topic for more information.

## Getting Started Deploying Java Apps

Page last updated:

This topic provides links to additional information about getting started deploying apps using the Java buildpack. See the following topics for deployment guides specific to your app framework:

- [Grails](#)
- [Ratpack](#)
- [Spring](#)

## Getting Started Deploying Grails Apps

Page last updated:

This guide is intended to walk you through deploying a Grails app to Pivotal Application Service. If you experience a problem following the steps below, refer to the [Known Issues](#) or [Troubleshooting Application Deployment and Health](#) topics for more information.

### Sample App Step

If you want to go through this tutorial using the sample app, run `git clone https://github.com/cloudfoundry-samples/pong_matcher_grails.git` to clone the `pong_matcher_grails` app from GitHub, and follow the instructions in the Sample App Step sections.



**Note:** Ensure that your Grails app runs locally before continuing with this procedure.

## Deploy a Grails Application

This section describes how to deploy a Grails application to PAS.

### Prerequisites

- A Grails app that runs locally on your workstation
- Intermediate to advanced Grails knowledge
- The [Cloud Foundry Command Line Interface \(cf CLI\)](#)
- JDK 1.7 or 1.8 for Java 7 or 8 configured on your workstation



**Note:** You can develop Grails applications in Groovy, Java 7 or 8, or any JVM language. The Cloud Foundry Java buildpack uses JDK 1.8, but you can modify the buildpack and the manifest for your app to compile to JDK 1.7 as described in *Step 8: Configure the Deployment Manifest* of this topic.

## Step 1: Declare App Dependencies

Declare all the dependency tasks for your app in the build script of your chosen build tool. The table lists build script information for Gradle, Grails, and Maven, and provides documentation links for each build tool.

| Build Tool | Build Script                    | Documentation                                                   |
|------------|---------------------------------|-----------------------------------------------------------------|
| Gradle     | <code>build.gradle</code>       | <a href="#">Gradle User Guide</a>                               |
| Grails     | <code>BuildConfig.groovy</code> | <a href="#">Grails: Configuration - Reference Documentation</a> |
| Maven      | <code>pom.xml</code>            | <a href="#">Apache Maven Project Documentation</a>              |

### Sample App Step

You can skip this step. The `pong_matcher_grails/app/grails-app/conf/BuildConfig.groovy` file contains the dependencies for the `pong_matcher_grails` sample app, as the example below shows.

```
dependencies {
 // specify dependencies here under either 'build', 'compile', 'runtime', 'test' or 'provided' scopes e.g.
 // runtime 'mysql:mysql-connector-java:5.1.29'
 // runtime 'org.postgresql:postgresql:9.3-1101-jdbc41'
 test "org.grails:grails-datastore-test-support:1.0-grails-2.4"
 runtime 'mysql:mysql-connector-java:5.1.33'
}
```

## Step 2: Allocate Sufficient Memory

Run the Cloud Foundry Command Line Interface (cf CLI) `cf push -m` command to specify the amount of memory that should be allocated to the application. Memory allocated this way is done in preset amounts of `64M`, `128M`, `256M`, `512M`, `1G`, or `2G`. For example:

```
$ cf push -m 128M
```

When your app is running, you can use the `cf app APP-NAME` command to see memory utilization.

### Sample App Step

You can skip this step. In the `manifest.yml` of the `pong_matcher_grails` sample app, the `memory` sub-block of the `applications` block allocates 1 GB to the app.

## Step 3: Provide a JDBC Driver

The Java buildpack does not bundle a JDBC driver with your application. If your application accesses a SQL RDBMS, you must do the following:

- Include the appropriate driver in your application.
- Create a dependency task for the driver in the build script for your build tool or IDE.

### Sample App Step

You can skip this step. The `pong_matcher_grails` sample app declares a MySQL JDBC driver in the `pong_matcher_grails/app/grails-app/conf/DataSource.groovy` file because the app uses ClearDB, which is a database-as-service for MySQL-powered apps. The example below shows this declaration.

```
dataSource {
 pooled = true
 jmxExport = true
 driverClassName = "com.mysql.jdbc.Driver"
 dialect = org.hibernate.dialect.MySQL5InnoDBDialect
 uri = new URI(System.env.DATABASE_URL ?: "mysql://foo:bar@localhost")
 username = uri.userInfo ? uri.userInfo.split(":")[0] : ""
 password = uri.userInfo ? uri.userInfo.split(":")[1] : ""
 url = "jdbc:mysql://"+ uri.host + uri.path

 properties {
 dbProperties {
 autoReconnect = true
 }
 }
}
```

## Step 4: (Optional) Configure a Procfile

Use a Procfile to declare required runtime processes for your web app and to specify your web server. For more information, see the [Configuring a Production Server](#) topic.

### Sample App Step

You can skip this step. The `pong_matcher_grails` app does not require a Procfile.

## Step 5: Create and Bind a Service Instance for a Grails Application

This section describes using the cf CLI to configure a ClearDB managed service instance for an app. You can use either the CLI or [Apps Manager](#) to perform this task.

PAS supports two types of service instances:

- Managed services integrate with PAS through service brokers that offer services and plans and manage the service calls between PAS and a service provider.
- User-provided service instances enable you to connect your application to pre-provisioned external service instances.

For more information about creating and using service instances, refer to the [Services Overview](#) topic.

## Create a Service Instance

Run the cf CLI `cf marketplace` command to view managed and user-provided services and plans available to you.

The example shows two of the available managed database-as-a-service providers and their offered plans: `cleardb` database-as-a-service for MySQL-powered apps and `postgresql-10-odb` PostgreSQL as a Service.

```
$ cf marketplace
Getting services from marketplace in org Cloud-Apps / space development as clouduser@example.com...
OK

service plans description
cleardb spark, boost, amp Highly available MySQL for your apps
postgresql-10-odb standalone, standalone-replica, general PostgreSQL as a Service
```

Run `cf create-service SERVICE PLAN SERVICE-INSTANCE` to create a service instance for your app. Choose a SERVICE and PLAN from the list, and provide a unique name for the SERVICE-INSTANCE.

### Sample App Step

Run `cf create-service cleardb spark mysql`. This creates a service instance named `mysql` that uses the `cleardb` service and the `spark` plan, as the example below shows.

```
$ cf create-service cleardb spark mysql
Creating service mysql in org Cloud-Apps / space development as clouduser@example.com....
OK
```

## Bind a Service Instance

When you bind an app to a service instance, PAS writes information about the service instance to the VCAP\_SERVICES app environment variable. The app can use this information to integrate with the service instance.

Most services support bindable service instances. Refer to your service provider's documentation to confirm if they support this functionality.

You can bind a service to an application with the command `cf bind-service APPLICATION SERVICE-INSTANCE`.

Alternately, you can configure the deployment manifest file by adding a `services` sub-block to the `applications` block and specifying the service instance. For more information and an example on service binding using a manifest, see the Sample App step.

You can also bind a service using the [Apps Manager](#).

### Sample App Step

You can skip this step because the service instance is already bound. Open the `manifest.yml` file in a text editor to view the bound service instance information. Locate the file in the app root directory and search for the `services` sub-block in the `applications` block, as the example below shows.

```

applications:
```



```
...
services:
 - mysql
```

## Step 6: Configure the Deployment Manifest

You can specify deployment options in the `manifest.yml` that the `cf push` command uses when deploying your app.

Refer to the [Deploying with Application Manifests](#) topic for more information.

### Sample App Step

You can skip this step. The `manifest.yml` file for the `pong_matcher_grails` sample app does not require any additional configuration to deploy the app.


## Step 7: Log in and Target the API Endpoint

Run `cf login -a API-ENDPOINT`, enter your login credentials, and select a space and org. The API endpoint is [the URL of the Cloud Controller in your PAS instance](#).


### Sample App Step

You must do this step to run the sample app.

## Step 8: Deploy the Application

 **Note:** You must use the cf CLI to deploy apps.

From the root directory of your application, run `cf push APP-NAME -p PATH-TO-FILE.war` to deploy your application.

 **Note:** You must deploy the `.war` artifact for a Grails app, and you must include the path to the `.war` file in the `cf push` command using the `-p` option if you do not declare the path in the `applications` block of the manifest file. For more information, refer to the [Grails section](#) in the Tips for Java Developers topic.

`cf push APP-NAME` creates a URL route to your application in the form `HOST.DOMAIN`, where `HOST` is your `APP-NAME` and `DOMAIN` is specified by your administrator. Your `DOMAIN` is `shared-domain.example.com`. For example: `cf push my-app` creates the URL `my-app.shared-domain.example.com`.

The URL for your app must be unique from other apps that PAS hosts or the push will fail. Use the following options to help create a unique URL:

- `-n` to assign a different HOST name for the app
- `--random-route` to create a URL that includes the app name and random words
- `cf help push` to view other options for this command


If you want to view log activity while the app deploys, launch a new terminal window and run `cf logs APP-NAME`.

Once your app deploys, browse to your app URL. Search for the `urls` field in the `App started` block in the output of the `cf push` command. Use the URL to access your app online.

### Sample App Step

1. Change to the `app` directory, and run `./grails war` to build the app.
2. Run `cf push pong_matcher_grails -n HOST-NAME` to push the app.

Example: `cf push pong_matcher_grails -n my-grails-app`

 **Note:** You do not have to include the `-p` flag when you deploy the sample app. The sample app manifest declares the path to the archive that `cf push` uses to upload the app files.

The example below shows the terminal output of deploying the `pong_matcher_grails` app. `cf push` uses the instructions in the manifest file to create the app, create and bind the route, and upload the app. It then binds the app to the `mysql` service and follows the instructions in the manifest to start two instances of the app, allocating 1 GB of memory between the instances. After the instances start, the output displays their health and status.

```
$ cf push pong_matcher_grails -n my-grails-app
Using manifest file /Users/example/workspace/pong_matcher_grails/app/manifest.yml

Creating app pong_matcher_grails in org Cloud-Apps / space development as clouduser@example.com...
OK

Creating route my-grails-app.cfapps.io...
OK

Binding my-grails-app.cfapps.io to pong_matcher_grails...
OK

Uploading pong_matcher_grails...
Uploading app files from: /Users/example/workspace/pong_matcher_grails/app/target/pong_matcher_grails-0.1.war
Uploading 4.8M, 704 files
OK
Binding service mysql to app pong_matcher_grails in org Cloud-Apps / space development as clouduser@example.com...
OK

Starting app pong_matcher_grails in org Cloud-Apps / space development as clouduser@example.com...
OK
-----> Downloaded app package (38M)
-----&; Java Buildpack Version: v2.5 | https://github.com/cloudfoundry/java-buildpack.git#840500e
-----> Downloading Open Jdk JRE 1.8.0_25 from https://download.run.pivotal.io/openjdk/lucid/x86_64/openjdk-1.8.0_25.tar.gz (1.5s)
 Expanding Open Jdk JRE to .java-buildpack/open_jdk_jre (1.1s)
-----> Downloading Spring Auto Reconfiguration 1.5.0_RELEASE from https://download.run.pivotal.io/auto-reconfiguration/auto-reconfiguration-1.5.0_RELEASE.jar (0.0s)
 Modifying /WEB-INF/web.xml for Auto Reconfiguration
-----> Downloading Tomcat Instance 8.0.14 from https://download.run.pivotal.io/tomcat/tomcat-8.0.14.tar.gz (0.4s)
 Expanding Tomcat to .java-buildpack/tomcat (0.1s)
-----> Downloading Tomcat Lifecycle Support 2.4.0_RELEASE from https://download.run.pivotal.io/tomcat-lifecycle-support/tomcat-lifecycle-support-2.4.0_RELEASE.jar (0.0s)
-----> Downloading Tomcat Logging Support 2.4.0_RELEASE from https://download.run.pivotal.io/tomcat-logging-support/tomcat-logging-support-2.4.0_RELEASE.jar (0.0s)
-----> Downloading Tomcat Access Logging Support 2.4.0_RELEASE from https://download.run.pivotal.io/tomcat-access-logging-support/tomcat-access-logging-support-2.4.0_RELEASE.jar (0.0s)

-----> Uploading droplet (83M)

0 of 2 instances running, 2 starting
0 of 2 instances running, 2 starting
0 of 2 instances running, 2 starting
2 of 2 instances running

App started

Showing health and status for app pong_matcher_grails in org Cloud-Apps / space development as clouduser@example.com...
OK

requested state: started
instances: 2/2
usage: 1G x 2 instances
urls: my-grails-app.cfapps.io

state since cpu memory disk
#0 running 2014-11-10 05:07:33 PM 0.0% 686.4M of 1G 153.6M of 1G
#1 running 2014-11-10 05:07:36 PM 0.0% 677.2M of 1G 153.6M of 1G
```

## Step 9: Test Your Deployed App

You've deployed an app to PAS!

Use the cf CLI or [Apps Manager](#) to review information and administer your app and your PAS account. For example, you can edit the `manifest.yml` to increase the number of app instances from 1 to 3, and redeploy the app with a new app name and host name.

See the [Manage Your Application with the cf CLI](#) section for more information. See also [Using the Apps Manager](#).

## Sample App Step

To test the sample app, do the following:

1. To export the test host, run `export HOST=SAMPLE-APP-URL`, substituting the URL for your app for `SAMPLE-APP-URL`.

2. To clear the database from any previous tests, run:

```
curl -v -X DELETE
$HOST/all
```

You should get a response of 200.

3. To request a match as “andrew”, run:

```
curl -v -H "Content-Type: application/json" -X PUT $HOST/match_requests/firstrequest -d '{"player":
"andrew"}'
```

You should again get a response of `200`.

4. To request a match as a different player, run:

```
curl -v -H "Content-Type: application/json" -X PUT $HOST/match_requests/secondrequest -d '{"player":
"navratilova"}'
```

5. To check the status of the first match request, run:

```
curl -v -X GET
$HOST/match_requests/firstrequest
```

The last line of the output shows the `match_id`.

6. Replace `MATCH_ID` with the `match_id` value from the previous step in the following command:

```
curl -v -H "Content-Type: application/json" -X POST $HOST/results -d ' { "match_id": "MATCH_ID", "winner": "andrew", "loser": "navratilova"
}'
```

You should receive a `201` response.

Created

## Manage Your Application with the cf CLI

Run `cf help` to view a complete list of commands, grouped by task categories, and run `cf help COMMAND` for detailed information about a specific

command. For more information about using the cf CLI, refer to the Cloud Foundry Command Line Interface (cf CLI) topics, especially the [Getting Started with cf CLI](#) topic.

**Note:** You cannot perform certain tasks in the CLI or [Apps Manager](#) because these are commands that only a PAS administrator can run. If you are not a PAS administrator, the following message displays for these types of commands:

```
error code: 10003, message: You are not authorized to perform the requested
action
```

For more information about specific Admin commands you can perform with

the Apps Manager, depending on your user role, refer to the [Getting Started with the Apps Manager](#) topic.

## Troubleshooting

If your application fails to start, verify that the application starts in your local environment. Refer to the [Troubleshooting Application Deployment and Health](#) topic to learn more about troubleshooting.

## App Deploy Fails

Even when the deploy fails, the app might exist on PAS. Run `cf apps` to review the apps in the currently targeted org and space. You might be able to correct the issue using the CLI or [Apps Manager](#), or you might have to delete the app and redeploy.

## App Requires a Unique URL

PAS requires that each app that you deploy have a unique URL. Otherwise, the new app URL collides with an existing app URL and PAS cannot successfully deploy the app. You can fix this issue by running `cf push` with either of the following flags to create a unique URL:

- `-n` to assign a different HOST name for the app.
- `--random-route` to create a URL that includes the app name and random words. Using this option might create a long URL, depending on the number of words that the app name includes.

## Getting Started Deploying Ratpack Apps

Page last updated:

This guide is intended to walk you through deploying a Ratpack app to Pivotal Application Service. If you experience a problem following the steps below, check the [Known Issues](#) topic or refer to the [Troubleshooting Application Deployment and Health](#) topic.

### Sample App Step

If you want to go through this tutorial using the sample app, run `git clone https://github.com/cloudfoundry-samples/pong_matcher_groovy.git` to clone the `pong_matcher_groovy` app from GitHub, and follow the instructions in the Sample App Step sections.



**Note:** Ensure that your Ratpack app runs locally before continuing with this procedure.

## Deploy a Ratpack Application

This section describes how to deploy a Ratpack application to PAS.

### Prerequisites

- A Ratpack app that runs locally on your workstation
- Intermediate to advanced Ratpack knowledge
- The [Cloud Foundry Command Line Interface \(cf CLI\)](#)
- JDK 1.7 or 1.8 for Java 7 or 8 configured on your workstation



**Note:** You can develop Ratpack applications in Java 7 or 8 or any JVM language. The Cloud Foundry Java buildpack uses JDK 1.8, but you can modify the buildpack and the manifest for your app to compile to JDK 1.7. Refer to Step 8: Configure the Deployment Manifest.

### Step 1: Declare App Dependencies

Declare all the dependency tasks for your app in the build script of your chosen build tool. The table lists build script information for Gradle and Maven and provides documentation links for each build tool.

| Build Tool | Build Script              | Documentation                                      |
|------------|---------------------------|----------------------------------------------------|
| Gradle     | <code>build.gradle</code> | <a href="#">Gradle User Guide</a>                  |
| Maven      | <code>pom.xml</code>      | <a href="#">Apache Maven Project Documentation</a> |

### Sample App Step

You can skip this step. The `build.gradle` file contains the dependencies for the `pong_matcher_groovy` sample app, as the example below shows.

```
dependencies {
 // SpringLoaded enables runtime hot reloading.
 // It is not part of the app runtime and is not shipped in the distribution.
 springloaded "org.springframework:springloaded:1.2.0.RELEASE"

 // Default SLF4J binding. Note that this is a blocking implementation.
 // See here for a non blocking appender http://logging.apache.org/log4j/2.x/manual/asnc.html
 runtime 'org.slf4j:slf4j-simple:1.7.7'

 compile group: 'redis.clients', name: 'jedis', version: '2.5.2', transitive: true

 testCompile "org.spockframework:spock-core:0.7-groovy-2.0"
}
```

## Step 2: Allocate Sufficient Memory

Use the `cf push -m` command to specify the amount of memory that should be allocated to the application. Memory allocated this way is done in preset amounts of `64M`, `128M`, `256M`, `512M`, `1G`, or `2G`. For example:

```
$ cf push -m 128M
```

When your app is running, you can use the `cf app APP-NAME` command to see memory utilization.

### Sample App Step

You can skip this step. In the `manifest.yml` of the `pong_matcher_groovy` sample app, the `memory` sub-block of the `applications` block allocates 512 MB to the app.

## Step 3: Provide a JDBC Driver

The Java buildpack does not bundle a JDBC driver with your application. If your application accesses a SQL RDBMS, you must do the following:

- Include the appropriate driver in your application.
- Create a dependency task for the driver in the build script for your build tool or IDE.

### Sample App Step

You can skip this step. The `pong_matcher_groovy` sample app does not require a JDBC driver.

## Step 4: (Optional) Configure a Procfile

Use a Procfile to declare required runtime processes for your web app and to specify your web server. For more information, see the [Configuring a Production Server](#) topic.

### Sample App Step

You can skip this step. The `pong_matcher_groovy` app does not require a Procfile.

## Step 5: Create and Bind a Service Instance for a Ratpack Application

This section describes using the CLI to configure a Redis managed service instance for an app. You can use either the CLI or [Apps Manager](#) to perform this task.

PAS supports two types of service instances:

- Managed services integrate with PAS through service brokers that offer services and plans and manage the service calls between PAS and a service provider.
- User-provided service instances enable you to connect your application to pre-provisioned external service instances.

For more information about creating and using service instances, refer to the [Services Overview](#) topic.

### Create a Service Instance

Run `cf marketplace` to view managed and user-provided services and plans available to you.

The example shows two of the available managed database-as-a-service providers and their offered plans: `postgresql-10-odb` PostgreSQL as a Service and `rediscloud` Enterprise-Class Redis for Developers.

```
$ cf marketplace
Getting services from marketplace in org Cloud-Apps / space development as clouduser@example.com...
OK
```

| service           | plans                                   | description                           |
|-------------------|-----------------------------------------|---------------------------------------|
| postgresql-10-odb | standalone, standalone-replica, general | PostgreSQL as a Service               |
| rediscloud        | 30mb, 100mb, 1gb, 10gb, 50gb            | Enterprise-Class Redis for Developers |

Run `cf create-service SERVICE PLAN SERVICE-INSTANCE` to create a service instance for your app. Choose a SERVICE and PLAN from the list, and provide a unique name for the SERVICE-INSTANCE.

### Sample App Step

Run `cf create-service rediscloud 30mb baby-redis`. This creates a service instance named `baby-redis` that uses the `rediscloud` service and the `30mb` plan, as the example below shows.

```
$ cf create-service rediscloud 30mb baby-redis
Creating service baby-redis in org Cloud-Apps / space development as clouduser@example.com....
OK
```

## Bind a Service Instance

When you bind an app to a service instance, PAS writes information about the service instance to the VCAP\_SERVICES app environment variable. The app can use this information to integrate with the service instance.

Most services support bindable service instances. Refer to your service provider's documentation to confirm if they support this functionality.

You can bind a service to an application with the command `cf bind-service APPLICATION SERVICE_INSTANCE`.

Alternately, you can configure the deployment manifest file by adding a `services` sub-block to the `applications` block and specifying the service instance. For more information and an example on service binding using a manifest, see the Sample App step.

You can also bind a service using the [Apps Manager](#).

### Sample App Step

You can skip this step because the service instance is already bound. Open the `manifest.yml` file in a text editor to view the bound service instance information. Locate the file in the app root directory and search for the `services` sub-block in the `applications` block, as the example below shows.

```

applications:
...
 services:
 - baby-redis
```

## Step 6: Configure the Deployment Manifest

You can specify deployment options in the `manifest.yml` that the `cf push` command uses when deploying your app.

Refer to the [Deploying with Application Manifests](#) topic for more information.

### Sample App Step

You can skip this step. The `manifest.yml` file for the `pong_matcher_groovy` sample app does not require any additional configuration to deploy the app.


## Step 7: Log in and Target the API Endpoint

Run `cf login -a API-ENDPOINT`, enter your login credentials, and select a space and org. The API endpoint is [the URL of the Cloud Controller in your PAS instance](#).


### Sample App Step

You must perform this step to run the sample app.

## Step 8: Deploy the Application

 **Note:** You must use the cf CLI to deploy apps.

From the root directory of your application, run `cf push APP-NAME -p PATH-TO-FILE.distZip` to deploy your application.

 **Note:** You must deploy the `.distZip` artifact for a Ratpack app, and you must include the path to the `.distZip` file in the `cf push` command using the `-p` option if you do not declare the path in the `applications` block of the manifest file. For more information, refer to the [Tips for Java Developers](#) topic.

`cf push APP-NAME` creates a URL route to your application in the form `HOST.DOMAIN`, where `HOST` is your `APP-NAME` and `DOMAIN` is specified by your administrator. Your `DOMAIN` is `shared-domain.example.com`. For example: `cf push my-app` creates the URL `my-app.shared-domain.example.com`.

The URL for your app must be unique from other apps that PAS hosts or the push will fail. Use the following options to help create a unique URL:

- `-n` to assign a different HOST name for the app
- `--random-route` to create a URL that includes the app name and random words
- `cf help push` to view other options for this command


If you want to view log activity while the app deploys, launch a new terminal window and run `cf logs APP-NAME`.

Once your app deploys, browse to your app URL. Search for the `urls` field in the `App started` block in the output of the `cf push` command. Use the URL to access your app online.

### Sample App Step

1. Change to the `app` directory, and run `./gradlew distZip` to build the app.
2. Run `cf push pong_matcher_groovy -n HOST-NAME` to push the app.

Example: `cf push pong_matcher_groovy -n groovy-ratpack-app`

 **Note:** You do not have to include the `-p` flag when you deploy the sample app. The sample app manifest declares the path to the archive that `cf push` uses to upload the app files.

The example below shows the terminal output of deploying the `pong_matcher_groovy` app. `cf push` uses the instructions in the manifest file to create the app, create and bind the route, and upload the app. It then binds the app to the `baby-redis` service and follows the instructions in the manifest to start one instance of the app with 512 MB. After the app starts, the output displays the health and status of the app.



```
$ cf push pong_matcher_groovy -n groovy-ratpack-app
Using manifest file /Users/example/workspace/pong_matcher_groovy/app/manifest.yml

Creating app pong_matcher_groovy in org Cloud-Apps / space development as clouduser@example.com...
OK

Creating route groovy-ratpack-app.cfapps.io...
OK

Binding groovy-ratpack-app.cfapps.io to pong_matcher_groovy...
OK

Uploading pong_matcher_groovy...
Uploading app files from: /Users/example/workspace/pong_matcher_groovy/app/build/distributions/app.zip
Uploading 138.2K, 18 files
OK
Binding service baby-redis to app pong_matcher_groovy in org Cloud-Apps / space development as clouduser@example.com...
OK

Starting app pong_matcher_groovy in org Cloud-Apps / space development as clouduser@example.com...
OK
-----> Downloaded app package (12M)
Cloning into '/tmp/buildpacks/java-buildpack'...
-----> Java Buildpack Version: 9e096be | https://github.com/cloudfoundry/java-buildpack#9e096be
 Expanding Open Jdk JRE to .java-buildpack/open_jdk_jre (1.3s)
-----> Uploading droplet (49M)

0 of 1 instances running, 1 starting
1 of 1 instances running

App started

Showing health and status for app pong_matcher_groovy in org Cloud-Apps / space development as clouduser@example.com...
OK

requested state: started
instances: 1/1
usage: 512M x 1 instances
urls: groovy-ratpack-app.cfapps.io

state since cpu memory disk
#0 running 2014-10-28 04:48:58 PM 0.0% 193.5M of 512M 111.7M of 1G
```

## Step 9: Test Your Deployed App

You've deployed an app to PAS!

Use the `cf` CLI or [Apps Manager](#) to review information and administer your app and your PAS account. For example, you can edit the `manifest.yml` to increase the number of app instances from 1 to 3, and redeploy the app with a new app name and host name.

See the [Manage Your Application with the cf CLI](#) section for more information. See also [Using the Apps Manager](#).

### Sample App Step

To test the sample app, do the following:

1. To export the test host, run `export HOST=SAMPLE-APP-URL`, substituting the URL for your app for `SAMPLE-APP-URL`.

2. To clear the database from any previous tests, run:

```
curl -v -X DELETE
$HOST/all
```

You should get a response of 200.

3. To request a match as "andrew", run:

```
curl -v -H "Content-Type: application/json" -X PUT $HOST/match_requests/firstrequest -d '{"player":
"andrew"}'
```

You should again get a response of `200`.

4. To request a match as a different player, run:

```
curl -v -H "Content-Type: application/json" -X PUT $HOST/match_requests/secondrequest -d '{"player":
"navratilova"}'
```

5. To check the status of the first match request, run:

```
curl -v -X GET
$HOST/match_requests/firstrequest
```

The last line of the output shows the `match_id`.

6. Replace `MATCH_ID` with the `match_id` value from the previous step in the following command:

```
curl -v -H "Content-Type: application/json" -X POST $HOST/results -d ' { "match_id": "MATCH_ID", "winner": "andrew", "loser": "navratilova"
}'
```


You should receive a `201` response.

```
Created
```

## Manage Your Application with the cf CLI

Run `cf help` to view a complete list of commands, grouped by task categories, and run `cf help COMMAND` for detailed information about a specific

command. For more information about using the cf CLI, refer to the Cloud Foundry Command Line Interface (cf CLI) topics, especially the [Getting Started with cf CLI](#) topic.

 **Note:** You cannot perform certain tasks in the CLI or [Apps Manager](#) because these are commands that only a PAS administrator can run. If you are not a PAS administrator, the following message displays for these types of commands:

```
error code: 10003, message: You are not authorized to perform the requested
action
```

For more information about specific Admin commands you can perform with

the Apps Manager, depending on your user role, refer to the [Getting Started with the Apps Manager](#) topic.

## Troubleshooting

If your application fails to start, verify that the application starts in your local environment. Refer to the [Troubleshooting Application Deployment and Health](#) topic to learn more about troubleshooting.

### App Deploy Fails

Even when the deploy fails, the app might exist on PAS. Run `cf apps` to review the apps in the currently targeted org and space. You might be able to correct the issue using the CLI or [Apps Manager](#), or you might have to delete the app and redeploy.

### App Requires a Unique URL

PAS requires that each app that you deploy have a unique URL. Otherwise, the new app URL collides with an existing app URL and PAS cannot successfully deploy the app. You can fix this issue by running `cf push` with either of the following flags to create a unique URL:

- `-n` to assign a different HOST name for the app.
- `--random-route` to create a URL that includes the app name and random words. Using this option might create a long URL, depending on the number of words that the app name includes.

## Getting Started Deploying Spring Apps

Page last updated:

This guide is intended to walk you through deploying a Spring app to Pivotal Application Service. You can choose whether to push a sample app, your own app, or both.

If you experience a problem following the steps below, see the [Known Issues](#) topic, or refer to the [Troubleshooting Application Deployment and Health](#) topic.

### Sample App Step

If you want to go through this tutorial using the sample app, run `git clone https://github.com/cloudfoundry-samples/pong_matcher_spring` to clone the `pong_matcher_spring` app from GitHub, and follow the instructions in the Sample App Step sections.



**Note:** Ensure that your Spring app runs locally before continuing with this procedure.

## Deploy a Spring Application

This section describes how to deploy your Spring application to PAS.

### Prerequisites

- A Spring app that runs locally on your workstation
- Intermediate to advanced Spring knowledge
- The [Cloud Foundry Command Line Interface \(cf CLI\)](#)
- JDK 1.6, 1.7, or 1.8 for Java 6, 7, or 8 configured on your workstation



**Note:** The Cloud Foundry Java buildpack uses JDK 1.8, but you can modify the buildpack and the manifest for your app to compile to an earlier version. For more information, refer to the [Custom Buildpacks](#) topic.

## Step 1: Declare App Dependencies

Be sure to declare all the dependency tasks for your app in the build script of your chosen build tool.

The [Spring Getting Started Guides](#) demonstrate features and functionality you can add to your app, such as consuming RESTful services or integrating data. These guides contain Gradle and Maven build script examples with dependencies. You can copy the code for the dependencies into your build script.

The table lists build script information for Gradle and Maven and provides documentation links for each build tool.

| Build Tool | Build Script              | Documentation                                      |
|------------|---------------------------|----------------------------------------------------|
| Gradle     | <code>build.gradle</code> | <a href="#">Gradle User Guide</a>                  |
| Maven      | <code>pom.xml</code>      | <a href="#">Apache Maven Project Documentation</a> |

### Sample App Step

You can skip this step. The `pom.xml` file contains the dependencies for the `pong_matcher_spring` sample app, as the example below shows.

```
<dependencies>
 <dependency>
 <groupId>mysql</groupId>
 <artifactId>mysql-connector-java</artifactId>
 </dependency>
 <dependency>
 <groupId>org.flywaydb</groupId>
 <artifactId>flyway-core</artifactId>
 </dependency>
 <dependency>
 <groupId>org.springframework.boot</groupId>
 <artifactId>spring-boot-starter-data-jpa</artifactId>
 </dependency>
 <dependency>
 <groupId>org.springframework.boot</groupId>
 <artifactId>spring-boot-starter-test</artifactId>
 </dependency>
 <dependency>
 <groupId>org.springframework.boot</groupId>
 <artifactId>spring-boot-starter-web</artifactId>
 </dependency>

 <dependency>
 <groupId>com.h2database</groupId>
 <artifactId>h2</artifactId>
 <scope>test</scope>
 </dependency>
 <dependency>
 <groupId>com.jayway.jsonpath</groupId>
 <artifactId>json-path</artifactId>
 <scope>test</scope>
 </dependency>
</dependencies>
```

 **Note:** Make sure you are not building [fully executable jars](#)  because application push may fail.

## Step 2: Allocate Sufficient Memory

Use the `cf push -m` command to specify the amount of memory that should be allocated to the application. Memory allocated this way is done in preset amounts of `64M`, `128M`, `256M`, `512M`, `1G`, or `2G`. For example:

```
$ cf push -m 128M
```

When your app is running, you can use the `cf app APP-NAME` command to see memory utilization.

### Sample App Step

You can skip this step. The Cloud Foundry Java buildpack uses settings declared in the sample app to allocate 1 GB of memory to the app.

## Step 3: Provide a JDBC Driver

The Java buildpack does not bundle a JDBC driver with your application. If your application accesses a SQL RDBMS, you must do the following:

- Include the appropriate driver in your application.
- Create a dependency task for the driver in the build script for your build tool or IDE.

### Sample App Step

You can skip this step. In the `pong_matcher_spring` sample app, the `src/main/resources/application.yml` file declares the JDBC driver, and the `pom.xml` file includes the JDBC driver as a dependency.

## Step 4: Configure Service Connections for a Spring App

PAS provides extensive support for creating and binding a Spring application to services such as MySQL, PostgreSQL, MongoDB, Redis, and RabbitMQ. For more information about creating and binding a service connection for your app, refer to the [Configure Service Connections for Spring](#) topic.

## Sample App Step: Create a Service Instance

Run `cf create-service cleardb spark mysql`. This creates a service instance named `mysql` that uses the `cleardb` service and the `spark` plan, as the example below shows.

```
$ cf create-service cleardb spark mysql
Creating service mysql in org Cloud-Apps / space development as a.user@example.com...
OK
```

## Sample App Step: Bind a Service Instance

You can skip this step because the service instance is already bound. Open the `manifest.yml` file in a text editor to view the bound service instance information. Locate the file in the app root directory and search for the `services` sub-block in the `applications` block, as the example below shows.

```

applications:
...
 services:
 - mysql
```

## Step 5: Configure the Deployment Manifest

You can specify deployment options in a manifest file `manifest.yml` that the `cf push` command uses when deploying your app.

Refer to the [Deploying with Application Manifests](#) topic for more information.

## Sample App Step

You can skip this step. The `manifest.yml` file for the `pong_matcher_spring` sample app does not require any additional configuration to deploy the app.


## Step 6: Log in and Target the API Endpoint

Run `cf login -a API-ENDPOINT`, enter your login credentials, and select a space and org. The API endpoint is [the URL of the Cloud Controller in your PAS instance](#).


## Sample App Step

You must do this step to run the sample app.

## Step 7: Deploy Your Application

 **Note:** You must use the cf CLI to deploy apps.

From the root directory of your application, run `cf push APP-NAME -p PATH-TO-FILE.war` to deploy your application.

 **Note:** Most Spring apps include an artifact, such as a `.jar`, `.war`, or `.zip` file. You must include the path to this file in the `cf push` command using the `-p` option if you do not declare the path in the `applications` block of the manifest file. The example shows how to specify a path to the `.war`

file for a Spring app. Refer to the [Tips for Java Developers](#) topic for CLI examples for specific build tools, frameworks, and languages that create an app with an artifact.

`cf push APP-NAME` creates a URL route to your application in the form HOST.DOMAIN, where HOST is your APP-NAME and DOMAIN is specified by your administrator. Your DOMAIN is `shared-domain.example.com`. For example: `cf push my-app` creates the URL `my-app.shared-domain.example.com`.

The URL for your app must be unique from other apps that PAS hosts or the push will fail. Use the following options to help create a unique URL:

- `-n` to assign a different HOST name for the app
- `--random-route` to create a URL that includes the app name and random words
- `cf help push` to view other options for this command


If you want to view log activity while the app deploys, launch a new terminal window and run `cf logs APP-NAME`.

Once your app deploys, browse to your app URL. Search for the `urls` field in the `App started` block in the output of the `cf push` command. Use the URL to access your app online.

#### Sample App Step

1. Run `brew install maven`.
2. Change to the `app` directory, and run `mvn package` to build the app.
3. Run `cf push pong_matcher_spring -n HOSTNAME` to push the app.

Example: `cf push pong_matcher_spring -n my-spring-app`

 **Note:** You do not have to include the `-p` flag when you deploy the sample app. The sample app manifest declares the path to the archive that `cf push` uses to upload the app files.

The example below shows the terminal output of deploying the `pong_matcher_spring` app. `cf push` uses the instructions in the manifest file to create the app, create and bind the route, and upload the app. It then binds the app to the `mysql` service and starts one instance of the app with 1 GB of memory. After the app starts, the output displays the health and status of the app.

```
$ cf push pong_matcher_spring -n spring1119
Using manifest file /Users/example/workspace/pong_matcher_spring/manifest.yml

Creating app pong_matcher_spring in org Cloud-Apps / space development as a.user@example.com...
OK

Creating route spring1119.cfapps.io...
OK

Binding spring1119.cfapps.io to pong_matcher_spring...
OK

Uploading pong_matcher_spring...
Uploading app files from: /Users/example/workspace/pong_matcher_spring/target/pong-matcher-spring-1.0.0.BUILD-SNAPSHOT.jar
Uploading 797.5K, 116 files
OK
Binding service mysql to app pong_matcher_spring in org Cloud-Apps / space development as a.user@example.com...
OK

Starting app pong_matcher_spring in org Cloud-Apps / space development as a.user@example.com...
OK
-----> Downloaded app package (25M)
-----> Downloading Open Jdk JRE 1.8.0_25 from https://download.run.pivotal.io/openjdk/lucid/x86_64/openjdk-1.8.0_25.tar.gz (1.2s)
 Expanding Open Jdk JRE to .java-buildpack/open_jdk_jre (1.1s)
-----> Downloading Spring Auto Reconfiguration 1.5.0_RELEASE from https://download.run.pivotal.io/auto-reconfiguration/auto-reconfiguration-1.5.0_RELEASE.jar (0.1s)

-----> Uploading droplet (63M)

0 of 1 instances running, 1 starting
1 of 1 instances running

App started

Showing health and status for app pong_matcher_spring in org Cloud-Apps / space development as a.user@example.com...
OK

requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: spring1119.cfapps.io

state since cpu memory disk
#0 running 2014-11-19 12:29:27 PM 0.0% 553.6M of 1G 127.4M of 1G
```

## Step 8: Test Your Deployed App

You've deployed an app to PAS!

Use the cf CLI or [Apps Manager](#) to review information and administer your app and your PAS account. For example, you can edit the `manifest.yml` to increase the number of app instances from 1 to 3, and redeploy the app with a new app name and host name.

See the [Manage Your Application with the cf CLI](#) section for more information. See also [Using the Apps Manager](#).

### Sample App Step

To test the sample app, do the following:

1. To export the test host, run `export HOST=SAMPLE-APP-URL`, substituting the URL for your app for `SAMPLE-APP-URL`.

2. To clear the database from any previous tests, run:

```
curl -v -X DELETE
$HOST/all
```

You should get a response of 200.

3. To request a match as "andrew", run:

```
curl -v -H "Content-Type: application/json" -X PUT $HOST/match_requests/firstrequest -d '{"player":
"andrew"}'
```

You should again get a response of `200`.

4. To request a match as a different player, run:

```
curl -v -H "Content-Type: application/json" -X PUT $HOST/match_requests/secondrequest -d '{"player":
"navratilova"}'
```

5. To check the status of the first match request, run:

```
curl -v -X GET
$HOST/match_requests/firstrequest
```

The last line of the output shows the `match_id`.

6. Replace `MATCH_ID` with the `match_id` value from the previous step in the following command:


```
curl -v -H "Content-Type: application/json" -X POST $HOST/results -d ' { "match_id": "MATCH_ID", "winner": "andrew", "loser": "navratilova"
}'
```

You should receive a `201 Created` response.

## Manage Your Application with the cf CLI

Run `cf help` to view a complete list of commands, grouped by task categories, and run `cf help COMMAND` for detailed information about a specific

command. For more information about using the cf CLI, refer to the Cloud Foundry Command Line Interface (cf CLI) topics, especially the [Getting Started with cf CLI](#) topic.

 **Note:** You cannot perform certain tasks in the CLI or [Apps Manager](#) because these are commands that only a PAS administrator can run. If you are not a PAS administrator, the following message displays for these types of commands:

```
error code: 10003, message: You are not authorized to perform the requested
action
```

For more information about specific Admin commands you can perform with

the Apps Manager, depending on your user role, refer to the [Getting Started with the Apps Manager](#) topic.

## Troubleshooting

If your application fails to start, verify that the application starts in your local environment. Refer to the [Troubleshooting Application Deployment and Health](#) topic to learn more about troubleshooting.

### App Deploy Fails

Even when the deploy fails, the app might exist on PAS. Run `cf apps` to review the apps in the currently targeted org and space. You might be able to correct the issue using the CLI or [Apps Manager](#), or you might have to delete the app and redeploy.

### App Requires a Content-Type

If you specify a `Content-Encoding` header of `gzip` but do not specify a `Content-Type` within your application, PAS might send a `Content-Type` of `application/x-gzip` to the browser. This scenario might cause the deploy to fail if it conflicts with the actual encoded content of your app. To avoid this issue, be sure to explicitly set `Content-Type` within your app.

### App Requires a Unique URL

PAS requires that each app that you deploy have a unique URL. Otherwise, the new app URL collides with an existing app URL and PAS cannot successfully deploy the app. You can fix this issue by running `cf push` with either of the following flags to create a unique URL:

- `-n` to assign a different HOST name for the app.
- `--random-route` to create a URL that includes the app name and random words. Using this option might create a long URL, depending on the number of words that the app name includes.



## Configuring Service Connections

Page last updated:

This topic provides links to additional information about configuring service connections for Java apps. See the specific documentation for your app framework:

- [Grails](#)
- [Play](#)
- [Spring](#)

## Configuring Service Connections for Grails

Page last updated:

Cloud Foundry provides extensive support for connecting a Grails application to services such as MySQL, Postgres, MongoDB, Redis, and RabbitMQ. In many cases, a Grails application running on Cloud Foundry can automatically detect and configure connections to services. For more advanced cases, you can control service connection parameters yourself.

### Auto-Configuration

Grails provides plugins for accessing SQL (using [Hibernate](#)), [MongoDB](#), and [Redis](#) services. If you install any of these plugins and configure them in your `Config.groovy` or `DataSource.groovy` file, Cloud Foundry reconfigures the plugin with connection information when your app starts.

If you use all three types of services, your configuration might look like this:

```
environments {
 production {
 dataSource {
 url = 'jdbc:mysql://localhost/db?useUnicode=true&characterEncoding=utf8'
 dialect = org.hibernate.dialect.MySQLInnoDBDialect
 driverClassName = 'com.mysql.jdbc.Driver'
 username = 'user'
 password = 'password'
 }
 grails {
 mongo {
 host = 'localhost'
 port = 27107
 dbName = 'foo'
 username = 'user'
 password = 'password'
 }
 redis {
 host = 'localhost'
 port = 6379
 password = 'password'
 timeout = 2000
 }
 }
 }
}
```

The `url`, `host`, `port`, `dbName`, `username`, and `password` fields in this configuration will be overridden by the Cloud Foundry auto-reconfiguration if it detects that the application is running in a Cloud Foundry environment. If you want to test the application locally against your own services, you can put real values in these fields. If the application will only be run against Cloud Foundry services, you can put placeholder values as shown here, but the fields must exist in the configuration.

### Manual Configuration

If you do not want to use auto-configuration, you can configure the Cloud Foundry service connections manually.

Follow the steps below to manually configure a service connection.

1. Add the `spring-cloud` library to the `dependencies` section of your `BuildConfig.groovy` file.

```
repositories {
 grailsHome()
 mavenCentral()
 grailsCentral()
 mavenRepo "http://repo.spring.io/milestone"
}

dependencies {
 compile "org.springframework.cloud:spring-cloud-cloudfoundry-connector:1.0.0.RELEASE"
 compile "org.springframework.cloud:spring-cloud-spring-service-connector:1.0.0.RELEASE"
}
```

Adding the `spring-cloud` library allows you to disable auto-configuration and use the `spring-cloud` API in your `DataSource.groovy` file to set the

connection parameters.

2. Add the following to your `grails-app/conf/spring/resources.groovy` file to disable auto-configuration:

```
beans = {
 cloudFactory(org.springframework.cloud.CloudFactory)
}
```

3. Add the following `imports` to your `DataSource.groovy` file to allow `spring-cloud` API commands:

```
import org.springframework.cloud.CloudFactory
import org.springframework.cloud.CloudException
```

4. Add the following code to your `DataSource.groovy` file to enable Cloud Foundry's `getCloud` method to function locally or in other environments outside of a cloud.

```
def cloud = null
try {
 cloud = new CloudFactory().cloud
} catch (CloudException) {}
```

5. Use code like the following to access the cloud object:

```
def dbInfo = cloud?.getServiceInfo('myapp-mysql')
url = dbInfo?.jdbcUrl
username = dbInfo?.userName
password = dbInfo?.password
```

`myapp-mysql` is the name of the service as it appears in the `name` column of the output from `cf services`. For example, `mysql` or `rabbitmq`.

The example `DataSource.groovy` file below contains the following:

- The `imports` that allow `spring-cloud` API commands
- The code that enables the `getCloud` method to function locally or in other environments outside of a cloud
- Code to access the cloud object for SQL, MongoDB, and Redis services

```
import org.springframework.cloud.CloudFactory
import org.springframework.cloud.CloudException

def cloud = null
try {
 cloud = new CloudFactory().cloud
} catch (CloudException) {}

dataSource {
 pooled = true
 dbCreate = 'update'
 driverClassName = 'com.mysql.jdbc.Driver'
}

environments {
 production {
 dataSource {
 def dbInfo = cloud?.getServiceInfo('myapp-mysql')
 url = dbInfo?.jdbcUrl
 username = dbInfo?.userName
 password = dbInfo?.password
 }
 grails {
 mongo {
 def mongoInfo = cloud?.getServiceInfo('myapp-mongodb')
 host = mongoInfo?.host
 port = mongoInfo?.port
 databaseName = mongoInfo?.database
 username = mongoInfo?.userName
 password = mongoInfo?.password
 }
 redis {
 def redisInfo = cloud?.getServiceInfo('myapp-redis')
 host = redisInfo?.host
 port = redisInfo?.port
 password = redisInfo?.password
 }
 }
 }
 development {
 dataSource {
 url = 'jdbc:mysql://localhost:5432/myapp'
 username = 'sa'
 password = ''
 }
 grails {
 mongo {
 host = 'localhost'
 port = 27107
 databaseName = 'foo'
 username = 'user'
 password = 'password'
 }
 redis {
 host = 'localhost'
 port = 6379
 password = 'password'
 }
 }
 }
}
```

## Configuring Service Connections for Play Framework

Page last updated:

Cloud Foundry supports running Play Framework applications and the Play JPA plugin for auto-configuration for Play versions up to and including v2.4.x.

Cloud Foundry provides support for connecting a Play Framework application to services such as MySQL and Postgres. In many cases, a Play Framework application running on Cloud Foundry can automatically detect and configure connections to services.

### Auto-Configuration

By default, Cloud Foundry detects service connections in a Play Framework application and configures them to use the credentials provided in the Cloud Foundry environment. Note that auto-configuration happens only if there is a single service of either of the supported types—MySQL or Postgres.

## Configuring Service Connections for Spring

Page last updated:

Cloud Foundry provides extensive support for connecting a Spring application to services such as MySQL, PostgreSQL, MongoDB, Redis, and RabbitMQ. In many cases, Cloud Foundry can automatically configure a Spring application without any code changes. For more advanced cases, you can control service connection parameters yourself.

### Auto-Reconfiguration

If your Spring application requires services such as a relational database or messaging system, you might be able to deploy your application to Cloud Foundry without changing any code. In this case, Cloud Foundry automatically re-configures the relevant bean definitions to bind them to cloud services.

For information about connecting to services from a Spring application, see [Spring Cloud Spring Service Connector](#).

Cloud Foundry auto-reconfigures applications only if the following items are true for your application:

- Only one service instance of a given service type is bound to the application. In this context, different relational databases services are considered the same service type. For example, if both a MySQL and a PostgreSQL service are bound to the application, auto-reconfiguration does not occur.
- Only one bean of a matching type is in the Spring application context. For example, you can have only one bean of type `javax.sql.DataSource`.

With auto-reconfiguration, Cloud Foundry creates the `DataSource` or connection factory bean itself, using its own values for properties such as host, port, and username. For example, if you have a single `javax.sql.DataSource` bean in your application context that Cloud Foundry auto-reconfigures and binds to its own database service, Cloud Foundry does not use the username, password, and driver URL you originally specified. Instead, Cloud Foundry uses its own internal values. This is transparent to the app, which really only cares about having a `DataSource` where it can write data but does not really care what the specific properties are that created the database. Also, if you have customized the configuration of a service, such as the pool size or connection properties, Cloud Foundry auto-reconfiguration ignores the customizations.

For more information about auto-reconfiguration of specific services types, see the [Service-Specific Details](#) section.

### Manual Configuration

Use manual configuration if you have multiple services of a given type or you want to have more control over the configuration than auto-reconfiguration provides.

To use manual configuration, include the `spring-cloud` library in your list of application dependencies. Update your application Maven `pom.xml` or Gradle `build.gradle` file to include dependencies on the `org.springframework.cloud:spring-cloud-spring-service-connector` and `org.springframework.cloud:spring-cloud-cloudfoundry-connector` artifacts.

For example, if you use Maven to build your application, the following `pom.xml` snippet shows how to add this dependency.

```
<dependencies>
 <dependency>
 <groupId>org.springframework.cloud</groupId>
 <artifactId>spring-cloud-spring-service-connector</artifactId>
 <version>1.2.3.RELEASE</version>
 </dependency>
 <dependency>
 <groupId>org.springframework.cloud</groupId>
 <artifactId>spring-cloud-cloudfoundry-connector</artifactId>
 <version>1.2.3.RELEASE</version>
 </dependency>
</dependencies>
```

You also need to update your application build file to include the Spring Framework Milestone repository. The following `pom.xml` snippet shows how to do this for Maven:

```
<repositories>
 <repository>
 <id>repository.springsource.milestone</id>
 <name>SpringSource Milestone Repository</name>
 <url>http://repo.springsource.org/milestone</url>
 </repository>
 ...
</repositories>
```

## Java Configuration

Typical use of Java config involves extending the `AbstractCloudConfig` class and adding methods with the `@Bean` annotation to create beans for services. Apps migrating from [auto-reconfiguration](#) might first try [Scanning for Services](#) until they need more explicit control. Java config also offers a way to expose application and service properties. Use this for debugging or to create service connectors using a lower-level access.

### Create a Service Bean

In the following example, the configuration creates a `DataSource` bean connecting to the only relational database service bound to the app. It also creates a `MongoDbFactory` bean, again, connecting to the only MongoDB service bound to the app. Check Javadoc for `AbstractCloudConfig` for ways to connect to other services.

```
class CloudConfig extends AbstractCloudConfig {
 @Bean
 public DataSource inventoryDataSource() {
 return connectionFactory().dataSource();
 }
 ... more beans to obtain service connectors
}
```

The bean names match the method names unless you specify an explicit value to the annotation such as `@Bean("inventory-service")`, following Spring's Java configuration standards.

If you have more than one service of a type bound to the app or want to have an explicit control over the services to which a bean is bound, you can pass the service names to methods such as `dataSource()` and `mongoDbFactory()` as follows:

```
class CloudConfig extends AbstractCloudConfig {

 @Bean
 public DataSource inventoryDataSource() {
 return connectionFactory().dataSource("inventory-db-service");
 }

 @Bean
 public MongoDbFactory documentMongoDbFactory() {
 return connectionFactory().mongoDbFactory("document-service");
 }

 ... more beans to obtain service connectors
}
```

Method such as `dataSource()` come in an additional overloaded variant that offer specifying configuration options such as the pooling parameters. See Javadoc for more details.

### Connect to Generic Services

Java config supports access to generic services through the `service()` method. Generic services do not have a directly mapped method. This is typical for a newly introduced service or when connecting to a private service in private PaaS. The generic `service()` method follows the same pattern as the `dataSource()`, except it allows supplying the connector type as an additional parameters.

### Scan for Services

You can scan for each bound service using the `@ServiceScan` annotation as shown below. This is conceptually similar to the `@ComponentScan` annotation in Spring:

```
@Configuration
@ServiceScan
class CloudConfig {

}
```

Here, one bean of the appropriate type (`DataSource` for a relational database service, for example) is created. Each created bean will have the `id` matching the corresponding service name. You can then inject such beans using auto-wiring:

```
@Autowired DataSource inventoryDb;
```

If the app is bound to more than one services of a type, you can use the `@Qualifier` annotation supplying it the name of the service as in the following code:

```
@Autowired @Qualifier("inventory-db") DataSource inventoryDb;
@Autowired @Qualifier("shipping-db") DataSource shippingDb;
```

## Access Service Properties

You can expose raw properties for all services and the app through a bean as follows:

```
class CloudPropertiesConfig extends AbstractCloudConfig {


 @Bean
 public Properties cloudProperties() {
 return properties();
 }
}
```

## Cloud Profile

Spring Framework versions 3.1 and above support bean definition profiles as a way to conditionalize the application configuration so that only specific bean definitions are activated when a certain condition is true. Setting up such profiles makes your application portable to many different environments so that you do not have to manually change the configuration when you deploy it to, for example, your local environment and then to Cloud Foundry.

See the Spring Framework documentation for additional information about using Spring bean definition profiles.

When you deploy a Spring application to Cloud Foundry, Cloud Foundry automatically enables the `cloud` profile.

 **Note:** Cloud Foundry auto-reconfiguration requires the Spring application to be version 3.1 or later and include the Spring context JAR. If you are using an earlier version, update your framework or use a custom buildpack.

## Profiles in Java Configuration

The `@Profile` annotation can be placed on `@Configuration` classes in a Spring application to set conditions under which configuration classes are invoked. By using the `default` and `cloud` profiles to determine whether the application is running on Cloud Foundry or not, your Java configuration can support both local and cloud deployments using Java configuration classes like these:



```
public class Configuration {
 @Configuration
 @Profile("cloud")
 static class CloudConfiguration {

 @Bean
 public DataSource dataSource() {
 CloudFactory cloudFactory = new CloudFactory();
 Cloud cloud = cloudFactory.getCloud();
 String serviceID = cloud.getServiceID();
 return cloud.getServiceConnector(serviceID, DataSource.class, null);
 }
 }

 @Configuration
 @Profile("default")
 static class LocalConfiguration {

 @Bean
 public DataSource dataSource() {
 BasicDataSource dataSource = new BasicDataSource();
 dataSource.setUrl("jdbc:postgresql://localhost/db");
 dataSource.setDriverClassName("org.postgresql.Driver");
 dataSource.setUsername("postgres");
 dataSource.setPassword("postgres");
 return dataSource;
 }
 }
}
```

## Property Placeholders

Cloud Foundry exposes a number of application and service properties directly into its deployed applications. The properties exposed by Cloud Foundry include basic information about the application, such as its name and the cloud provider, and detailed connection information for all services currently bound to the application.

Service properties generally take one of the following forms:

```
cloud.services.{service-name}.connection.{property}
cloud.services.{service-name}.{property}
```

In this form, `{service-name}` refers to the name you gave the service when you bound it to your application at deploy time, and `{property}` is a field in the credentials section of the `VCAP_SERVICES` environment variable.

For example, assume that you created a Postgres service called `my-postgres` and then bound it to your application. Assume also that this service exposes credentials in `VCAP_SERVICES` as discrete fields. Cloud Foundry exposes the following properties about this service:

```
cloud.services.my-postgres.connection.hostname
cloud.services.my-postgres.connection.name
cloud.services.my-postgres.connection.password
cloud.services.my-postgres.connection.port
cloud.services.my-postgres.connection.username
cloud.services.my-postgres.plan
cloud.services.my-postgres.type
```

If the service exposed the credentials as a single `uri` field, then the following properties would be set up:

```
cloud.services.my-postgres.connection.uri
cloud.services.my-postgres.plan
cloud.services.my-postgres.type
```

For convenience, if you have bound just one service of a given type to your application, Cloud Foundry creates an alias based on the service type instead of the service name. For example, if only one MySQL service is bound to an application, the properties takes the form `cloud.services.mysql.connection.{property}`. Cloud Foundry uses the following aliases in this case:

- `mysql`
- `postgresql`
- `mongodb`

- `redis`
- `rabbitmq`

A Spring application can take advantage of these Cloud Foundry properties using the property placeholder mechanism. For example, assume that you have bound a MySQL service called `spring-mysql` to your application. Your application requires a `c3p0` connection pool instead of the connection pool provided by Cloud Foundry, but you want to use the same connection properties defined by Cloud Foundry for the MySQL service - in particular the username, password and JDBC URL.

The following table lists all the application properties that Cloud Foundry exposes to deployed applications.

| Property                            | Description                                                                           |
|-------------------------------------|---------------------------------------------------------------------------------------|
| <code>cloud.application.name</code> | The name provided when the application was pushed to Cloud Foundry.                   |
| <code>cloud.provider.url</code>     | The URL of the cloud hosting the application, such as <code>cloudfoundry.com</code> . |

The service properties that are exposed for each type of service are listed in the [Service-Specific Details](#) section.

## Service-Specific Details

The following sections describe Spring auto-reconfiguration and manual configuration for the services supported by Cloud Foundry.

### MySQL and Postgres

#### Auto-Reconfiguration

Auto-reconfiguration occurs if Cloud Foundry detects a `javax.sql.DataSource` bean in the Spring application context. The following snippet of a Spring application context file shows an example of defining this type of bean which Cloud Foundry will detect and potentially auto-reconfigure:

```
<bean class="org.apache.commons.dbcp.BasicDataSource" destroy-method="close" id="dataSource">
 <property name="driverClassName" value="org.h2.Driver" />
 <property name="url" value="jdbc:h2:mem:" />
 <property name="username" value="sa" />
 <property name="password" value="" />
</bean>
```

The relational database that Cloud Foundry actually uses depends on the service instance you explicitly bind to your application when you deploy it: MySQL or Postgres. Cloud Foundry creates either a commons DBCP or Tomcat datasource depending on which datasource implementation it finds on the classpath.

Cloud Foundry internally generates values for the following properties: `driverClassName`, `url`, `username`, `password`, `validationQuery`.

#### Manual Configuration in Java

To configure a database service in Java configuration, create a `@Configuration` class with a `@Bean` method to return a `javax.sql.DataSource` bean. The bean can be created by helper classes in the `spring-cloud` library, as shown here:

```
@Configuration
public class DataSourceConfig {
 @Bean
 public DataSource dataSource() {
 CloudFactory cloudFactory = new CloudFactory();
 Cloud cloud = cloudFactory.getCloud();
 String serviceID = cloud.getServiceID();
 return cloud.getServiceConnector(serviceID, DataSource.class, null);
 }
}
```

### MongoDB

## Auto-Reconfiguration

You must use Spring Data MongoDB 1.0 M4 or later for auto-reconfiguration to work.

Auto-reconfiguration occurs if Cloud Foundry detects an `org.springframework.data.mongodb.MongoDbFactory` bean in the Spring application context. The following snippet of a Spring XML application context file shows an example of defining this type of bean which Cloud Foundry will detect and potentially auto-reconfigure:

```
<mongo:db-factory
 id="mongoDbFactory"
 dbname="pwdtest"
 host="127.0.0.1"
 port="1234"
 username="test_user"
 password="test_pass" />
```

Cloud Foundry creates a `SimpleMongoDbFactory` with its own values for the following properties: `host`, `port`, `username`, `password`, `dbname`.

## Manual Configuration in Java

To configure a MongoDB service in Java configuration, create a `@Configuration` class with a `@Bean` method to return an `org.springframework.data.mongodb.MongoDbFactory` bean from Spring Data MongoDB. The bean can be created by helper classes in the `spring-cloud` library, as shown here:

```
@Configuration
public class MongoConfig {

 @Bean
 public MongoDbFactory mongoDbFactory() {
 CloudFactory cloudFactory = new CloudFactory();
 Cloud cloud = cloudFactory.getCloud();
 MongoServiceInfo serviceInfo = (MongoServiceInfo) cloud.getServiceInfo("my-mongodb");
 String serviceID = serviceInfo.getID();
 return cloud.getServiceConnector(serviceID, MongoDbFactory.class, null);
 }

 @Bean
 public MongoTemplate mongoTemplate() {
 return new MongoTemplate(mongoDbFactory());
 }
}
```

## Redis

### Auto-Configuration

You must be using Spring Data Redis 1.0 M4 or later for auto-configuration to work.

Auto-configuration occurs if Cloud Foundry detects a `org.springframework.data.redis.connection.RedisConnectionFactory` bean in the Spring application context. The following snippet of a Spring XML application context file shows an example of defining this type of bean which Cloud Foundry will detect and potentially auto-configure:

```
<bean id="redis"
 class="org.springframework.data.redis.connection.jedis.JedisConnectionFactory"
 p:hostName="localhost" p:port="6379" />
```

Cloud Foundry creates a `JedisConnectionFactory` with its own values for the following properties: `host`, `port`, `password`. This means that you must package the Jedis JAR in your application. Cloud Foundry does not currently support the JRedis and RJC implementations.

## Manual Configuration in Java

To configure a Redis service in Java configuration, create a `@Configuration` class with a `@Bean` method to return an `org.springframework.data.redis.connection.RedisConnectionFactory` bean from Spring Data Redis. The bean can be created by helper classes in the `spring-cloud`

library, as shown here:

```
@Configuration
public class RedisConfig {

 @Bean
 public RedisConnectionFactory redisConnectionFactory() {
 CloudFactory cloudFactory = new CloudFactory();
 Cloud cloud = cloudFactory.getCloud();
 RedisServiceInfo serviceInfo = (RedisServiceInfo) cloud.getServiceInfo("my-redis");
 String serviceID = serviceInfo.getID();
 return cloud.getServiceConnector(serviceID, RedisConnectionFactory.class, null);
 }

 @Bean
 public RedisTemplate redisTemplate() {
 return new StringRedisTemplate(redisConnectionFactory());
 }
}
```

## RabbitMQ

### Auto-Configuration

You must be using Spring AMQP 1.0 or later for auto-configuration to work. Spring AMQP provides publishing, multi-threaded consumer generation, and message conversion. It also facilitates management of AMQP resources while promoting dependency injection and declarative configuration.

Auto-configuration occurs if Cloud Foundry detects an `org.springframework.amqp.rabbit.connection.ConnectionFactory` bean in the Spring application context. The following snippet of a Spring application context file shows an example of defining this type of bean which Cloud Foundry will detect and potentially auto-configure:

```
<rabbit:connection-factory
 id="rabbitConnectionFactory"
 host="localhost"
 password="testpwd"
 port="1238"
 username="testuser"
 virtual-host="virthost" />
```

Cloud Foundry creates an `org.springframework.amqp.rabbit.connection.CachingConnectionFactory` with its own values for the following properties: `host`, `virtual-host`, `port`, `username`, `password`.

### Manual Configuration in Java

To configure a RabbitMQ service in Java configuration, create a `@Configuration` class with a `@Bean` method to return an `org.springframework.amqp.rabbit.connection.ConnectionFactory` bean from the Spring AMQP library. The bean can be created by helper classes in the `spring-cloud` library, as shown here:

```
@Configuration
public class RabbitConfig {

 @Bean
 public ConnectionFactory rabbitConnectionFactory() {
 CloudFactory cloudFactory = new CloudFactory();
 Cloud cloud = cloudFactory.getCloud();
 AmqpServiceInfo serviceInfo = (AmqpServiceInfo) cloud.getServiceInfo("my-rabbit");
 String serviceID = serviceInfo.getID();
 return cloud.getServiceConnector(serviceID, ConnectionFactory.class, null);
 }

 @Bean
 public RabbitTemplate rabbitTemplate(ConnectionFactory connectionFactory) {
 return new RabbitTemplate(connectionFactory);
 }
}
```




## Cloud Foundry Java Client Library

Page last updated:

### Introduction

This is a guide to using the [Cloud Foundry Java Client Library](#) to manage an account on a Cloud Foundry instance.

 **Note:** The 1.1.x versions of the Cloud Foundry Java Client Library work with apps using Spring 4.x, and the 1.0.x versions of the Cloud Foundry Java Client Library work with apps using Spring 3.x. Both versions are available in the [source repository](#) on GitHub.

### Adding the Library

Visit the [Cloud Foundry Java Client Library](#) GitHub page to obtain the correct components.

Most projects need two dependencies: the Operations API and an implementation of the Client API. Refer to the following sections for more information about how to add the Cloud Foundry Java Client Library as dependencies to a Maven or Gradle project.

#### Maven

Add the `cloudfoundry-client-reactor` dependency (formerly known as `cloudfoundry-client-spring`) to your `pom.xml` as follows:

```
<dependencies>
 <dependency>
 <groupId>org.cloudfoundry</groupId>
 <artifactId>cloudfoundry-client-reactor</artifactId>
 <version>2.0.0.BUILD-SNAPSHOT</version>
 </dependency>
 <dependency>
 <groupId>org.cloudfoundry</groupId>
 <artifactId>cloudfoundry-operations</artifactId>
 <version>2.0.0.BUILD-SNAPSHOT</version>
 </dependency>
 <dependency>
 <groupId>io.projectreactor</groupId>
 <artifactId>reactor-core</artifactId>
 <version>2.5.0.BUILD-SNAPSHOT</version>
 </dependency>
 <dependency>
 <groupId>io.projectreactor</groupId>
 <artifactId>reactor-netty</artifactId>
 <version>2.5.0.BUILD-SNAPSHOT</version>
 </dependency>
 ...
</dependencies>
```

The artifacts can be found in the Spring release and snapshot repositories:

```
<repositories>
 <repository>
 <id>spring-releases</id>
 <name>Spring Releases</name>
 <url>http://repo.spring.io/release</url>
 </repository>
 ...
</repositories>
```

```
<repositories>
 <repository>
 <id>spring-snapshots</id>
 <name>Spring Snapshots</name>
 <url>http://repo.spring.io/snapshot</url>
 <snapshots>
 <enabled>true</enabled>
 </snapshots>
 </repository>
 ...
</repositories>
```

## Gradle

Add the `cloudfoundry-client-reactor` dependency to your `build.gradle` file as follows:

```
dependencies {
 compile 'org.cloudfoundry:cloudfoundry-client-reactor:2.0.0.BUILD-SNAPSHOT'
 compile 'org.cloudfoundry:cloudfoundry-operations:2.0.0.BUILD-SNAPSHOT'
 compile 'io.projectreactor:reactor-core:2.5.0.BUILD-SNAPSHOT'
 compile 'io.projectreactor:reactor-netty:2.5.0.BUILD-SNAPSHOT'
 ...
}
```

The artifacts can be found in the Spring release and snapshot repositories:

```
repositories {
 maven { url 'http://repo.spring.io/release' }
 ...
}
```

```
repositories {
 maven { url 'http://repo.spring.io/snapshot' }
 ...
}
```

## Sample Code

The following is a very simple sample application that connects to a Cloud Foundry instance, logs in, and displays some information about the Cloud Foundry account. When running the program, provide the Cloud Foundry target API endpoint, along with a valid user name and password as command-line parameters.

```
import org.cloudfoundry.client.lib.CloudCredentials;
import org.cloudfoundry.client.lib.CloudFoundryClient;
import org.cloudfoundry.client.lib.domain.CloudApplication;
import org.cloudfoundry.client.lib.domain.CloudService;
import org.cloudfoundry.client.lib.domain.CloudSpace;

import java.net.MalformedURLException;
import java.net.URI;
import java.net.URL;

public final class JavaSample {

 public static void main(String[] args) {
 String target = args[0];
 String user = args[1];
 String password = args[2];

 CloudCredentials credentials = new CloudCredentials(user, password);
 CloudFoundryClient client = new CloudFoundryClient(credentials, getTargetURL(target));
 client.login();

 System.out.printf("%nSpaces:%n");
 for (CloudSpace space : client.getSpaces()) {
 System.out.printf(" %s\t(%s)%n", space.getName(), space.getOrganization().getName());
 }

 System.out.printf("%nApplications:%n");
 for (CloudApplication application : client.getApplications()) {
 System.out.printf(" %s%n", application.getName());
 }

 System.out.printf("%nServices%n");
 for (CloudService service : client.getServices()) {
 System.out.printf(" %s\t(%s)%n", service.getName(), service.getLabel());
 }
 }

 private static URL getTargetURL(String target) {
 try {
 return URI.create(target).toURL();
 } catch (MalformedURLException e) {
 throw new RuntimeException("The target URL is not valid: " + e.getMessage());
 }
 }
}
```

For more details about the Cloud Foundry Java Client Library, visit the [source repository](#) in GitHub. The [domain package](#) shows the objects that you can query and inspect.



## .NET Core Buildpack

Page last updated:

This topic describes how to push Cloud Foundry apps using the .NET Core buildpack. You can find supported ASP.NET Core versions in the [.NET Core buildpack release notes](#).

Pivotal Application Service for Windows (PASW) automatically uses the .NET Core buildpack when one or more of the following conditions are met:

- The pushed app contains one or more `*.csproj` or `*.fsproj` files.
- The app is pushed from the output directory of the `dotnet publish` command.

For information about deploying different types of .NET apps, follow the links in the table below.

| Type of .NET App                                                                                  | Buildpack                 |
|---------------------------------------------------------------------------------------------------|---------------------------|
| ASP.NET MVC<br>ASP.NET Web Forms<br>ASP.NET WebAPI Apps<br>Windows Communication Foundation (WCF) | <a href="#">HWC</a>       |
| .NET Console                                                                                      | <a href="#">Binary</a>    |
| .NET Core pushed to Linux stack                                                                   | <a href="#">.NET Core</a> |
| .NET Core pushed to Windows stack                                                                 | <a href="#">Binary</a>    |

## Push an App

Follow the steps below to push your app.

1. Run `cf push APP-NAME` command to push your app, where `APP-NAME` is the name you want to give your app. For example:

```
$ cf push my-app
Creating app my-app in org sample-org / space sample-space as username@example.com...
OK
...
requested state: started
instances: 1/1
usage: 1GB x 1 instances
urls: my-app.example.com
```

If your PASW deployment does not have the .NET Core buildpack installed or the installed version is out of date, push your app with the `-b` option to specify the buildpack:

```
cf push APP-NAME -b https://github.com/cloudfoundry/dotnet-core-buildpack.git
```

Where `APP-NAME` is the name of your app.

2. Find the URL of your app in the output from the push command and navigate to it to see your app running. In the example above, `my-app.example.com` is the URL of your app.

For a basic example app, see [ASP.NET Core getting started app](#) in GitHub.

## Source-Based, Non-Published Deployments

When using this workflow, you push the source code for your app to Cloud Foundry by running the `cf push` command. Note that for a source-based, non-published deployment, you push the source code for your app, not the output directory of the `dotnet publish` command.

The source-based, non-published workflow ensures the buildpack can keep all your dependencies in sync and up to date. For additional information about using source-based, non-published deployments, see the following sections:

- [Deploy Apps with Multiple Projects](#)
- [Use Non-Default Package Sources](#)

- [Disable and Clear Your NuGet Package Cache](#)

## Deploy Apps with Multiple Projects

If you want to deploy an app that contains multiple projects, you must specify your main project for the buildpack to run.

To specify your main project, create a `.deployment` file in the root folder of the app that sets the path to the main project in the following format:

```
[config]
project = PATH-TO-YOUR-MAIN-PROJECT
```

Where `PATH-TO-YOUR-MAIN-PROJECT` is the location of your main project. Set `project` to the `*.csproj` or `*.fsproj` file of your main project.

For example, if an app contains three projects in the `src` folder, the main project `MyApp.Web` as well as `MyApp.DAL` and `MyApp.Services`, format the `.deployment` file as follows:

```
[config]
project = src/MyApp.Web/MyApp.Web.csproj
```

In this example, the buildpack automatically compiles the `MyApp.DAL` and `MyApp.Services` projects if the `MyApp.Web.csproj` file of the main project lists them as dependencies. The buildpack attempts to execute the main project using the `dotnet run -p src/MyApp.Web/MyApp.Web.csproj` command.

## Use Non-Default Package Sources

If you want to deploy an app that uses non-default package sources, you must specify those package sources in the `NuGet.Config` file. For information about `NuGet.Config`, see [nuget.config reference](#) in the Microsoft documentation.

## Disable and Clear Your NuGet Package Cache

You may need to disable NuGet package caching or clear NuGet packages cached in the staging environment in one of the following scenarios:

- Your app fails to stage because it runs out of space, exceeding the maximum allowable disk quota.
- You have added pre-release packages to test a new feature and then decided to revert back to the main NuGet feed. You may need to remove the packages you changed from the cache to avoid conflicts.

Disabling NuGet caching clears any existing NuGet dependencies from the staging cache and prevents the buildpack from adding NuGet dependencies to the staging cache.

To disable NuGet package caching, set the `CACHE_NUGET_PACKAGES` environment variable to `false`. If the variable is not set, no change is required.

To set `CACHE_NUGET_PACKAGES` to `false`, do one of the following:

- Locate your app manifest, `manifest.yml`, and set the `CACHE_NUGET_PACKAGES` environment variable to `false`:

```

applications:
- name: sample-aspnetcore-app
 memory: 512M
 env:
 CACHE_NUGET_PACKAGES: false
```

- Use `cf set-env` to set the `CACHE_NUGET_PACKAGES` environment variable on the command line:

```
cf set-env APP-NAME CACHE_NUGET_PACKAGES false
```

Where `APP-NAME` is the name of your app.

For more information, see the [Environment Variables](#) section of the *Deploying with Application Manifests* topic.

## Framework-Dependent Deployments

For a framework-dependent deployment (FDD), you deploy only your app and third-party dependencies. Cloud Foundry recommends using this workflow if you deploy an app in an offline setting. For information about deploying FDDs, see [Framework-dependent deployments \(FDD\)](#) in the Microsoft documentation.


To deploy an FDD using the buildpack, do the following:

1. Publish the app by running the `dotnet publish` command:

```
dotnet publish [-f YOUR-FRAMEWORK] [-c Release]
```


Where `YOUR-FRAMEWORK` is your target framework.

2. Navigate to the `bin/Debug/Release/YOUR-FRAMEWORK/YOUR-RUNTIME/publish` directory. Alternatively, if your app uses a `manifest.yml`, specify a path to the output folder of `dotnet publish`. This allows you to push your app from any directory.
3. Push your app.

 **Note:** Set `applyPatches: false` in `*.runtimeconfig.json` only if you want to pin your .NET Framework to a specific version. This prevents your app from receiving updates to the runtime version and assemblies.

## Self-Contained Deployments

For a self-contained deployment (SCD), you deploy your app, third-party dependencies, and the version of .NET Core that you used to build your app. For information about SCDs, see [Self-contained deployments \(SCD\)](#) in the Microsoft documentation.

 **Note:** Cloud Foundry does not recommend using the SCD workflow. Because this workflow results in a pre-published binary, the buildpack is not able to keep all your dependencies in sync and up to date.

When using the SCD workflow for deploying your app, you must specify a runtime in the `dotnet publish` command. For example:

```
$ dotnet publish -r ubuntu14.04-x64
```

In addition, you must include the specified runtime in the `RuntimeIdentifiers` section of the project file.

## Specify .NET Core SDKs

To pin the .NET Core SDK to a specific version or version line, create a `buildpack.yml` file at the app root and add your SDK version in one of the following formats:


```
dotnet-core:
sdk: 2.1.201
```

```
dotnet-core:
sdk: 2.1.x
```

```
dotnet-core:
sdk: 2.x
```

The buildpack chooses what SDK to install based on the files present at the app root in the following order of precedence:

1. `buildpack.yml`
2. `global.json`
3. `*.fsproj`

 **Note:** The app respects the SDK version specified in `global.json` at runtime. If you provide versions in the `global.json` and `buildpack.yml` files, ensure that you specify the same versions in both files.

## Specify .NET Runtime Versions

This section explains how to specify a .NET Runtime version for source-based and framework-dependent apps.

### Source-Based Apps

For source-based apps, specify a minor version of the .NET Runtime. Do not specify a patch version because buildpacks contain only the two most recent patch versions of each minor version.

If you want to lock the .NET Runtime version, add the following to your `.csproj` or `.fsproj` file:

```
<PropertyGroup>
 <TargetFramework>netcoreapp2.1</TargetFramework>
 <RuntimeFrameworkVersion>2.1.*</RuntimeFrameworkVersion>
</PropertyGroup>
```

### Framework-Dependent Apps


In your `.runtimeconfig.json` app, the latest .NET Runtime patch version is used by default. If you want to set a specific .NET Runtime version, add the `applyPatches` property and set it to `false` as follows:

```
{
 "runtimeOptions": {
 "tfm": "netcoreapp2.0",
 "framework": {
 "name": "Microsoft.NETCore.App",
 "version": "2.0.0"
 },
 },
 "applyPatches": false
}
```

## Push an App in a Disconnected Environment

For offline environments, Cloud Foundry recommends using the [Framework-Dependent Deployments](#) workflow. This workflow enables the deployed app to use the latest runtime provided by the offline buildpack.

## Maintain ASP.NET Core Assemblies

 **Note:** This section applies only to source-based and framework-dependent deployments.

For maintaining ASP.NET Core assemblies, update your `.csproj` file with the following:


```
<PropertyGroup>
 <PublishWithAspNetCoreTargetManifest>>false</PublishWithAspNetCoreTargetManifest>
</PropertyGroup>
```

This results in a fully vendored app that requires fewer buildpack updates.

Alternatively, to keep your SDK up to date, you can set `buildpack.yml` to the .NET SDK line you want to use:

```

dotnet-core:
 sdk: 2.0.x
```

 **Note:** `2.0.x` ASP.NET Core assemblies are released in the `2.1.200` - `2.1.299` SDK versions, and `2.1.x` assemblies are released in the `2.1.300` and above SDK versions.

## Configure the Listen Port

For your .NET Core app to work on PASW, you must modify the `Main` method to configure the app to listen on the port specified by the `$PORT` environment variable. PASW sets this environment variable automatically.

1. Open the file that contains your `Main` method.
2. Add a `using` statement to the top of the file.

```
using Microsoft.Extensions.Configuration;
```

3. Add the following lines before the line `var host = new WebHostBuilder()`:

```
var config = new ConfigurationBuilder()
 .AddCommandLine(args)
 .Build();
```

4. Add the following line after `.UseKestrel()`:

```
.UseConfiguration(config)
```

This allows the buildpack to pass the correct port from `$PORT` to the app when running the initial startup command.

5. Add `Microsoft.Extensions.Configuration.CommandLine` as a dependency in `*.csproj`:

```
<PackageReference Include="Microsoft.Extensions.Configuration.CommandLine">
 <Version>VERSION</Version>
</PackageReference>
```

In the above example, replace `VERSION` with the version of the package to use. To find a list of valid versions, navigate to <https://www.nuget.org>.

6. If your app requires any other files at runtime, such as JSON configuration files, add them to the `include` section of `copyToOutput`.
7. Save your changes.

With these changes, the `dotnet run` command copies your app `Views` to the build output where the .NET CLI can find them. Refer to the following example


`Main` method:

```
public static void Main(string[] args)
{
 var config = new ConfigurationBuilder()
 .AddCommandLine(args)
 .Build();

 var host = new WebHostBuilder()
 .UseKestrel()
 .UseConfiguration(config)
 .UseContentRoot(Directory.GetCurrentDirectory())
 .UseStartup<Startup>()
 .Build();
 host.Run();
}
```

## Add Custom Libraries

If your app requires external shared libraries that are not provided by the rootfs or the buildpack, you must place the libraries in an `ld_library_path` directory at the app root.


 **Note:** You must keep these libraries up to date. They do not update automatically.

The .NET Core buildpack automatically adds the directory `<app-root>/ld_library_path` to `LD_LIBRARY_PATH` so that your app can access these libraries at runtime.

## NGINX Buildpack

Page last updated:

This topic describes how to push your NGINX app to Cloud Foundry and how to configure your NGINX app to use the NGINX buildpack.

 **Note:** This buildpack is not distributed as part of Pivotal Application Service (PAS) v2.4. However, it is supported for use with PAS. You can download an offline version of this buildpack from [Pivotal Network](#).

## Push an App

If your app contains an `nginx.conf` file, Cloud Foundry automatically uses the NGINX buildpack when you run `cf push` to deploy your app.

If your Cloud Foundry deployment does not have the NGINX buildpack installed or the installed version is outdated, run `cf push YOUR-APP -b https://github.com/cloudfoundry/nginx-buildpack.git` to deploy your app with the current buildpack. Replace `YOUR-APP` with the name of your app.

For example:

```
$ cf push my-app -b https://github.com/cloudfoundry/nginx-buildpack.git
```

## Configure NGINX

We recommend that you use the default NGINX directory structure for your NGINX webserver. You can view this directory structure in the [nginx-buildpack](#) repository in GitHub.

The NGINX webserver setup includes the following:

- A root folder for all static web content
- A MIME type configuration file
- An NGINX configuration file
- A `buildpack.yml` YAML file that defines the version of NGINX to use. As an example, see [buildpack.yml](#) in the Cloud Foundry NGINX Buildpack repository in GitHub.

You should make any custom configuration changes based on these default files to ensure compatibility with the buildpack.

## Create the nginx.conf File

Use the templating syntax when you create an `nginx.conf` file. This templating syntax loads modules and binds to ports based on values known at launch time.

### Port

Use `{{port}}` to set the port to listen on. At launch time, `{{port}}` will interpolate in the value of `$PORT`.

 **Note:** You must use `{{port}}` in your `nginx.conf` file.

For example, to set an NGINX server to listen on `$PORT`, include the following in your `nginx.conf` file:

```
server {
 listen {{port}};
}
```

## Environment Variables

To use an environment variable, include `{{env "YOUR-VARIABLE"}}`. Replace `YOUR-VARIABLE` with the name of an environment variable. At staging and at launch, the current value of the environment variable is retrieved.

For example, include the following in your `nginx.conf` file to enable or disable GZipping based on the value of `GZIP_DOWNLOADS`:

```
gzip {{env "GZIP_DOWNLOADS"}};
```

- If you set `GZIP_DOWNLOADS` to `off`, NGINX does not GZip files.
- If you set `GZIP_DOWNLOADS` to `on`, NGINX GZips files.

## Loading Dynamic Modules

To load an NGINX module, use the following syntax in your app's `nginx.conf` file:

```
{{module "MODULE-NAME"}}
```

If you have provided a module in a `modules` directory located at the root of your app, the buildpack instructs NGINX to load that module. If you have not provided a module, the buildpack instructs NGINX to search for a matching built-in module.


As of v0.0.5 of the buildpack, the `ngx_stream_module` is available as a built-in module.

For example, to load a custom module named `ngx_hello_module`, provide a `modules/ngx_hello_module.so` file in your app directory and add the following to the top of your `nginx.conf` file:

```
{{module "ngx_hello_module"}}
```

To load a built-in module like `ngx_stream_module`, add the following to the top of your `nginx.conf` file. You do not need to provide an `ngx_stream_module.so` file:

```
{{module "ngx_stream_module"}}
```

 **Note:** To name your modules directory something other than `modules`, use the NGINX `load_module` directive, providing a path to the module relative to the location of your `nginx.conf` file. For example:

```
load_module
some_module_dir/my_module.so
```

## Buildpack Support

The following resources can assist you when using the NGINX buildpack or when developing your own NGINX buildpack:

- **NGINX Buildpack Repository in GitHub:** Find more information about using and extending the NGINX buildpack in the [NGINX buildpack](#) GitHub repository.
- **Release Notes:** Find current information about this buildpack on the [NGINX buildpack release page](#) in GitHub.
- **Slack:** Join the #buildpacks channel in the [Cloud Foundry Slack community](#).



## Node.js Buildpack

Page last updated:

Use the Node.js buildpack with Node or JavaScript apps.

You must install the [Cloud Foundry Command Line Interface tool](#) (cf CLI) to run some of the commands listed in this topic.

## Push Node.js Apps

Cloud Foundry automatically uses the Node.js buildpack if it detects a `package.json` file in the root directory of your project.

The `-b` option lets you specify a buildpack to use with the `cf push` command. If your Cloud Foundry deployment does not have the Node.js buildpack installed or the installed version is out of date, run `cf push APP-NAME -b https://github.com/cloudfoundry/nodejs-buildpack`, where `APP-NAME` is the name of your app, to push your app with the latest version of the buildpack.

For example:

```
$ cf push my-nodejs-app -b https://github.com/cloudfoundry/nodejs-buildpack
```

For more detailed information about deploying Node.js apps, see the following topics:

- [Tips for Node.js Developers](#)
- [Environment Variables Defined by the Node Buildpack](#)
- [Configuring Service Connections for Node](#)
- [Node.js Buildpack Source Code on GitHub](#)

## Supported Versions

For a list of supported Node versions, see the Node.js Buildpack [release notes](#) on GitHub.

## Specify a Node.js Version

To specify a Node.js version, set the `engines.node` in the `package.json` file to the semantic versioning specification (semver) range or the specific version of Node you are using.

Example showing a semver range:

```
"engines": {
 "node": "6.9.x"
}
```

Example showing a specific version:

```
"engines": {
 "node": "6.9.0"
}
```

If you try to use a version that is not currently supported, staging your app fails with the following error message:

```
Could not get translated url, exited with: DEPENDENCY_MISSING_IN_MANIFEST:...
!
! exit
!
Staging failed: Buildpack compilation step failed
```

## Specify an npm Version

To specify an npm version, set `engines.npm` in the `package.json` file to the semantic versioning specification (semver) range or the specific version of npm you are using:

Example showing a semver range:

```
"engines": {
 "node": "6.9.x",
 "npm": "2.15.x"
}
```

Example showing a specific version:

```
"engines": {
 "node": "6.9.0",
 "npm": "2.15.1"
}
```

If you do not specify an npm version, your app uses the default npm packaged with the Node.js version used by your app, as specified on the [Node.js releases](#) page.

If your environment cannot connect to the Internet and you specified a non-supported version of npm, the buildpack fails to download npm and you see the following error message:

```
We're unable to download the version of npm you've provided (...).
Please remove the npm version specification in package.json (...)
Staging failed: Buildpack compilation step failed
```


## Vendor App Dependencies

To vendor dependencies for an app using the Node.js buildpack, run `npm install` from your app directory. This command vendors dependencies into the `node_modules` directory of your app directory.

For example, the following example vendors dependencies into the `my-nodejs-app/node_modules` directory:

```
$ cd my-nodejs-app
$ npm install
```

The `cf push` command uploads the vendored dependencies with the app.

 **Note:** For an app to run in a disconnected environment, it must vendor its dependencies. For more information, see [Disconnected environments](#).

## Using Yarn in a Disconnected Environment

Versions 1.5.28 and later of the Node.js buildpack include the ability to use the package manager [Yarn](#) in a disconnected environment. To do so, you must mirror the Yarn registry locally:

```
$ cd APP-DIR
$ yarn config set yarn-offline-mirror ./npm-packages-offline-cache
$ yarn config set yarn-offline-mirror-pruning true
$ cp ~/.yarnrc .
$ rm -rf node_modules/ yarn.lock # if they were previously generated
$ yarn install
```

When you push the app, the buildpack looks for an `npm-packages-offline-cache` directory at the top level of the app directory. If this directory exists, the buildpack runs Yarn in offline mode. Otherwise, it runs Yarn normally, which requires an Internet connection.

For more information about using an offline mirror with Yarn, see the [Yarn Blog](#).

## Integrity Check

By default, the Node.js buildpack uses npm to download dependencies. Note that npm does not perform integrity checks of the downloaded packages, which is a [security risk](#).

If missing dependencies are detected, the buildpack runs `npm install` for non-vendored dependencies or `npm rebuild` for dependencies that are already vendored. This may result in code being downloaded and executed without verification.

You can use Yarn as an alternative that verifies dependencies.

## OpenSSL Support

The [nodejs-buildpack](#) packages binaries of Node.js with OpenSSL that are statically linked. The Node.js buildpack supports Node.js 4.x and later, which relies on the Node.js release cycle to provide OpenSSL updates. The [binary-builder](#) enables [static OpenSSL compilation](#).

## Proxy Support

If you need to use a proxy to download dependencies during staging, you can set the `http_proxy` and/or `https_proxy` environment variables. For more information, see [Proxy Usage](#).

## BOSH Configured Custom Trusted Certificate Support

Node.js hardcodes root CA certs in its source code. To use [BOSH configured custom trusted certificates](#), a developer must pass the specified CAs to the [tls.connect](#) function as extra arguments.

## Help and Support

Join the #buildpacks channel in our [Slack community](#) if you need any further assistance.

For more information about using and extending the Node.js buildpack in Cloud Foundry, see the [Node.js GitHub repository](#).

You can find current information about this buildpack in the Node.js buildpack [release page](#) in GitHub.

## Tips for Node.js Applications

Page last updated:

This topic provides Node-specific information to supplement the general guidelines in the [Deploy an Application](#) topic.

## About the Node.js Buildpack

For information about using and extending the Node.js buildpack in Cloud Foundry, see the [nodejs-buildpack repository](#).

You can find current information about this buildpack on the Node.js buildpack [release page](#) in GitHub.

The buildpack uses a default Node.js version. To specify the versions of Node.js and npm an app requires, edit the app's `package.json`, as described in “node.js and npm versions” in the [nodejs-buildpack repository](#).

## Application Package File

Cloud Foundry expects a `package.json` in your Node.js app. You can specify the version of Node.js you want to use in the `engine` node of your `package.json` file.

In general, Cloud Foundry supports the two most recent versions of Node.js. See the GitHub [Node.js buildpack page](#) for current information.

Example `package.json` file:

```
{
 "name": "first",
 "version": "0.0.1",
 "author": "Demo",
 "dependencies": {
 "express": "3.4.8",
 "consolidate": "0.10.0",
 "swig": "1.3.2"
 },
 "engines": {
 "node": "0.12.7",
 "npm": "2.7.4"
 }
}
```

## Application Port

You must use the PORT environment variable to determine which port your app should listen on. To also run your app locally, set the default port as

`3000`.

```
app.listen(process.env.PORT || 3000);
```

## Low Memory Environments

When running node apps, you might notice that instances are occasionally restarted due to memory constraints. Node does not know how much memory it is allowed to use, and thus sometimes allows the garbage collector to wait past the allowed amount of memory. To resolve this issue, set the `OPTIMIZE_MEMORY` environment variable to `true` (requires node v6.12.0 or greater). This sets `max_old_space_size` based on the available memory in the instance.

```
$ cf set-env my-app OPTIMIZE_MEMORY true
```

## Application Start Command

Node.js apps require a start command. You can specify the web start command for a Node.js app in a Procfile or in the app deployment manifest. For more information about Procfiles, see the [Configuring a Production Server](#) topic.

The first time you deploy, you are asked if you want to save your configuration. This saves a `manifest.yml` in your app with the settings you entered during the initial push. Edit the `manifest.yml` file and create a start command as follows:

```

applications:
- name: my-app
 command: node my-app.js
... the rest of your settings ...
```

Alternately, specify the start command with `cf push -c`.

```
$ cf push my-app -c "node my-app.js"
```

## Application Bundling

You do not need to run `npm install` before deploying your app. Cloud Foundry runs it for you when your app is pushed. You can, if you prefer, run `npm install` and create a `node_modules` folder inside of your app.

## Solve Discovery Problems

If Cloud Foundry does not automatically detect that your app is a Node.js app, you can override auto-detection by specifying the Node.js buildpack.

Add the buildpack into your `manifest.yml` and re-run `cf push` with your manifest:

```

applications:
- name: my-app
 buildpack: https://github.com/cloudfoundry/nodejs-buildpack
... the rest of your settings ...
```

Alternately, specify the buildpack on the command line with `cf push -b`:

```
$ cf push my-app -b https://github.com/cloudfoundry/nodejs-buildpack
```

## Bind Services

Refer to [Configure Service Connections for Node.js](#).

## Environment Variables

You can access environments variable programmatically.

For example, you can obtain `VCAP_SERVICES` as follows:

```
process.env.VCAP_SERVICES
```

Environment variables available to you include both those [defined by the system](#) and those defined by the Node.js buildpack, as described below.

## BUILD\_DIR

Directory into which Node.js is copied each time a Node.js app is run.

## CACHE\_DIR

Directory that Node.js uses for caching.

## PATH

The system path used by Node.js.

```
PATH=/home/vcap/app/bin:/home/vcap/app/node_modules/.bin:/bin:/usr/bin
```

## Environment Variables Defined by the Node Buildpack

Page last updated:

Pivotal Application Service provides configuration information to applications through environment variables. This topic describes the additional environment variables provided by the Node buildpack.

For more information about the standard environment variables provided by Pivotal Application Service, see the [Cloud Foundry Environment Variables](#) topic.

### Node Buildpack Environment Variables

The following table describes the environment variables provided by the Node buildpack.

| Environment Variable   | Description                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>BUILD_DIR</code> | The directory where Node.js is copied each time a Node.js application runs.                                          |
| <code>CACHE_DIR</code> | The directory Node.js uses for caching.                                                                              |
| <code>PATH</code>      | The system path used by Node.js: <code>PATH=/home/vcap/app/bin:/home/vcap/app/node_modules/.bin:/bin:/usr/bin</code> |

## Configuring Service Connections for Node.js

Page last updated:

This guide is for developers who wish to bind a data source to a Node.js application deployed and running on Cloud Foundry.

### Parse VCAP\_SERVICES for Credentials

You must parse the VCAP\_SERVICES environment variable in your code to get the required connection details such as host address, port, user name, and password.

For example, if you are using PostgreSQL, your VCAP\_SERVICES environment variable might look something like this:

```
{
 "mypostgres": [{
 "name": "myinstance",
 "credentials": {
 "uri": "postgres://myusername:mypassword@host.example.com:5432/serviceinstance"
 }
 }]
}
```

This example JSON is simplified; yours may contain additional properties.

### Parse with cfenv

The `cfenv` package provides access to Cloud Foundry application environment settings by parsing all the relevant environment. The settings are returned as JavaScript objects. `cfenv` provides reasonable defaults when running locally, as well as when running as a Cloud Foundry application.

- <https://www.npmjs.org/package/cfenv> [↗](#)

### Manual Parsing

First, parse the VCAP\_SERVICES environment variable.

For example:

```
var vcap_services = JSON.parse(process.env.VCAP_SERVICES)
```

Then pull out the credential information required to connect to your service. Each service packages requires different information. If you are working with Postgres, for example, you will need a `uri` to connect. You can assign the value of the `uri` to a variable as follows:

```
var uri = vcap_services.mypostgres[0].credentials.uri
```

Once assigned, you can use your credentials as you would normally in your program to connect to your database.

## Connecting to a Service

You must include the appropriate package for the type of services your application uses. For example:

- Rabbit MQ via the [amqp](#) [↗](#) module
- Mongo via the [mongodb](#) [↗](#) and [mongoose](#) [↗](#) modules
- MySQL via the [mysql](#) [↗](#) module
- Postgres via the [pg](#) [↗](#) module
- Redis via the [redis](#) [↗](#) module



## Add the Dependency to package.json

Edit `package.json` and add the intended module to the `dependencies` section. Normally, only one would be necessary, but for the sake of the example we will add all of them:

```
{
 "name": "hello-node",
 "version": "0.0.1",
 "dependencies": {
 "express": "*",
 "mongodb": "*",
 "mongoose": "*",
 "mysql": "*",
 "pg": "*",
 "redis": "*",
 "amqp": "*"
 },
 "engines": {
 "node": "0.8.x"
 }
}
```

You must run `npm shrinkwrap` to regenerate your `npm-shrinkwrap.json` file after you edit `package.json`.

## PHP Buildpack

Page last updated:

Use the PHP buildpack with PHP or HHVM runtimes.

## Supported Software and Versions

The [release notes page](#) has a list of currently supported modules and packages.

- **PHP Runtimes**
  - php-cli
  - php-cgi
  - php-fpm
- **Third-Party Modules**
  - New Relic, in connected environments only.

## Push an App

### 30 Second Tutorial

Getting started with this buildpack is easy. With the [cf command line utility](#) installed, open a shell, change directories to the root of your PHP files and push your application using the argument `-b https://github.com/cloudfoundry/php-buildpack.git`.

Example:

```
$ mkdir my-php-app
$ cd my-php-app
$ cat << EOF > index.php
<?php
 phpinfo();
?>
EOF
$ cf push -m 128M -b https://github.com/cloudfoundry/php-buildpack.git my-php-app
```

Change **my-php-app** in the above example to a unique name on your target Cloud Foundry instance to prevent a hostname conflict error and failed push.

The example above creates and pushes a test application, **my-php-app**, to Cloud Foundry. The `-b` argument instructs CF to use this buildpack. The remainder of the options and arguments are not specific to the buildpack, for questions on those consult the output of `cf help push`.

Here's a breakdown of what happens when you run the example above.

- On your PC:
  - It will create a new directory and one PHP file, which just invokes `phpinfo()`
  - Run `cf` to push your application. This will create a new application with a memory limit of 128M (more than enough here) and upload our test file.
- Within Cloud Foundry:
  - The buildpack is executed.
  - Application files are copied to the `htdocs` folder.
  - Apache HTTPD & PHP are downloaded, configured with the buildpack defaults and run.
  - Your application is accessible at the URL `http://my-php-app.example.com` (Replacing `example.com` with the domain of your public CF provider or private instance).

## More information about deploying

While the *30 Second Tutorial* shows how quick and easy it is to get started using the buildpack, it skips over quite a bit of what you can do to adjust, configure and extend the buildpack. The following sections and links provide a more in-depth look at the buildpack.

## Features

Here are some special features of the buildpack.

- Supports running commands or migration scripts prior to application startup.
- Supports an extension mechanism that allows the buildpack to provide additional functionality.
- Allows for application developers to provide custom extensions.
- Easy troubleshooting with the `BP_DEBUG` environment variable.
- Download location is configurable, allowing users to host binaries on the same network (i.e. run without an Internet connection)
- Smart session storage, defaults to file w/sticky sessions but can also use redis for storage.

## Examples

Here are some example applications that can be used with this buildpack.

- [php-info](#) This app has a basic index page and shows the output of `phpinfo()`.
- [PHPMyAdmin](#) A deployment of PHPMyAdmin that uses bound MySQL services.
- [PHPPgAdmin](#) A deployment of PHPPgAdmin that uses bound PostgreSQL services.
- [Drupal](#) A deployment of Drupal that uses bound MySQL service.
- [CodeIgniter](#) CodeIgniter tutorial application running on CF.
- [Stand Alone](#) An example which runs a standalone PHP script.
- [pgbouncer](#) An example which runs the PgBouncer process in the container to pool database connections.
- [phalcon](#) An example which runs a Phalcon based application.
- [composer](#) An example which uses Composer.

## Advanced Topics

See the following topics:

- [Tips for PHP Developers](#)
- [Getting Started Deploying PHP Apps](#)
- [PHP Buildpack Configuration](#)
- [Composer](#)
- [Sessions](#)
- [New Relic](#)

You can find the source for the buildpack on GitHub: <https://github.com/cloudfoundry/php-buildpack>

## Proxy Support

If you need to use a proxy to download dependencies during staging, you can set the `http_proxy` and/or `https_proxy` environment variables. For more information, see [Using a Proxy](#).

## BOSH Configured Custom Trusted Certificate Support

For versions of PHP 5.6.0 and later, the default certificate location is `/usr/lib/ssl/certs`, which symlinks to `/etc/ssl/certs`. Your platform operator can configure the platform to [add the custom certificates into the application container](#).

## Help and Support

Join the #buildpacks channel in our [Slack community](#) if you need any further assistance.

For more information about using and extending the PHP buildpack in Cloud Foundry, see the [php-buildpack GitHub repository](#).

You can find current information about this buildpack on the PHP buildpack [release page](#) in GitHub.

## License

The Cloud Foundry PHP Buildpack is released under version 2.0 of the [Apache License](#).

## Tips for PHP Developers

Page last updated:

### About the PHP Buildpack

For information about using and extending the PHP buildpack in Cloud Foundry, see the [php-buildpack Github repository](#).

You can find current information about this buildpack on the PHP buildpack [release page](#) in GitHub.

The buildpack uses a default PHP version specified in `.defaults/options.json` under the `PHP_VERSION` key.

To change the default version, specify the `PHP_VERSION` key in your app's `.bp-config/options.json` file.

## Getting Started Deploying PHP Apps

Page last updated:

This topic is intended to guide you through the process of deploying PHP apps to Pivotal Application Service. If you experience a problem deploying PHP apps, review the [Troubleshooting](#) section below.

## Getting Started

### Prerequisites

- Basic PHP knowledge
- The [Cloud Foundry Command Line Interface \(cf CLI\)](#) installed on your workstation

### A First PHP Application

```
$ mkdir my-php-app
$ cd my-php-app
$ cat << EOF > index.php
<?php
 phpinfo();
?>
EOF
$ cf push my-php-app -m 128M
```

Change “my-php-app” to a unique name or you may see an error and a failed push.

The example above creates and pushes a test application to Cloud Foundry.

Here is a breakdown of what happens when you run the example above:

- On your workstation...
  - It creates a new directory and one PHP file, which calls `phpinfo()`
  - Run `cf push` to push your application. This will create a new application with a memory limit of 128M and upload our test file.
- On Cloud Foundry...
  - The buildpack detects that your app is a php app
  - The buildpack is executed.
    - Application files are copied to the `htdocs` folder.
  - Apache HTTPD & PHP are downloaded, configured with the buildpack defaults, and run.
  - Your application is accessible at the default route. Use `cf app my-php-app` to view the url of your new app.

## Folder Structure

The easiest way to use the buildpack is to put your assets and PHP files into a directory and push it to PAS. This way, the buildpack will take your files and automatically move them into the `WEBDIR` (defaults to `htdocs`) folder, which is the directory where your chosen web server looks for the files.

### URL Rewriting

If you select Apache as your web server, you can include `.htaccess` files with your application.

Alternatively, you can [provide your own Apache or Nginx configurations](#).

## Prevent Access To PHP Files

The buildpack will put all of your files into a publicly accessible directory. In some cases, you might want to have PHP files that are not publicly accessible but are on the [include\\_path](#). To do that, create a `lib` directory in your project folder and place your protected files there.

For example:

```
$ ls -IRh
total 0
-rw-r--r-- 1 daniel staff 0B Feb 27 21:40 images
-rw-r--r-- 1 daniel staff 0B Feb 27 21:39 index.php
drwxr-xr-x 3 daniel staff 102B Feb 27 21:40 lib

./lib:
total 0
-rw-r--r-- 1 daniel staff 0B Feb 27 21:40 my.class.php <-- not public, http://app.cfapps.io/lib/my.class.php == 404
```

This comes with a catch. If your project legitimately has a `lib` directory, these files will not be publicly available because the buildpack does not copy a top-level `lib` directory into the `WEBDIR` folder. If your project has a `lib` directory that needs to be publicly available, then you have two options as follows:

### Option #1

In your project folder, create an `htdocs` folder (or whatever you've set for `WEBDIR`). Then move any files that should be publicly accessible into this directory. In the example below, the `lib/controller.php` file is publicly accessible.

Example:

```
$ ls -IRh
total 0
drwxr-xr-x 7 daniel staff 238B Feb 27 21:48 htdocs

./htdocs: <-- create the htdocs directory and put your files there
total 0
-rw-r--r-- 1 daniel staff 0B Feb 27 21:40 images
-rw-r--r-- 1 daniel staff 0B Feb 27 21:39 index.php
drwxr-xr-x 3 daniel staff 102B Feb 27 21:48 lib

./htdocs/lib: <-- anything under htdocs is public, including a lib directory
total 0
-rw-r--r-- 1 daniel staff 0B Feb 27 21:48 controller.php
```

Given this setup, it is possible to have both a public `lib` directory and a protected `lib` directory. The following example demonstrates this setup:

Example:

```
$ ls -IRh
total 0
drwxr-xr-x 7 daniel staff 238B Feb 27 21:48 htdocs
drwxr-xr-x 3 daniel staff 102B Feb 27 21:51 lib

./htdocs:
total 0
-rw-r--r-- 1 daniel staff 0B Feb 27 21:40 images
-rw-r--r-- 1 daniel staff 0B Feb 27 21:39 index.php
drwxr-xr-x 3 daniel staff 102B Feb 27 21:48 lib

./htdocs/lib: <-- public lib directory
total 0
-rw-r--r-- 1 daniel staff 0B Feb 27 21:48 controller.php

./lib: <-- protected lib directory
total 0
-rw-r--r-- 1 daniel staff 0B Feb 27 21:51 my.class.php
```

### Option #2

The second option is to pick a different name for the `LIBDIR`. This is a configuration option that you can set (it defaults to `lib`). Thus if you set it to something else such as `include`, your application's `lib` directory would no longer be treated as a special directory and it would be placed into `WEBDIR`.

(i.e. become public).

## Other Folders

Beyond the `WEBDIR` and `LIBDIR` directories, the buildpack also supports a `.bp-config` directory and a `.extensions` directory.

The `.bp-config` directory should exist at the root of your project directory and it is the location of application-specific configuration files. Application-specific configuration files override the default settings used by the buildpack. This link explains [application configuration files](#) in depth.

The `.extensions` directory should also exist at the root of your project directory and it is the location of application-specific custom extensions. Application-specific custom extensions allow you, the developer, to override or enhance the behavior of the buildpack. See the [php-buildpack README](#) in GitHub for more information about extensions.

## Troubleshooting

To troubleshoot problems using the buildpack, you can do one of the following:

1. Review the output from the buildpack. The buildpack writes basic information to stdout, for example the files that it downloads. The buildpack also writes information in the form of stack traces when a process fails.
2. Review the logs from the buildpack. The buildpack writes logs to disk. Follow the steps below to access these logs:
  - a. Run `cf ssh APP-NAME` to ssh into the app container, replacing `APP-NAME` with the name of your app.
  - b. Run `cat app/.bp/logs/bp.log` to view the logs.

```
$ cf ssh my-app
$ cat app/.bp/logs/bp.log
```

By default, log files contain more detail than output to stdout. Set the `BP_DEBUG` environment variable to `true` for more verbose logging. This instructs the buildpack to set its log level to `DEBUG`, and to output logs to stdout. Follow [Environment Variables documentation](#) to set `BP_DEBUG`.

## Increase Log Output with fpm.d

If you use [fpm.d](#), follow the steps below to configure `fpm` to redirect worker stdout and stderr into the logs.

1. Create a file in the `.bp-config/php/fpm.d/` directory of your app.
2. Add `catch_workers_output=yes` to the file you created.
3. Push your app.

For more information about allowed configuration settings in the `.bp-config/php/fpm.d` directory, see the [List of global php-fpm.conf directives](#).

You can see an example [fpm fixture and configuration file](#) in the php-buildpack GitHub repository.



## PHP Buildpack Configuration

Page last updated:

### Defaults

The PHP buildpack stores all of its default configuration settings in the [defaults](#) directory.

### options.json

The `options.json` file is the configuration file for the buildpack itself. It instructs the buildpack what to download, where to download it from, and how to install it. It allows you to configure package names and versions (i.e. PHP, HTTPD, or Nginx versions), the web server to use (HTTPD, Nginx, or None), and the PHP extensions that are enabled.

The buildpack overrides the default `options.json` file with any configuration it finds in the `.bp-config/options.json` file of your application.

Below is an explanation of the common options you might need to change.

| Variable                   | Explanation                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WEB_SERVER                 | Sets the web server to use. Must be one of <code>httpd</code> , <code>nginx</code> , or <code>none</code> . This value defaults to <code>httpd</code> .                                                                                                                                                                                                          |
| HTTPD_VERSION              | Sets the version of Apache HTTPD to use. Currently the build pack supports the latest stable version. This value will default to the latest release that is supported by the build pack.                                                                                                                                                                         |
| ADMIN_EMAIL                | The value used in HTTPD's configuration for <a href="#">ServerAdmin</a> .                                                                                                                                                                                                                                                                                        |
| NGINX_VERSION              | Sets the version of Nginx to use. By default, the buildpack uses the latest stable version.                                                                                                                                                                                                                                                                      |
| PHP_VERSION                | Sets the version of PHP to use.<br>Set to a minor instead of a patch version, such as <code>"{PHP_70_LATEST}"</code> . See <a href="#">options.json</a> .                                                                                                                                                                                                        |
| PHP_EXTENSIONS             | (DEPRECATED) A list of the <a href="#">extensions</a> to enable. <code>bz2</code> , <code>zlib</code> , <code>curl</code> , and <code>mcrypt</code> are enabled by default.                                                                                                                                                                                      |
| PHP_MODULES                | A list of the <a href="#">modules</a> to enable. No modules are explicitly enabled by default, but the buildpack automatically chooses either <code>fpm</code> or <code>cli</code> . You can explicitly enable any or all of the following: <code>fpm</code> , <code>cli</code> , <code>cgi</code> , and <code>pear</code> .                                     |
| ZEND_EXTENSIONS            | A list of the Zend extensions to enable. Nothing is enabled by default.                                                                                                                                                                                                                                                                                          |
| APP_START_CMD              | When the <code>WEB_SERVER</code> option is set to <code>none</code> , this command is used to start your app. If <code>WEB_SERVER</code> and <code>APP_START_CMD</code> are not set, then the buildpack searches, in order, for <code>app.php</code> , <code>main.php</code> , <code>run.php</code> , or <code>start.php</code> . This option accepts arguments. |
| WEBDIR                     | The root directory of the files served by the web server specified in <code>WEB_SERVER</code> . Defaults to <code>htdocs</code> . Other common settings are <code>public</code> , <code>static</code> , or <code>html</code> . The path is relative to the root of your application.                                                                             |
| LIBDIR                     | This path is added to PHP's <code>include_path</code> . Defaults to <code>lib</code> . The path is relative to the root of your application.                                                                                                                                                                                                                     |
| HTTP_PROXY                 | The buildpack downloads uncached dependencies using HTTP. If you are using a proxy for HTTP access, set its URL here.                                                                                                                                                                                                                                            |
| HTTPS_PROXY                | The buildpack downloads uncached dependencies using HTTPS. If you are using a proxy for HTTPS access, set its URL here.                                                                                                                                                                                                                                          |
| ADDITIONAL_PREPROCESS_CMDS | A list of additional commands that run prior to the application starting. For example, you might use this command to run migration scripts or static caching tools before the application launches.                                                                                                                                                              |

For details about supported versions, see the [release notes](#) for your buildpack version.

### HTTPD, Nginx, and PHP configuration

The buildpack automatically configures HTTPD, Nginx, and PHP for your application. This section explains how to modify the configuration.

The `.bp-config` directory in your application can contain configuration overrides for these components. Name the directories `httpd`, `nginx`, and `php`. We recommend that you use [php.ini.d](#) or [fpm.d](#).

 **NOTE:** If you override the `php.ini` or `php-fpm.conf` files, many other forms of configuration will not work.

For example: `.bp-config httpd nginx php`

Each directory can contain configuration files that the component understands.

For example, to change HTTPD logging configuration:

```
$ ls -l .bp-config/httpd/extra/
total 8
-rw-r--r-- 1 daniel staff 396 Jan 3 08:31 httpd-logging.conf
```

In this example, the `httpd-logging.conf` file overrides the one provided by the buildpack. We recommend that you copy the default from the buildpack and modify it.

You can find the default configuration files in the [PHP Buildpack](#) `/defaults/config` [directory](#).

You should be careful when modifying configurations, as doing so can cause your application to fail, or cause Cloud Foundry to fail to stage your application.

You can add your own configuration files. The components will not know about these, so you must ensure that they are included. For example, you can add an include directive to the [httpd configuration](#) to include your file:

```
ServerRoot "${HOME}/httpd"
Listen ${PORT}
ServerAdmin "${HTTPD_SERVER_ADMIN}"
ServerName "0.0.0.0"
DocumentRoot "${HOME}/#/{WEBDIR}"
Include conf/extra/httpd-modules.conf
Include conf/extra/httpd-directories.conf
Include conf/extra/httpd-mime.conf
Include conf/extra/httpd-logging.conf
Include conf/extra/httpd-mpm.conf
Include conf/extra/httpd-default.conf
Include conf/extra/httpd-remoteip.conf
Include conf/extra/httpd-php.conf
Include conf/extra/httpd-my-special-config.conf # This line includes your additional file.
```

## `.bp-config/php/php.ini.d/`

The buildpack adds any `.bp-config/php/php.ini.d/FILE-NAME.ini` files it finds in the application to the PHP configuration. You can use this to change any value acceptable to `php.ini`. See <http://php.net/manual/en/ini.list.php> for a list of directives.

For example, adding a file `.bp-config/php/php.ini.d/something.ini` to your app, with the following contents, overrides both the default charset and mimetype.

```
default_charset="UTF-8"
default_mimetype="text/xhtml"
```

## Precedence

In order of highest precedence, php configuration values come from the following sources:

- php scripts using `ini_set()` to manually override config files
- user.ini files for local values
- `.bp-config/php/php.ini.d` to override master value, but not local values from user.ini files

## `.bp-config/php/fpm.d/`

The buildpack adds any files it finds in the application under `.bp-config/php/fpm.d` that end with `.conf` (i.e. `my-config.conf`) to the PHP-FPM configuration. You can use this to change any value acceptable to `php-fpm.conf`. See <http://php.net/manual/en/install.fpm.configuration.php> for a list of directives.

PHP FPM config snippets are included by the buildpack into the global section of the configuration file. If you need to apply configuration settings for a PHP FPM worker, that needs to be indicated in your configuration file as well.

For example:

```
; This option is specific to the `www` pool
[www]
catch_workers_output = yes
```

## PHP Extensions

The buildpack adds any `.bp-config/php/php.ini.d/FILE-NAME.ini` files it finds in the application to the PHP configuration. You can use this to enable PHP or ZEND extensions. For example:

```
extension=redis.so
extension=gd.so
zend_extension=opcache.so
```

If an extension is already present and enabled in the compiled php, for example `intl`, you do not need to explicitly enable it to use that extension.

## PHP\_EXTENSIONS vs. ZEND\_EXTENSIONS

PHP has two kinds of extensions, *PHP extensions* and *Zend extensions*. These hook into the PHP executable in different ways. See <https://wiki.php.net/internals/extensions> for more information about the way extensions work internally in the engine.

Because they hook into the PHP executable in different ways, they are specified differently in ini files. Apps fail if a Zend extension is specified as a PHP extension, or a PHP extension is specified as a Zend extension.

If you see the following error, move the `example` extension from `extension` to `zend_extension`, then re-push your app:

```
php-fpm | [warn-ioncube] The example Loader is a Zend-Engine extension and not a module (pid 40)
php-fpm | [warn-ioncube] Please specify the Loader using 'zend_extension' in php.ini (pid 40)
php-fpm | NOTICE: PHP message: PHP Fatal error: Unable to start example Loader module in Unknown on line 0
```

If you see the following error, move the `example` extension from `zend_extension` to `extension`, then re-push your app.

```
NOTICE: PHP message: PHP Warning: example MUST be loaded as a Zend extension in Unknown on line 0
```

## PHP Modules

You can include the following modules by adding them to the `PHP_MODULES` list:

- `cli`, installs `php` and `phar`
- `fpm`, installs `PHP-FPM`
- `cgi`, installs `php-cgi`
- `pear`, installs Pear

By default, the buildpack installs the `cli` module when you push a standalone app, and installs the `fpm` module when you push a web app. You must specify `cgi` and `pear` if you want them installed.

## Buildpack Extensions

The buildpack comes with extensions for its default behavior. These are the [HTTPD](#), [Nginx](#), [PHP](#), and [NewRelic](#) extensions.

The buildpack is designed with an extension mechanism, allowing app developers to add behavior to the buildpack without modifying the buildpack code.

When you push an app, the buildpack runs any extensions found in the `.extensions` directory of your app.

The [Developer Documentation](#) explains how to write extensions.

## Composer

Page last updated:

Composer is activated when you supply a `composer.json` or `composer.lock` file. A `composer.lock` is not required, but is strongly recommended for consistent deployments.

You can require dependencies for packages and extensions. Extensions must be prefixed with the standard `ext-`. If you reference an extension that is available to the buildpack, it will automatically be installed. See the main [README](#) for a list of supported extensions.

The buildpack uses the version of PHP specified in your `composer.json` or `composer.lock` file. Composer settings override the version set in the `options.json` file.

The PHP buildpack supports a subset of the version formats supported by Composer. The buildpack supported formats are:

| Example | Expected Version                            |
|---------|---------------------------------------------|
| 5.3.*   | latest 5.4.x release (5.3 is not supported) |
| >=5.3   | latest 5.4.x release (5.3 is not supported) |
| 5.4.*   | latest 5.4.x release                        |
| >=5.4   | latest 5.4.x release                        |
| 5.5.*   | latest 5.5.x release                        |
| >=5.5   | latest 5.5.x release                        |
| 5.4.x   | specific 5.4.x release that is listed       |
| 5.5.x   | specific 5.5.x release that is listed       |

## Configuration

The buildpack runs with a set of default values for Composer. You can adjust these values by adding a `.bp-config/options.json` file to your application and setting any of the following values in it.

| Variable                 | Explanation                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| COMPOSER_VERSION         | The version of Composer to use. It defaults to the latest bundled with the buildpack.                                                                                                                                                                                                                                                                                                            |
| COMPOSER_INSTALL_OPTIONS | A list of options that should be passed to <code>composer install</code> . This defaults to <code>--no-interaction --no-dev --no-progress</code> . The <code>--no-progress</code> option must be used due to the way the buildpack calls Composer.                                                                                                                                               |
| COMPOSER_VENDOR_DIR      | Allows you to override the default value used by the buildpack. This is passed through to Composer and instructs it where to create the <code>vendor</code> directory. Defaults to <code>{BUILD_DIR}/{LIBDIR}/vendor</code> .                                                                                                                                                                    |
| COMPOSER_BIN_DIR         | Allows you to override the default value used by the buildpack. This is passed through to Composer and instructs it where to place executables from packages. Defaults to <code>{BUILD_DIR}/php/bin</code> .                                                                                                                                                                                     |
| COMPOSER_CACHE_DIR       | Allows you to override the default value used by the buildpack. This is passed through to Composer and instructs it where to place its cache files. Generally you should not change this value. The default is <code>{CACHE_DIR}/composer</code> which is a subdirectory of the cache folder passed in to the buildpack. Composer cache files will be restored on subsequent application pushes. |

By default, the PHP buildpack uses the `composer.json` and `composer.lock` files that reside inside the root directory, or in the directory specified as `WEBDIR` in your `options.json`. If you have composer files inside your app, but not in the default directories, use a `COMPOSER_PATH` environment variable for your app to specify this custom location, relative to the app root directory. Note that the `composer.json` and `composer.lock` files must be in the same directory.

## Github API Request Limits

Composer uses Github's API to retrieve zip files for installation into the application folder. If you do not vendor dependencies before pushing an app, Composer will fetch dependencies during staging using the Github API.

Github's API is request-limited. If you reach your daily allowance of API requests (typically 60), Github's API returns a `403` error and staging fails.

There are two ways to avoid the request limit:

1. Vendor dependencies before pushing your application.
2. Supply a Github OAuth API token.

## Vendor Dependencies

To vendor dependencies, you must run `composer install` before you push your application. You might also need to configure `COMPOSER_VENDOR_DIR` to “vendor”.

## Supply a Github Token

Composer can use [Github API OAuth tokens](#), which increase your request limit, typically to 5000 per day.

During staging, the buildpack looks for this token in the environment variable `COMPOSER_GITHUB_OAUTH_TOKEN`. If you supply a valid token, Composer uses it. This mechanism does not work if the token is invalid.

To supply the token, you can use either of the following methods:

1. `cf set-env YOUR_APP_NAME COMPOSER_GITHUB_OAUTH_TOKEN "OAUTH_TOKEN_VALUE"`
2. Add the token to the `env` block of your application manifest.

## Buildpack Staging Environment

Composer runs in the buildpack staging environment. Variables set with `cf set-env` or with [a manifest.yml ‘env’ block](#) are visible to Composer.

For example:

```
$ cf push a_symfony_app --no-start
$ cf set-env a_symfony_app SYMFONY_ENV "prod"
$ cf start a_symfony_app
```

In this example, `a_symfony_app` is supplied with an environment variable, `SYMFONY_ENV`, which is visible to Composer and any scripts started by Composer.

## Non-configurable Environment Variables

User-assigned environment variables are applied to staging and runtime. Unfortunately, `LD_LIBRARY_PATH` and `PHPRC` must be different for staging and runtime. The buildpack takes care of setting these variables, which means user values for these variables are ignored.

## Sessions

Page last updated:

### Usage

When your application has one instance, it's mostly safe to use the default session storage, which is the local file system. You would only see problems if your single instance crashes as the local file system would go away and you'd lose your sessions. For many applications, this will work just fine but please consider how this will impact your application.

If you have multiple application instances or you need a more robust solution for your application, then you'll want to use Redis or Memcached as a backing store for your session data. The build pack supports both and when one is bound to your application it will detect it and automatically configure PHP to use it for session storage.

By default, there's no configuration necessary. Create a Redis or Memcached service, make sure the service name contains `redis-sessions` or `memcached-sessions` and then bind the service to the application.

Example:

```
$ cf create-service redis some-plan app-redis-sessions
$ cf bind-service app app-redis-sessions
$ cf restage app
```

If you want to use a specific service instance or change the search key, you can do that by setting either `REDIS_SESSION_STORE_SERVICE_NAME` or `MEMCACHED_SESSION_STORE_SERVICE_NAME` in `.bp-config/options.json` to the new search key. The session configuration extension will then search the bound services by name for the new session key.

## Configuration Changes

When detected, the following changes will be made.

### Redis


- the `redis` PHP extension will be installed, which provides the session save handler
- `session.name` will be set to `PHPSESSIONID` which disables sticky sessions
- `session.save_handler` is configured to `redis`
- `session.save_path` is configured based on the bound credentials, for example `tcp://host:port?auth=pass`

### Memcached

- the `memcached` PHP extension will be installed, which provides the session save handler
- `session.name` will be set to `PHPSESSIONID` which disables sticky sessions
- `session.save_handler` is configured to `memcached`
- `session.save_path` is configured based on the bound credentials (i.e. `PERSISTENT=app_sessions host:port`)
- `memcached.sess_binary` is set to `On`
- `memcached.use_sasl` is set to `On`, which enables authentication
- `memcached.sess_sasl_username` and `memcached.sess_sasl_password` are set with the service credentials

## New Relic

Page last updated:

[New Relic](#)  collects analytics about application and client-side performance.


## Configuration

You can configure New Relic for the PHP buildpack in one of two ways:

- With a license key
- With a Cloud Foundry service

### With a License Key

Use this method if you already have a New Relic account,

1. In a web browser, navigate to the New Relic website to find your [license key](#) .
2. Set the value of the environment variable `NEWRELIC_LICENSE` to your New Relic license key, either through the [manifest.yml file](#) or by running the `cf set-env` command.

For more information, see <https://github.com/cloudfoundry/php-buildpack#supported-software> .

### With a Cloud Foundry Service

To configure New Relic for the PHP buildpack with a Cloud Foundry service, bind a New Relic service to the app. The buildpack automatically detects and configures New Relic.

Your `VCAP_SERVICES` environment variable must contain a service named `newrelic`, the `newrelic` service must contain a key named `credentials`, and the `credentials` key must contain named `licenseKey`.



**NOTE:** You cannot configure New Relic for the PHP buildpack with user-provided services.



## Python Buildpack

Page last updated:

### Push an App

Cloud Foundry automatically uses this buildpack if it detects a `requirements.txt` or `setup.py` file in the root directory of your project.

If your Cloud Foundry deployment does not have the Python Buildpack installed, or the installed version is out of date, you can use the latest version by specifying it with the `-b` option when you push your app. For example:

```
$ cf push my_app -b https://github.com/cloudfoundry/buildpack-python.git
```

### Supported Versions

You can find the list of supported Python versions in the [Python buildpack release notes](#).

### Specify a Python Version

You can specify a version of the Python runtime by including it within a `runtime.txt` file. For example:

```
$ cat runtime.txt
python-3.5.2
```

The buildpack only supports the stable Python versions, which are listed in the `manifest.yml` and [Python buildpack release notes](#).

To request the latest Python version in a patch line, replace the patch version with `x`: `3.6.x`. To request the latest version in a minor line, replace the minor version: `3.x`.

If you try to use a binary that is not currently supported, staging your app fails and you see the following error message:

```
Could not get translated url, exited with: DEPENDENCY_MISSING_IN_MANIFEST: ...
!
! exit
!
Staging failed: Buildpack compilation step failed
```

### Specify a Start Command

The Python buildpack does not generate a [default start command](#) for your applications.

To stage with the Python buildpack and start an application, do one of the following:

- Supply a Procfile. For more information about Procfiles, see the [Configuring a Production Server](#) topic. The following example Procfile specifies `gunicorn` as the start command for a web app running on Gunicorn:

```
web: gunicorn SERVER-NAME:APP-NAME
```

- Specify a start command with `-c`. The following example specifies `waitress-serve` as the start command for a web app running on Waitress:

```
$ cf push python-app -c "waitress-serve --port=$PORT DJANGO-WEB-APP.wsgi:MY-APP"
```

- Specify a start command in the application manifest by setting the `command` attribute. For more information, see the [Deploying with Application Manifests](#) topic.

## Vendor App Dependencies


If you are deploying in an environment that is disconnected from the Internet, your application [must vendor its dependencies](#).

For the Python buildpack, use `pip`:

```
$ cd YOUR-APP-DIR
$ mkdir -p vendor

vendors all the pip *.tar.gz into vendor/
$ pip install --download vendor -r requirements.txt --no-binary :all:
```

`cf push` uploads your vendored dependencies. The buildpack installs them directly from the `vendor/` directory.

 **Note:** To ensure proper installation of dependencies, we recommend non-binary vendored dependencies. The above `pip install` command achieves this.

## Private Dependency Repository

To deploy apps in an environment that needs to use a private dependency repository, you have the following options:

- [PIP](#)
- [Conda](#)

### PIP

To install dependencies using PIP, add the URL of the repository to the `requirements.txt` file in the following format:

```
--index-url=https://example.com/api/pypi/ext_pypi/simple
fixtures==2.0.0
```

If the private repository uses a custom SSL certificate that is installed on the platform, you may see an error similar to the following:

```
Could not fetch URL https://example.com/api/pypi/ext_pypi/simple/fixtures/:
There was a problem confirming the ssl certificate:
[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:777) - skipping
```

This error occurs because `pip` does not use system certificates by default. To resolve this issue, set the `PIP_CERT` environment variable in the `manifest.yml` file to point to the system certificate store.

For example:

```

env:
 PIP_CERT: /etc/ssl/certs/ca-certificates.crt
```

### Conda

To install dependencies using Conda, add a `channels` block to the `environment.yml` file.

In the `channels` block, list custom channels and add `nodefaults`. Specifying `nodefaults` tells Conda to only use the channels in the channels block.

For example:

```
channels:
 - https://conda.example.com/repo
 - nodefaults
```

If the private repository uses a custom SSL certificate that is installed on the platform, you may see an error similar to the following:

Error: Connection error: [SSL: CERTIFICATE\_VERIFY\_FAILED] certificate verify failed (\_ssl.c:581):

This error occurs because `conda` does not use system certificates by default. To resolve this issue, set the `CONDA_SSL_VERIFY` environment variable in the `manifest.yml` file to point to the system certificate store.

For example:

```

env:
 CONDA_SSL_VERIFY: /etc/ssl/certs/ca-certificates.crt
```

## Parse Environment Variables

The `cfenv` package provides access to Cloud Foundry application environment settings by parsing all the relevant environment variables. The settings are returned as a class instance. See <https://github.com/jmcarp/py-cfenv> for more information.

## Miniconda Support (starting in buildpack version [1.5.6](#))

To use miniconda instead of pip for installing dependencies, place an `environment.yml` file in the root directory.

For examples, see our sample apps:

- [Using Python 2 with miniconda](#)
- [Using Python 3 with miniconda](#)

## Pipenv Support (starting in buildpack version [1.5.19](#))

To use [Pipenv](#) instead of pip (directly) for installing dependencies, place a `Pipfile` in the root directory. Easiest to let Pipenv generate this for you.

## NLTK Support

To use NLTK corpora in your app, you can include an `nltk.txt` file in the root of your application. Each line in the file specifies one dataset to download. The full list of data sets available this way can be found [on the NLTK website](#). The `id` listed for the corpora on that page is the string you should include in your app's `nltk.txt`.

Example `nltk.txt`: `brown wordnet`

Having an `nltk.txt` file only causes the buildpack to download the corpora. You still must specify NLTK as a dependency of your app if you want to use it to process the corpora files.

## Proxy Support

If you need to use a proxy to download dependencies during staging, you can set the `http_proxy` and `https_proxy` environment variables. For more information, see [Using a Proxy](#).

## BOSH Configured Custom Trusted Certificate Support

Versions of Python 2.7.9 and later use certificates stored in `/etc/ssl/certs`. Your platform operator can configure the platform to [add the custom certificates into the application container](#).

## Help and Support


Join the #buildpacks channel in our [Slack community](#) if you need any further assistance.

For more information about using and extending the Python buildpack in Cloud Foundry, see the [python-buildpack GitHub repository](#).

You can find current information about this buildpack on the [Python buildpack release page](#) in GitHub.

## R Buildpack

This topic describes how to push your R app to Cloud Foundry and how to configure your R app to use the R buildpack.

 **Note:** This buildpack is not distributed as part of Pivotal Application Service (PAS) v2.4. However, it is supported for use with PAS. You can download an offline version of this buildpack from [Pivotal Network](#).

## Push an App

Cloud Foundry automatically uses the R buildpack if it detects a `r.yml` file in the root directory of your project.

If your Cloud Foundry deployment does not have the R buildpack installed, or the installed version is out of date, you can use the latest version by specifying it with the `-b` option when you push your app. For example:

```
$ cf push my_app -b https://github.com/cloudfoundry/r-buildpack.git
```

## Supported Versions

You can find the list of supported R versions in the [R buildpack release notes](#).

## Start Command

The R buildpack does not generate a default start command for your applications. Instead, you must specify a start command for your app.

To stage an app with the R buildpack and start the app, do one of the following:

- **Option 1:** Supply a Procfile. For more information about Procfiles, see [Production Server Configuration](#). The following example Procfile specifies `R -f simple.r` as the start command for a web app with the entrypoint `simple.r`:

```
web: R -f simple.r
```

- **Option 2:** Specify a start command with `-c`:

```
$ cf push r-app -c "R -f simple.r"
```

- **Option 3:** Specify a start command in the application manifest by setting the `command` attribute. For more information, see the [Deploying with Application Manifests](#) topic.

For more information about starting apps, see [Starting, Restarting, and Restaging Applications](#).

## Specifying App Dependencies

As of v0.0.5, the following packages are provided by the buildpack:

- Rserve
- forecast
- shiny

To specify additional packages needed by your app, provide the CRAN mirror and names of the packages inside your `r.yml` file. You can also specify the number of threads to use for parallel installation. For example:

```

packages:
- cran_mirror: https://cran.r-project.org
 num_threads: 2
packages:
- name: stringr
- name: jsonlite
```

## Vendoring App Dependencies

If you are deploying in an environment that is disconnected from the Internet, you must *vendor* your app's dependencies, which means you must make these packages available for offline use. You can vendor dependencies by using a package manager.

To set up your own custom, local CRAN-like repository to vendor your packages, create the `src/contrib` directories and populate them with your package source tarballs. For more information, see [How to Set Up a Custom CRAN-like Repository](#) published on the *Packrat Documentation* site.

Add the `src/contrib` directories containing your package tarballs to a `vendor_r` directory at the root of your app. This directory is named `vendor_r` so as not to conflict with vendor directories of other languages, such as python.

Then, inside your `r.yml`, provide the names of your vendored packages in the `packages` list:

```

packages:
- packages:
 - name: stringr
 - name: jsonlite
```

`cf push` uploads your vendored dependencies. The buildpack installs them directly from the `vendor_r/` directory.

Example app directory tree:

```
├── r.yml
├── simple-app.r
└── vendor_r
 ├── src
 │ └── contrib
 │ ├── PACKAGES
 │ ├── PACKAGES.gz
 │ ├── jsonlite_1.5.tar.gz
 │ └── stringr_1.3.1.tar.gz
```

For more information about using buildpacks in disconnected environments, see [Disconnected environments](#).

## Proxy Support

If you need to use a proxy to download dependencies during staging, you can set the `http_proxy` and `https_proxy` environment variables. For more information, see the [Proxy Usage Documentation](#).

## BOSH Configured Custom Trusted Certificate Support

R uses certificates stored in `/etc/ssl/certs`. Your platform operator can configure the platform to add the custom certificates into the application container. For more information, see [Configuring Trusted System Certificates for Applications](#).

## Help and Support

Join the `#buildpacks` channel in our [Slack community](#) if you need any further assistance.

For more information about using and extending the R buildpack in Cloud Foundry, see the [R-buildpack GitHub repository](#).

You can also find current information about this buildpack on the [R buildpack release page](#) in GitHub.



## Ruby Buildpack

Page last updated:

### Push Apps

Cloud Foundry uses the Ruby buildpack if your app has a `Gemfile` and `Gemfile.lock` in the root directory. The Ruby buildpack uses Bundler to install your dependencies.

If your Cloud Foundry deployment does not have the Ruby buildpack installed or the installed version is out of date, push your app with the `-b` option to specify the buildpack:

```
$ cf push MY-APP -b https://github.com/cloudfoundry/ruby-buildpack.git
```

For more detailed information about deploying Ruby applications see the following topics:

- [Tips for Ruby Developers](#)
- [Getting Started Deploying Apps](#)
- [Configuring Rake Tasks for Deployed Apps](#)
- [Environment Variables Defined by the Ruby Buildpack](#)
- [Configuring Service Connections for Ruby](#)
- [Support for Windows Gemfiles](#)

You can find the source for the Ruby buildpack in the [Ruby buildpack repository](#) on GitHub.

### Supported Versions

You can find supported Ruby versions in the [release notes for the Ruby buildpack](#) on GitHub.

### Specify a Ruby Version

Specify specific versions of the Ruby runtime in the `Gemfile` for your app as described in the sections below.


#### MRI

For MRI, specify the version of Ruby in your `Gemfile` as follows:

```
ruby '~> 2.2.3'
```

With this example declaration in the `Gemfile`, if Ruby versions `2.2.4`, `2.2.5`, and `2.3.0` are present in the Ruby buildpack, the app uses Ruby version `2.2.5`.

For more information about the `ruby` directive for Bundler Gemfiles, see the [Bundler documentation](#).

 **Note:** If you use v1.6.18 or earlier, you must specify an exact version, such as `ruby '2.2.3'`. In [Ruby Buildpack v1.6.18](#) and earlier, Rubygems do not support version operators for the `ruby` directive.

#### JRuby

For JRuby, specify the version of Ruby in your `Gemfile` based on the version of JRuby your app uses.

JRuby version `1.7.x` supports either `1.9` mode or `2.0` mode.




- For `1.9` mode, use the following: `ruby ruby '1.9.3', :engine => 'jruby', :engine_version => '1.7.25'`
- For `2.0` mode, use the following: `ruby ruby '2.0.0', :engine => 'jruby', :engine_version => '1.7.25'`

For Jruby version `>= 9.0`, use the following: `ruby ruby '2.2.3', :engine => 'jruby', :engine_version => '9.0.5.0'`

The Ruby buildpack only supports the stable Ruby versions listed in the `manifest.yml` and [release notes for the Ruby buildpack](#) on GitHub.

If you try to use a binary that is not supported, staging your app fails with the following error message:

```
Could not get translated url, exited with: DEPENDENCY_MISSING_IN_MANIFEST: ...
!
! exit
!
Staging failed: Buildpack compilation step failed
```

 **Note:** The Ruby buildpack does not support the pessimistic version operator `~>` on the Gemfile `ruby` directive for JRuby.

## Vendor App Dependencies

As stated in the [Disconnected Environments documentation](#), your application must ‘vendor’ its dependencies.

For the Ruby buildpack, use the `bundle package --all` command in Bundler to vendor the dependencies.

Example:

```
$ cd my-app-directory
bundle package --all
```

The `cf push` command uploads your vendored dependencies. The Ruby buildpack compiles any dependencies requiring compilation while staging your app.

## Buildpack Logging and Application Logging

The Ruby buildpack only runs during the staging process, and only logs what is important to staging, such as what is being downloaded, what the configuration is, and work that the buildpack does on your application.

The buildpack stops logging when the staging process finishes. The Loggregator handles application logging.

Your application must write to STDOUT or STDERR for its logs to be included in the Loggregator stream. For more information, see the [Application Logging in Cloud Foundry](#) topic.

If you are deploying a Rails application, the buildpack may or may not automatically install the necessary plugin or gem for logging, depending on the Rails version of the application:

- Rails 2.x: The buildpack automatically installs the `rails_log_stdout` plugin into the application. For more information about the `rails_log_stdout` plugin, refer to the [Github README](#).
- Rails 3.x: The buildpack automatically installs the `rails_12factor` gem if it is not present and issues a warning message. You must add the `rails_12factor` gem to your `Gemfile` to quiet the warning message. For more information about the `rails_12factor` gem, refer to the [Github README](#).
- Rails 4.x: The buildpack only issues a warning message that the `rails_12factor` gem is not present, but does not install the gem. You must add the `rails_12factor` gem to your `Gemfile` to quiet the warning message. For more information about the `rails_12factor` gem, refer to the [Github README](#).

For more information about the `rails_12factor` gem, refer to the [Github README](#).

## Proxy Support

If you need to use a proxy to download dependencies during staging, you can set the `http_proxy` and/or `https_proxy` environment variables. For more information, see [Using a Proxy](#).

## BOSH Configured Custom Trusted Certificate Support

Ruby uses certificates stored in `/etc/ssl/certs`. Your platform operator can configure the platform to add the custom certificates into the app container.

## Help and Support

Join the #buildpacks channel in our [Slack community](#) if you need any further assistance.

For more information about using and extending the Ruby buildpack in Cloud Foundry, see the [Ruby buildpack repository](#) on GitHub.

You can find current information about the Ruby buildpack in the [release notes for the Ruby buildpack](#) on GitHub.

## Tips for Ruby Developers

Page last updated:

This page has information specific to deploying Rack, Rails, or Sinatra apps.

## App Bundling

You must run [Bundler](#) to create a `Gemfile` and a `Gemfile.lock`. These files must be in your app before you push to Cloud Foundry.

## Rack Config File

For Rack and Sinatra, you must have a `config.ru` file. For example:

```
require './hello_world'
run HelloWorld.new
```

## Asset Precompilation

Cloud Foundry supports the Rails asset pipeline. If you do not precompile assets before deploying your app, Cloud Foundry precompiles them when staging the app. Precompiling before deploying reduces the time it takes to stage an app.

Use the following command to precompile assets before deployment:

```
$ rake assets:precompile
```

Note that the Rake precompile task reinitializes the Rails app. This could pose a problem if initialization requires service connections or environment checks that are unavailable during staging. To prevent reinitialization during precompilation, add the following line to `application.rb`:

```
config.assets.initialize_on_precompile = false
```

If the `assets:precompile` task fails, Cloud Foundry uses live compilation mode, the alternative to asset precompilation. In this mode, assets are compiled when they are loaded for the first time. You can force live compilation by adding the following line to `application.rb`.

```
Rails.application.config.assets.compile = true
```

## Running Rake Tasks

Cloud Foundry does not provide a mechanism for running a Rake task on a deployed app. If you need to run a Rake task that must be performed in the Cloud Foundry environment, rather than locally before deploying or redeploying, you can configure the command that Cloud Foundry uses to start the app to invoke the Rake task.

An app start command is configured in the app manifest file, `manifest.yml`, using the `command` attribute.

For more information about app manifests and supported attributes, see the [Deploying with Application Manifests](#) topic.

## Example: Invoking a Rake database migration task at app startup

The following is an example of migrating a database schema using a Rake task. For more information about migrating database schemas, see [Services Overview](#).

1. If a Rakefile does not exist, create one and add it to your app directory.

2. In your Rakefile, add a Rake task to limit an idempotent command to the first instance of a deployed app:

```
namespace :cf do
 desc "Only run on the first application instance"
 task :on_first_instance do
 instance_index = JSON.parse(ENV["VCAP_APPLICATION"])[["instance_index"]] rescue nil
 exit(0) unless instance_index == 0
 end
end
```

3. Add the task to the `manifest.yml` file, referencing the idempotent command `rake db:migrate` with the `command` attribute.

```


applications:
- name: my-rails-app
 command: bundle exec rake cf:on_first_instance db:migrate && bundle exec rails s -p $PORT -e $RAILS_ENV
```

4. Update the app using `cf push`.

## Rails 3 Worker Tasks





This section shows you how to create and deploy an example Rails app that uses a worker library to defer a task that a separate app executes.

The guide also describes how to scale the resources available to the worker app.

 **Note:** Most worker tasks do not serve external requests. Use the `--no-route` flag with the `cf push` command, or `no-route: true` in the app manifest, to suppress route creation and remove existing routes.

## Choose a Worker Task Library

You must choose a worker task library. The table below summarizes the three main libraries available for Ruby / Rails:

| Library                                                                                                         | Description                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Delayed::Job</a>  | A direct extraction from <a href="#">Shopify</a>  where the job table is responsible for a multitude of core tasks.                                                       |
| <a href="#">Resque</a>       | A Redis-backed library for creating background jobs, placing those jobs on multiple queues, and processing them later.                                                                                                                                       |
| <a href="#">Sidekiq</a>      | Uses threads to handle many messages at the same time in the same process. It does not require Rails, but integrates tightly with Rails 3 to simplify background message processing. This library is Redis-backed and semi-compatible with Resque messaging. |

For other alternatives, see [https://www.ruby-toolbox.com/categories/Background\\_Jobs](https://www.ruby-toolbox.com/categories/Background_Jobs) .

## Create an Example App

For the purposes of the example app, we use Sidekiq.

First, create a Rails app with an arbitrary model named “Things”:

```
$ rails create rails-sidekiq
$ cd rails-sidekiq
$ rails g model Thing title:string description:string
```

Add `sidekiq` and `uuidtools` to the Gemfile:

```
source 'https://rubygems.org'

gem 'rails', '3.2.9'
gem 'mysql2'

group :assets do
 gem 'sass-rails', '~> 3.2.3'
 gem 'coffee-rails', '~> 3.2.1'
 gem 'uglifier', '>= 1.0.3'
end

gem 'jquery-rails'
gem 'sidekiq'
gem 'uuidtools'
```

Install the bundle.

```
$ bundle install
```

In `app/workers`, create a worker for Sidekiq to carry out its tasks:

```
$ touch app/workers/thing_worker.rb
```

```
class ThingWorker

 include Sidekiq::Worker

 def perform(count)

 count.times do

 thing_uuid = UUIDTools::UUID.random_create.to_s
 Thing.create :title => "New Thing ({thing_uuid})", :description =>
 "Description for thing #{thing_uuid}"
 end
 end

end
```

This worker create `n` number of things, where `n` is the value passed to the worker.

Create a controller for “Things”:

```
$ rails g controller Thing
```

```
class ThingController < ApplicationController

 def new
 ThingWorker.perform_async(2)
 redirect_to '/thing'
 end

 def index
 @things = Thing.all
 end

end
```

Add a view to inspect our collection of “Things”:

```
$ mkdir app/views/things
$ touch app/views/things/index.html.erb
```

```
nil
```

## Deploy the App

This app needs to be deployed twice for it to work, once as a Rails web app and once as a standalone Ruby app. One way to do this is to keep separate

Cloud Foundry manifests for each app type:

Web Manifest: Save this as `web-manifest.yml` :

```

applications:
- name: sidekiq
 memory: 256M
 instances: 1
 host: sidekiq
 domain: ${target-base}
 path: .
 services:
 - sidekiq-mysql:
 - sidekiq-redis:
```

Worker Manifest: Save this as `worker-manifest.yml` :

```

applications:
- name: sidekiq-worker
 memory: 256M
 instances: 1
 path: .
 command: bundle exec sidekiq
 no-route: true
 services:
 - sidekiq-redis:
 - sidekiq-mysql:
```

Since the url “sidekiq.cloudfoundry.com” is probably already taken, change it in `web-manifest.yml` first, then push the app with both manifest files:

```
$ cf push -f web-manifest.yml
$ cf push -f worker-manifest.yml
```

If the cf CLI asks for a URL for the worker app, select **none**.

## Test the App

Test the app by visiting the new action on the “Thing” controller at the assigned url. In this example, the URL would be `http://sidekiq.cloudfoundry.com/thing/new`

This creates a new Sidekiq job which is queued in Redis, then picked up by the worker app. The browser is then redirected to `/thing` which shows the collection of “Things”.

## Scale Workers

Use the `cf scale` command to change the number of Sidekiq workers.

Example:


```
$ cf scale sidekiq-worker -i 2
```

## Use rails\_serve\_static\_assets on Rails 4

By default Rails 4 returns a 404 if an asset is not handled via an external proxy such as Nginx. The `rails_serve_static_assets` [gem](#) enables your Rails server to deliver static assets directly, instead of returning a 404. You can use this capability to populate an edge cache CDN or serve files directly from your web app. The gem enables this behavior by setting the `config.serve_static_assets` option to `true`, so you do not need to configure it manually.

## Add Custom Libraries

If your app requires external shared libraries that are not provided by the rootfs or the buildpack, you must place the libraries in an `ld_library_path` directory at the app root.

 **Note:** You must keep these libraries up-to-date. They do not update automatically.

The Ruby buildpack automatically adds the directory `<app-root>/ld_library_path` to `LD_LIBRARY_PATH` so that your app can access these libraries at runtime.

## Environment Variables

You can access environments variable programmatically. For example, you can obtain `VCAP_SERVICES` as follows:

```
ENV['VCAP_SERVICES']
```

Environment variables available to you include both those defined by the system and those defined by the Ruby buildpack, as described below. For more information about system environment variables, see the [Application-Specific System Variables](#) section of the *Cloud Foundry Environment Variables* topic.

### BUNDLE\_BIN\_PATH

Location where Bundler installs binaries.

Example: `BUNDLE_BIN_PATH:/home/vcap/app/vendor/bundle/ruby/1.9.1/gems/bundler-1.3.2/bin/bundle`

### BUNDLE\_GEMFILE

Path to app Gemfile.

Example: `BUNDLE_GEMFILE:/home/vcap/app/Gemfile`

### BUNDLE\_WITHOUT

The `BUNDLE_WITHOUT` environment variable instructs Cloud Foundry to skip gem installation in excluded groups.

Use this with Rails applications, where “assets” and “development” gem groups typically contain gems that are not needed when the app runs in production.

Example: `BUNDLE_WITHOUT=assets`

### DATABASE\_URL

Cloud Foundry examines the `database_uri` for bound services to see if they match known database types. If known relational database services are bound to the app, the `DATABASE_URL` environment variable is set using the first match in the list.

If your app depends on `DATABASE_URL` to be set to the connection string for your service and Cloud Foundry does not set it, use the `cf set-env` command to can set this variable manually.

Example:

```
$ cf set-env my-app-name DATABASE_URL mysql://example-database-connection-string
```

### GEM\_HOME

Location where gems are installed.

Example: `GEM_HOME=/home/vcap/app/vendor/bundle/ruby/1.9.1`

## GEM\_PATH

Location where gems can be found.

Example: `GEM_PATH=/home/vcap/app/vendor/bundle/ruby/1.9.1:`

## RACK\_ENV

This variable specifies the Rack deployment environment. Valid value are `development`, `deployment`, and `none`. This governs which middleware is loaded to run the app.

Example: `RACK_ENV=development`

## RAILS\_ENV

This variable specifies the Rails deployment environment. Valid value are `development`, `test`, and `production`. This controls which of the environment-specific configuration files governs how the app is executed.

Example: `RAILS_ENV=production`

## RUBYOPT

This Ruby environment variable defines command-line options passed to Ruby interpreter.

Example: `RUBYOPT: -I/home/vcap/app/vendor/bundle/ruby/1.9.1/gems/bundler-1.3.2/lib -rbundler/setup`



## Getting Started Deploying Ruby Apps

Page last updated:

This topic provides links to additional information about getting started deploying apps using the Ruby buildpack. See the following topics for deployment guides specific to your app language and framework:

- [Ruby](#)
- [Ruby on Rails](#)


## Getting Started Deploying Ruby Apps

Page last updated:

This guide is intended to walk you through deploying a Ruby app to Pivotal Application Service. If you experience a problem following the steps below, check the [Known Issues](#) topic, or refer to the [Troubleshooting Application Deployment and Health](#) topic.

### Sample App Step

If you want to go through this tutorial using the sample app, run `git clone https://github.com/cloudfoundry-samples/pong_matcher_ruby.git` to clone the `pong_matcher_ruby` app from GitHub, and follow the instructions in the Sample App Step sections.

 **Note:** Ensure that your Ruby app runs locally before continuing with this procedure.

## Deploy a Ruby Application

This section describes how to deploy a Ruby application to PAS, and uses output from a sample app to show specific steps of the deployment process.

### Prerequisites

- A Ruby 2.x application that runs locally on your workstation
- [Bundler](#) configured on your workstation
- Basic to intermediate Ruby knowledge
- The [Cloud Foundry Command Line Interface \(cf CLI\)](#) installed on your workstation

### Step 1: Create and Bind a Service Instance for a Ruby Application

This section describes using the cf CLI to configure a Redis Cloud managed service instance for an app. You can use either the CLI or [Apps Manager](#) to perform this task.

PAS supports two types of service instances:

- Managed services integrate with PAS through service brokers that offer services and plans and manage the service calls between PAS and a service provider.
- User-provided service instances enable you to connect your application to pre-provisioned external service instances.

For more information about creating and using service instances, refer to the [Services Overview](#) topic.

### Create a Service Instance

Run `cf marketplace` to view managed and user-provided services and plans that are available to you.

The example shows three of the available managed database-as-a-service providers and the plans that they offer: `cleardb` MySQL and `postgresql-10-odb` PostgreSQL as a Service.

```
$ cf marketplace
Getting services from marketplace in org Cloud-Apps / space development as clouduser@example.com...
OK

service plans description
...
cleardb spark, boost, amp, shock Highly available MySQL for your Apps
...
postgresql-10-odb standalone, standalone-replica, general PostgreSQL as a Service
...
```

Run `cf create-service SERVICE_PLAN SERVICE_INSTANCE` to create a service instance for your app. Choose a SERVICE and PLAN from the list, and provide a unique name for the SERVICE\_INSTANCE.

## Sample App Step

Run `cf create-service rediscloud 30mb redis`. This creates a service instance named `redis` that uses the `rediscloud` service and the `30mb` plan, as the example below shows.

```
$ cf create-service rediscloud 30mb redis
Creating service redis in org Cloud-Apps / space development as clouduser@example.com...
OK
```

## Bind a Service Instance

When you bind an app to a service instance, PAS writes information about the service instance to the VCAP\_SERVICES app environment variable. The app can use this information to integrate with the service instance.

Most services support bindable service instances. Refer to your service provider's documentation to confirm if they support this functionality.

You can bind a service to an application with the command `cf bind-service APPLICATION SERVICE_INSTANCE`.

Alternately, you can configure the deployment manifest file by adding a `services` block to the `applications` block and specifying the service instance. For more information and an example on service binding using a manifest, see the Sample App Step.

You can also bind a service using the [Apps Manager](#).

## Sample App Step

You can skip this step. The manifest for the sample app contains a `services` sub-block in the `applications` block, as the example below shows. This binds the `redis` service instance that you created in the previous step.

```
services:
- redis
```

## Step 2: Configure Deployment Options

### Configure the Deployment Manifest

You can specify app deployment options in a manifest that the `cf push` command uses. For more information about application manifests and supported attributes, refer to the [Deploying with Application Manifests](#) topic.

### Configure a Production Server

PAS uses the default standard Ruby web server library, WEBrick, for Ruby and RoR apps. However, PAS can support a more robust production web server, such as Phusion Passenger, Puma, Thin, or Unicorn. If your app requires a more robust web server, refer to the [Configuring a Production Server](#) topic for help configuring a server other than WEBrick.

## Sample App Step

You can skip this step. The `manifest.yml` file for `pong_matcher_ruby` does not require any additional configuration to deploy the app.


## Step 3: Log in and Target the API Endpoint

Run `cf login -a API_ENDPOINT`, enter your login credentials, and select a space and org. The API endpoint is [the URL of the Cloud Controller in your PAS instance](#).

### Sample App Step

You must do this step to run the sample app.

## Step 4: Deploy an App

 **Note:** You must use the cf CLI to deploy apps.

From the root directory of your application, run `cf push APP_NAME` to deploy your application.

`cf push APP_NAME` creates a URL route to your application in the form HOST.DOMAIN, where HOST is your APP\_NAME and DOMAIN is specified by your administrator. Your DOMAIN is `shared-domain.example.com`. For example: `cf push my-app` creates the URL `my-app.shared-domain.example.com`.

The URL for your app must be unique from other apps that PAS hosts or the push will fail. Use the following options to help create a unique URL:

- `-n` to assign a different HOST name for the app.
- `--random-route` to create a URL that includes the app name and random words.
- `cf help push` to view other options for this command.

If you want to view log activity while the app deploys, launch a new terminal window and run `cf logs APP_NAME`.


Once your app deploys, browse to your app URL. Search for the `urls` field in the `App started` block in the output of the `cf push` command. Use the URL to access your app online.

### Sample App Step

Run `cf push pong_matcher_ruby -n HOST_NAME`.

Example: `cf push pong_matcher_ruby -n pongmatch-ex12`

The example below shows the terminal output of deploying the `pong_matcher_ruby` app. `cf push` uses the instructions in the manifest file to create the app, create and bind the route, and upload the app. It then binds the app to the `redis` service and follows the instructions in the manifest to start one instance of the app with 256M. After the app starts, the output displays the health and status of the app.

 **Note:** The `pong_matcher_ruby` app does not include a web interface. To interact with the `pong_matcher_ruby` app, see the interaction instructions on GitHub: [https://github.com/cloudfoundry-samples/pong\\_matcher\\_ruby](https://github.com/cloudfoundry-samples/pong_matcher_ruby).

```
$ cf push pong_matcher_ruby -n pongmatch-ex12
Using manifest file /Users/clouduser/workspace/pong_matcher_ruby/manifest.yml

Creating app pong_matcher_ruby in org Cloud-Apps / space development as clouduser@example.com...
OK

Creating route pongmatch-ex12.shared-domain.example.com
Binding pongmatch-ex12.shared-domain.example.com to pong_matcher_ruby...
OK

Uploading pong_matcher_ruby...
Uploading app files from: /Users/clouduser/workspace/pong_matcher_ruby
Uploading 8.8K, 12 files
OK
Binding service redis to app pong_matcher_ruby in org Cloud-Apps / space development as clouduser@example.com...
OK

Starting app pong_matcher_ruby in org Cloud-Apps / space development as clouduser@example.com...
OK
...

0 of 1 instances running, 1 starting
1 of 1 instances running

App started

Showing health and status for app pong_matcher_ruby in org Cloud-Apps / space development as clouduser@example.com...
OK

requested state: started
instances: 1/1
usage: 256M x 1 instances
urls: pongmatch-ex12.cfapps.io

state since cpu memory disk
#0 running 2014-12-09 10:04:40 AM 0.0% 35.2M of 256M 45.8M of 1G
```

## Step 5: Test a Deployed App

You've deployed an app to PAS!

Use the cf CLI or [Apps Manager](#) to review information and administer your app and your PAS account. For example, you could edit the `manifest.yml` to increase the number of app instances from 1 to 3, and redeploy the app with a new app name and host name.

See the [Manage Your Application with the cf CLI](#) section for more information. See also [Using the Apps Manager](#).

## Manage Your Application with the cf CLI

Run `cf help` to view a complete list of commands, grouped by task categories, and run `cf help COMMAND` for detailed information about a specific command. For more information about using the cf CLI, refer to the Cloud Foundry Command Line Interface (cf CLI) topics, especially the [Getting Started with cf CLI](#) topic.

**Note:** You cannot perform certain tasks in the CLI or [Apps Manager](#) because these are commands that only a PAS administrator can run. If you are not a PAS administrator, the following message displays for these types of commands:

error code: 10003, message: You are not authorized to perform the requested action

For more information about specific Admin commands you can perform with the Apps Manager, depending on your user role, refer to the [Getting Started with the Apps Manager](#) topic.

## Troubleshooting

If your application fails to start, verify that the application starts in your local environment. Refer to the [Troubleshooting Application Deployment and Health](#) topic to learn more about troubleshooting.

## App Deploy Fails

Even when deploying an app fails, the app might exist on PAS. Run `cf apps` to review the apps in the currently targeted org and space. You might be able to correct the issue using the CLI or [Apps Manager](#), or you might have to delete the app and redeploy.

Common reasons deploying an app fails include:

- You did not successfully create and bind a needed service instance to the app, such as a PostgreSQL service instance. Refer to Step 2: Create and Bind a Service Instance for a Ruby Application.
- You did not successfully create a unique URL for the app. Refer to the troubleshooting tip **App Requires Unique URL**.

## App Requires Unique URL

PAS requires that each app that you deploy has a unique URL. Otherwise, the new app URL collides with an existing app URL and PAS cannot successfully deploy the app. You can resolve this issue by running `cf push` with either of the following flags to create a unique URL:

- `-n` to assign a different HOST name for the app.
- `--random-route` to create a URL that includes the app name and random words. Using this option might create a long URL, depending on the number of words that the app name includes.

## Getting Started Deploying Ruby on Rails Apps

Page last updated:

This guide walks you through deploying a Ruby on Rails app to Pivotal Cloud Foundry (PCF).

### Prerequisites

In order to deploy a sample Ruby on Rails app, you must have the following:

- A Cloud Foundry deployment or a Pivotal Web Services account
- The [Cloud Foundry Command Line Interface](#)
- A Cloud Foundry username and password with **Space Developer** [permissions](#). See your [Org Manager](#) if you require permissions.

### Step 1: Clone the App

Run the following terminal command to create a local copy of the cf-sample-app-rails.

```
$ git clone https://github.com/cloudfoundry-samples/cf-sample-app-rails.git
```

The newly created directory contains a `manifest.yml` file, which assists CF with deploying the app. See [Deploying with Application Manifests](#) for more information.

### Step 2: Log in and Target the API Endpoint

1. Run the following terminal command to log in and target the API endpoint of your deployment. For more information, see the [Identifying the API Endpoint for your PAS Instance](#) [topic](#).

```
$ cf login -a YOUR-API-ENDPOINT
```

2. Use your credentials to log in, and to select a [Space and Org](#).

### Step 3: Create a Service Instance

Run the following terminal command to create a PostgreSQL service instance for the sample app. Our service instance is `rails-postgres`. It uses the `postgresql-10-odb` service and the `standalone` plan. For more information about the `postgresql-10-odb` service, see [Crunchy PostgreSQL](#) [topic](#).

```
$ cf create-service postgresql-10-odb standalone rails-postgres
Creating service rails-postgres in org YOUR-ORG / space development as clouser@example.com...
OK
```

### Step 4: Deploy the App

Make sure you are in the `cf-sample-app-rails` directory. Run the following terminal command to deploy the app:

```
$ cf push cf-sample-app-rails
```

`cf push cf-sample-app-rails` creates a URL route to your application in the form `HOST.DOMAIN`. In this example, `HOST` is `cf-sample-app-rails`. Administrators specify the `DOMAIN`. For example, for the `DOMAIN` `shared-domain.example.com`, running `cf push cf-sample-app-rails` creates the URL `cf-sample-app-rails.shared-domain.example.com`.

The example below shows the terminal output when deploying the `cf-sample-app-rails`. `cf push` uses the instructions in the manifest file to create the app, create and bind the route, and upload the app. It then follows the information in the manifest to start one instance of the app with 256M of RAM. After the app starts, the output displays the health and status of the app.

```
$ cf push cf-sample-app-rails
Using manifest file ~/workspace/cf-sample-app-rails/manifest.yml

Creating app cf-sample-app-rails in org my-org / space dev as clouduser@example.com...
OK

Creating route cf-sample-app-rails.cfapps.io...
OK

Binding cf-sample-app-rails.cfapps.io to cf-sample-app-rails...
OK

Uploading cf-sample-app-rails...
Uploading app files from: ~/workspace/cf-sample-app-rails
Uploading 746.6K, 136 files
Done uploading
OK

Starting app cf-sample-app-rails in org my-org / space dev as clouduser@example.com...
...
0 of 1 instances running, 1 starting
1 of 1 instances running

App started


OK

App cf-sample-app-rails was started using this command `bundle exec rails server -p $PORT`

Showing health and status for app cf-sample-app-rails in org my-org / space dev as clouduser@example.com...
OK

requested state: started
instances: 1/1
usage: 512M x 1 instances
urls: cf-sample-app-rails.cfapps.io
last uploaded: Fri Dec 22 18:08:32 UTC 2017
stack: cflinuxfs2
buildpack: ruby

state since cpu memory disk details
#0 running 2017-12-22 10:09:57 AM 0.0% 20.7M of 512M 186.8M of 1G
```

 **Note:** If you want to view log activity while the app deploys, launch a new terminal window and run `cf logs cf-sample-app-rails`.

## Step 5: Bind the Service Instance

1. Run the command below to bind the service instance to the sample app. Once bound, environment variables are stored that allow the app to connect to the service after a `cf push`, `cf restage`, or `cf restart` command.

```
$ cf bind-service cf-sample-app-rails rails-postgres
Binding service rails-postgres to app cf-sample-app-rails in org my-org / space dev
OK
TIP: Use 'cf restage cf-sample-app-rails' to ensure your env variable changes take effect
```

2. Run the following command to restage the sample app.

```
$ cf restage cf-sample-app-rails
```

3. Run the following command to verify the service instance is bound to the sample app.

```
$ cf services
Getting services in org my-org / space dev
OK
name service plan bound apps last operation
rails-postgres postgresql-10-odb standalone cf-sample-app-rails create succeeded
```



## Step 6: Verify the App

Verify that the app is running by browsing to the URL generated in the output of the previous step. In this example, navigating to `cf-sample-app-rails.shared-domain.example.com` verifies that the app is running.

You've now pushed an app to PAS! For more information about this topic, see the [Deploy an Application](#) topic.

## What to Do Next

You have deployed an app to PCF. Consult the sections below for information about what to do next.

## Test a Deployed App

Use the cf CLI or [Apps Manager](#) to review information and administer your app and your PCF account. For example, you could edit the `manifest.yml` file to increase the number of app instances from 1 to 3 or redeploy the app with a new app name.

## Manage Your App with the cf CLI

Run `cf help` to view a complete list of commands and run `cf help COMMAND` for detailed information about a specific command. For more information about using the cf CLI, refer to the cf CLI topics, especially the [Getting Started with cf CLI](#) topic.

## Troubleshooting

If your app fails to start, verify that the app starts in your local environment. Refer to the [Troubleshooting Application Deployment and Health](#) topic to learn more about troubleshooting.

## Configure Rake Tasks for Deployed Apps

Page last updated:

For PAS to automatically invoke a Rake task while a Ruby or Ruby on Rails app is deployed, you must do the following:

- Include the Rake task in your app
- Configure the application start command using the `command` attribute in the application manifest

The following is an example that shows how to invoke a Rake database migration task at application startup.

1. Create a file with the Rake task name and the extension `.rake`, and store it in the `lib/tasks` directory of your application.
2. Add the following code to your rake file:

```
namespace :cf do
 desc "Only run on the first application instance"
 task :on_first_instance do
 instance_index = JSON.parse(ENV["VCAP_APPLICATION"])["instance_index"] rescue nil
 exit(0) unless instance_index == 0
 end
end
```

This Rake task limits an idempotent command to the first instance of a deployed application.

3. Add the task to the `manifest.yml` file with the `command` attribute, referencing the idempotent command `rake db:migrate` chained with a start command.

```
applications:
- name: my-rails-app
 command: bundle exec rake cf:on_first_instance db:migrate && rails s -p $PORT
```

## Environment Variables Defined by the Ruby Buildpack

Pivotal Application Service provides configuration information to apps through environment variables. This topic describes the additional environment variables provided by the Ruby buildpack.

For more information about the standard environment variables provided by Pivotal Application Service, see the [Cloud Foundry Environment Variables](#) topic.

## Ruby Buildpack Environment Variables

The following table describes the environment variables provided by the Ruby buildpack.

| Environment Variable         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>BUNDLE_BIN_PATH</code> | The directory where Bundler installs binaries. Example:<br><code>BUNDLE_BIN_PATH:/home/vcap/app/vendor/bundle/ruby/1.9.1/gems/bundler-1.3.2/bin/bundle</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>BUNDLE_GEMFILE</code>  | The path to the Gemfile for the app. Example: <code>BUNDLE_GEMFILE:/home/vcap/app/Gemfile</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <code>BUNDLE_WITHOUT</code>  | Instructs Cloud Foundry to skip gem installation in excluded groups. Use this with Rails applications, where “assets” and “development” gem groups typically contain gems that are not needed when the app runs in production. Example:<br><code>BUNDLE_WITHOUT=assets</code>                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>DATABASE_URL</code>    | Cloud Foundry examines the <code>database_uri</code> for bound services to see if they match known database types. If known relational database services are bound to the app, then the <code>DATABASE_URL</code> environment variable is set to the first services in the list.<br><br>If your application requires that <code>DATABASE_URL</code> is set to the connection string for your service, and Cloud Foundry does not set it, use the Cloud Foundry Command Line Interface (cf CLI) <code>cf set-env</code> command to set this variable manually. Example:<br><pre>\$ cf set-env my-app DATABASE_URL mysql://example-database-connection-string</pre> |
| <code>GEM_HOME</code>        | The directory where gems are installed. Example: <code>GEM_HOME:/home/vcap/app/vendor/bundle/ruby/1.9.1</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>GEM_PATH</code>        | The directory where gems can be found. Example: <code>GEM_PATH=/home/vcap/app/vendor/bundle/ruby/1.9.1:</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>RACK_ENV</code>        | The Rack deployment environment, which governs the middleware loaded to run the app. Valid value are <code>development</code> , <code>deployment</code> , and <code>none</code> . Example: <code>RACK_ENV=none</code>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>RAILS_ENV</code>       | The Rails deployment environment, which controls which environment-specific configuration file governs how the app is executed. Valid value are <code>development</code> , <code>test</code> , and <code>production</code> . Example: <code>RAILS_ENV=production</code>                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>RUBYOPT</code>         | Defines command-line options passed to Ruby interpreter. Example:<br><code>RUBYOPT: -I/home/vcap/app/vendor/bundle/ruby/1.9.1/gems/bundler-1.3.2/lib -rbundler/setup</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Configure Service Connections for Ruby

Page last updated:

After you create a service instance and bind it to an application, you must configure the application to connect to the service.

### Query VCAP\_SERVICES with cf-app-utils

The `cf-app-utils` gem allows your application to search for credentials from the `VCAP_SERVICES` environment variable by name, tag, or label.

- [cf-app-utils-ruby](#) ↗

### VCAP\_SERVICES defines DATABASE\_URL

At runtime, Cloud Foundry creates a `DATABASE_URL` environment variable for every application based on the `VCAP_SERVICES` environment variable.

Example VCAP\_SERVICES:

```
VCAP_SERVICES =
{
 "postgresql-10-odb": [
 {
 "name": "postgresql-10-odb-c6c60",
 "label": "postgresql-10-odb",
 "credentials": {
 "uri": "postgres://exampleuser:examplepass@babar.postgresql-10-odb.com:5432/exampledb"
 }
 }
]
}
```

Based on this `VCAP_SERVICES`, Cloud Foundry creates the following `DATABASE_URL` environment variable:

```
DATABASE_URL = postgres://exampleuser:examplepass@babar.postgresql-10-odb.com:5432/exampledb
```

Cloud Foundry uses the structure of the `VCAP_SERVICES` environment variable to populate `DATABASE_URL`. Any service containing a JSON object with the following form will be recognized by Cloud Foundry as a candidate for `DATABASE_URL`:

```
{
 "some-service": [
 {
 "credentials": {
 "uri": "<some database URL>"
 }
 }
]
}
```

Cloud Foundry uses the first candidate found to populate `DATABASE_URL`.

### Configure Non-Rails Applications

Non-Rails applications can also access the `DATABASE_URL` variable.

If you have more than one service with credentials, only the first will be populated into `DATABASE_URL`. To access other credentials, you can inspect the `VCAP_SERVICES` environment variable.

```
vcap_services = JSON.parse(ENV['VCAP_SERVICES'])
```

Use the hash key for the service to obtain the connection credentials from `VCAP_SERVICES`.

- For services that use the [v2 format](#), the hash key is the name of the service.
- For services that use the [v1 format](#), the hash key is formed by combining the service provider and version, in the format PROVIDER-VERSION.

For example, the service provider “p-mysql” with version “n/a” forms the hash key `p-mysql-n/a`.

## Seed or Migrate Database

Before you can use your database the first time, you must create and populate or migrate it. For more information about migrating database schemas, see [Services Overview](#).

## Troubleshooting

To aid in troubleshooting issues connecting to your service, you can examine the environment variables and log messages Cloud Foundry records for your application.

### View Environment Variables

Use the `cf env` command to view the Cloud Foundry environment variables for your application. `cf env` displays the following environment variables:

- The `VCAP_SERVICES` variables existing in the container environment
- The user-provided variables set using the `cf set-env` command

```
$ cf env my-app
Getting env variables for app my-app in org My-Org / space development as admin...
OK

System-Provided:
{
 "VCAP_SERVICES": {
 "p-mysql-n/a": [
 {
 "credentials": {
 "uri": "postgres://lrra:e6B-X@p-mysqlprovider.example.com:5432/lrra"
 },
 "label": "p-mysql-n/a",
 "name": "p-mysql",
 "syslog_drain_url": "",
 "tags": ["postgres", "postgresql", "relational"]
 }
]
 }
}

User-Provided:
my-env-var: 100
my-drain: http://drain.example.com
```

### View Logs

Use the `cf logs` command to view the Cloud Foundry log messages for your application. You can direct current logging to standard output, or you can dump the most recent logs to standard output.

Run `cf logs APPNAME` to direct current logging to standard output:

```
$ cf logs my-app
Connected, tailing logs for app my-app in org My-Org / space development as admin...
1:27:19.72 [App/0] OUT [CONTAINER] org.apache.coyote.http11.Http11Protocol INFO Starting ProtocolHandler ["http-bio-61013"]
1:27:19.77 [App/0] OUT [CONTAINER] org.apache.catalina.startup.Catalina INFO Server startup in 10427 ms
```

Run `cf logs APPNAME --recent` to dump the most recent logs to standard output:

```
$ cf logs my-app --recent
```

```
Connected, dumping recent logs for app my-app in org My-Org / space development as admin...
```

```
1:27:15.93 [App/0] OUT 15,935 INFO EmbeddedDatabaseFactory:124 - Creating embedded database 'SkyNet'
```

```
1:27:16.31 [App/0] OUT 16,318 INFO LocalEntityManagerFactory:287 - Building TM container EntityManagerFactory for unit 'default'
```

```
1:27:16.50 [App/0] OUT 16,505 INFO Version:37 - HCANN001: Hibernate Commons Annotations {4.0.1.Final}
```

```
1:27:16.51 [App/0] OUT 16,517 INFO Version:41 - HHH412: Hibernate Core {4.1.9.Final}
```

```
1:27:16.95 [App/0] OUT 16,957 INFO SkyNet-Online:73 - HHH268: Transaction strategy: org.hibernate.internal.TransactionFactory
```

```
1:27:16.96 [App/0] OUT 16,963 INFO InitiateTerminatorT1000Deployment:48 - HHH000397: Using TranslatorFactory
```

```
1:27:17.02 [App/0] OUT 17,026 INFO Version:27 - HV001: Hibernate Validator 4.3.0.Final
```

If you encounter the error, “A fatal error has occurred. Please see the Bundler troubleshooting documentation,” update your version of bundler and run

```
bundle install
```

```
$ gem update bundler
```

```
$ gem update --system
```

```
$ bundle install
```

## Support for Windows Gemfiles

Page last updated:

This topic describes how the Ruby buildpack handles dependencies on Windows machines.

### Windows Gemfiles

When a `Gemfile.lock` is generated on a Windows machine, it often contains gems with Windows-specific versions. This results in versions of gems such as `mysql2`, `thin`, and `pg` containing “-x86-mingw32.” For example, the `Gemfile` may contain the following:

```
gem 'sinatra'
gem 'mysql2'
gem 'json'
```

When you run `bundle install` with the above `Gemfile` on a Windows machine, it results in the following `Gemfile.lock`:

```
GEM remote: http://rubygems.org/
specs:
 json (1.7.3)
 mysql2 (0.3.11-x86-mingw32)
 rack (1.4.1)
 rack-protection (1.2.0)
 rack sinatra (1.3.2)
 rack (~> 1.3, >= 1.3.6)
 rack-protection (~> 1.2)
 tilt (~> 1.3, >= 1.3.3)
 tilt (1.3.3)
PLATFORMS x86-mingw32
DEPENDENCIES
 json
 mysql2
 sinatra
```

Notice the “-x86-mingw32” in the version number of `mysql2`. Since Cloud Foundry runs on Linux machines, this would fail to install. To mitigate this, the Ruby Buildpack removes the `Gemfile.lock` and uses Bundler to resolve dependencies from the `Gemfile`.



**Note:** Removing the `Gemfile.lock` will cause dependency versions to be resolved from the `Gemfile`. This could result in different versions being installed than those listed in the `Gemfile.lock`.

## Staticfile Buildpack

Page last updated:

### Overview

This topic describes how to configure and use the Staticfile buildpack.



**Note:** [BOSH configured custom trusted certificates](#) are not supported by the Staticfile buildpack.

### Definitions

**Staticfile app:** An app or content that requires no backend code other than the NGINX webserver, which the buildpack provides. Examples of staticfile apps are front-end JavaScript apps, static HTML content, and HTML/JavaScript forms.

**Staticfile buildpack:** The buildpack that provides runtime support for staticfile apps and apps with backends hosted elsewhere. To find which version of NGINX the current Staticfile buildpack uses, see the [Staticfile buildpack release notes](#).

### Staticfile Detection

If you create a file named `.staticfile` in the root directory of your app, Cloud Foundry automatically uses the Staticfile buildpack when you push your app.

The `.staticfile` file can be an empty file, or it can contain configuration settings for your app. For more information, see [Configuring the Buildpack](#) and [Pushing an App](#).

### Memory Usage

NGINX requires 20 MB of RAM to serve static assets. When using the Staticfile buildpack, we recommend pushing apps with the `-m 64M` option to reduce RAM allocation from the default 1 GB allocated to containers by default.

## Configure the Buildpack

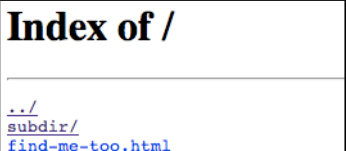




This section describes configuration options available for the Staticfile buildpack. If you need to make configuration changes to NGINX that are not listed in the table below, use the NGINX Buildpack instead of the Staticfile buildpack. For more information, see [NGINX Buildpack](#).

### Staticfile File Configuration

To configure these options, add the configuration property as a new line in your `.staticfile` file as described in the following table.

| Staticfile Configuration Property                                                   | Description                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>root: YOUR-DIRECTORY-NAME</code><br><br>Example:<br><code>root: public</code> | <p><b>Alternative root:</b> Specifies a root directory other than the default. Use this option to serve <code>index.html</code> and other assets, such as HTML, CSS, or JavaScript files, from a location other than the root directory.</p> <p>For example, you can specify an alternate folder such as <code>dist</code> or <code>public</code>.</p> |
| <code>directory: visible</code>                                                     | <p><b>Directory list:</b> Displays an HTML page that shows a directory index for your site. A sample of a directory list is shown below.</p>                                                                                                                                                                                                           |



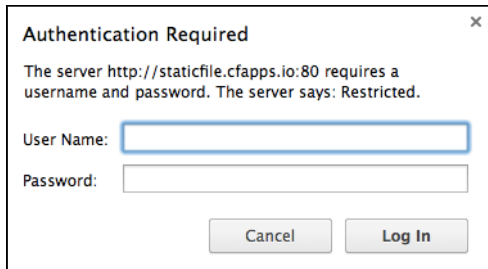
|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <pre>ssi: enabled</pre>                                                                                                                                                           | <p><b>SSI:</b> Enables Server Side Includes (SSI), which allow you to embed the contents of one or more files into a web page on a web server. For general information about SSI, see the <a href="#">Server Side Includes</a> entry on Wikipedia.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>pushstate: enabled</pre>                                                                                                                                                     | <p><b>Pushstate routing:</b> Keeps browser-visible URLs clean for client-side JavaScript apps that serve multiple routes. For example, pushstate routing allows a single JavaScript file to route to multiple anchor-tagged URLs that look like <code>/some/path1</code> instead of <code>/some#path1</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <pre>gzip: off</pre>                                                                                                                                                              | <p><b>GZip file serving and compression:</b> Disables <a href="#">gzip_static</a> and <a href="#">gunzip</a> modules, which are enabled by default. These modules allow NGINX to serve files stored in compressed GZ format and to uncompress them for clients that do not support compressed content or responses.</p> <p>You may want to disable compression under particular circumstances such as serving content to very old browser clients.</p>                                                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>http_proxy: HTTP-URL</pre> <pre>https_proxy: HTTPS-URL</pre> <p>Example:</p> <pre>http_proxy: http://www.example.com/</pre> <pre>https_proxy: https://www.example.com/</pre> | <p><b>Proxy support:</b> Allows you to use a proxy when downloading dependencies during the staging of your app.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <pre>force_https: true</pre> <p>Alternatively, set the <code>FORCE_HTTPS</code> environment variable to <code>true</code>.</p>                                                    | <p><b>Force HTTPS:</b> Forces all requests to be sent through HTTPS. This redirects non-HTTPS requests as HTTPS requests.</p> <div> <p> <b>Note:</b> Do not enable <code>FORCE_HTTPS</code> if you have a proxy server or load balancer that terminates SSL/TLS. Doing so can cause infinite redirect loops, for example, if you use <a href="#">Flexible SSL</a> with CloudFlare.</p> </div>                                                                                                                                                                                                                                                                                                                                                                                      |
| <pre>host_dot_files: true</pre>                                                                                                                                                   | <p><b>Dot files:</b> By default, hidden files, which are those starting with a <code>.</code>, are not served by this buildpack.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <pre>http_strict_transport_security: true</pre>                                                                                                                                   | <p><b>HTTP Strict Transport Security (HSTS):</b> Causes NGINX to respond to all requests with the header <code>Strict-Transport-Security: max-age=31536000</code>. This forces receiving browsers to make all subsequent requests over HTTPS. This setting defaults to a <code>max-age</code> of one year.</p> <div> <p> <b>Note:</b> Because this setting persists in browsers for a long time, only enable this setting after you ensure that you have completed your app configuration.</p> </div>                                                                                                                                                                                                                                                                              |
| <pre>http_strict_transport_security_include_subdomains: true</pre>                                                                                                                | <p><b>HSTS includes subdomains:</b> Causes NGINX to respond to all requests with the following header: <code>Strict-Transport-Security: max-age=31536000; includeSubDomains</code>. This forces browsers to make all subsequent requests over HTTPS including subdomains. This setting defaults to a <code>max-age</code> of one year.</p> <div> <p> <b>Note:</b> Setting this property to <code>true</code> also makes <code>http_strict_transport_security</code> default to true.</p> </div>                                                                                                                                                                                                                                                                                    |
| <pre>http_strict_transport_security_preload: true</pre>                                                                                                                           | <p><b>HSTS preload:</b> Causes NGINX to respond to all requests with the following header: <code>Strict-Transport-Security: max-age=31536000; includeSubDomains; preload</code>. This forces browsers to make all subsequent requests over HTTPS including subdomains and requests inclusion in browser-managed HSTS preload lists. For more information, see <a href="https://hstspreload.org">https://hstspreload.org</a>. This setting defaults to a <code>max-age</code> of one year. This setting defaults to a <code>max-age</code> of one year.</p> <div> <p> <b>Note:</b> Setting this property to <code>true</code> also makes <code>http_strict_transport_security</code> and <code>http_strict_transport_security_include_subdomains</code> default to true.</p> </div> |

## Other Configuration

Follow the instructions below to make other configuration changes.

### Basic Authentication

Allows you to enable basic authentication for your app or website. A sample basic authentication dialog box is shown below:



You can create a hashed username and password pair for each user by using a site like [Htpasswd Generator](#).

### Configuration

Add a new `Staticfile.auth` file to the root or alternative root directory. In the new file, add one or more username and password entries using the following format: `USERNAME:HASHED_PASSWORD`

Example:

```
pat:$example1$DuUQEQp8$ZccZCHQEINSjrgerw$FC0
stevie:$example1$22derfaecZSJJRw4rKE$KKEWKS
```

### Custom Location

Allows you to specify custom location definitions with additional directives. For information about NGINX directives, see [Creating NGINX Plus and NGINX Configuration Files](#) and [Alphabetical index of directives](#) in the *NGINX documentation*.

### Configuration

To customize the `location` block of the NGINX configuration file, follow the steps below.

1. Set an alternative `root` directory. The `location_include` property only works in conjunction with an alternative `root`.
2. Create a file with location-scoped NGINX directives. See the following example, which causes visitors of your site to receive the `X-MySiteName` HTTP header:
  - o **File:** `nginx/conf/includes/custom_header.conf`
  - o **Content:** `add_header X-MySiteName BestSiteEver;`
3. Set the `location_include` variable in your **Staticfile** to the path of the file from the previous step. This path is relative to `nginx/conf`.

Example:

```
...
root: public
location_include: includes/*.conf
...
```

### Additional MIME Type Support

Allows you to configure additional MIME types on your NGINX server.

### Configuration

To add MIME types, add a `mime.types` file to your root folder, or to the alternate root folder if you specified one.

For more information about the `mime.types` file, see [mime.types](#) in the *NGINX documentation*.

Example MIME types file:

```
types {
 text/html html htm shtml;
 text/css css;
 text/xml xml rss;
 image/gif gif;
 ...
}
```

## Push an App

To push your app, you can use either the system Staticfile buildpack or specify a Staticfile buildpack.

### Option 1: Use the System Staticfile Buildpack

To use the Staticfile buildpack installed in your deployment, run the command below in the root directory of the app. The root directory of the app must contain a file named `Staticfile`.

```
cf push APP-NAME
```

Where `APP-NAME` is the name you want to give your app.

For example:

```
$ cf push my-app
Creating app my-app in org sample-org / space sample-space as username@example.com...
OK
...
requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: my-app.example.com
last uploaded: Wed Apr 1 12:55:41 UTC 2020
stack: cflinuxfs2
buildpack: staticfile
```

|    | state   | since                  | cpu  | memory      | disk       | details |
|----|---------|------------------------|------|-------------|------------|---------|
| #0 | running | 2020-04-01 12:55:57 PM | 0.0% | 12.6M of 1G | 5.9M of 1G |         |

### Option 2: Specify a Staticfile Buildpack

To explicitly specify a Staticfile buildpack, run the command below in the root directory of the app. You may want to specify a buildpack if your deployment does not have the Staticfile buildpack installed or the installed version is outdated.

```
cf push APP-NAME -b BUILDPACK-NAME-OR-PATH
```

Where:

- `APP-NAME` is the name you want to give your app.
- `BUILDPACK-NAME-OR-PATH` is either the name of a buildpack that is installed in your deployment or the path to a buildpack. You can find the Cloud Foundry Staticfile buildpack in the [Staticfile repository](#) on GitHub.

For example:

```
$ cf push my-app -b https://github.com/cloudfoundry/staticfile-buildpack.git
Creating app my-app in org sample-org / space sample-space as username@example.com...
OK
...
requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: my-app.example.com
last uploaded: Wed Apr 1 12:55:41 UTC 2020
stack: cflinuxfs2
buildpack: https://github.com/cloudfoundry/staticfile-buildpack.git
```

|    | state   | since                  | cpu  | memory      | disk       | details |
|----|---------|------------------------|------|-------------|------------|---------|
| #0 | running | 2020-04-01 12:55:57 PM | 0.0% | 12.6M of 1G | 5.9M of 1G |         |

## Verifying the Push

After you push the app, follow the steps below to verify that the push was successful:

1. Find the URL of your app in the output of the `cf push` command. For example, the URL in the terminal output above is `my-app.example.com`.
2. In a browser, navigate to the URL to view your app.

## Example Staticfile Buildpack Apps

For different examples of apps that use the Staticfile buildpack, see the [fixtures](#) directory in the Staticfile buildpack GitHub repo.

## Help and Support

A number of channels exist where you can get more help when using the Staticfile buildpack, or with developing your own Staticfile buildpack.

- **Staticfile Buildpack Repository in Github:** Find more information about using and extending the Staticfile buildpack in [GitHub repository](#).
- **Release Notes:** Find current information about this buildpack on the Staticfile buildpack [release page](#) in GitHub.
- **Slack:** Join the #buildpacks channel in the [Cloud Foundry Slack community](#).

## Customizing and Developing Buildpacks

Page last updated:

Buildpacks enable you to packaging frameworks and/or runtime support for your application. Cloud Foundry provides with system buildpacks out-of-the-box and provides an interface for customizing existing buildpacks and developing new ones.

## Customizing and Creating Buildpacks

If your application uses a language or framework that the Cloud Foundry system buildpacks do not support, do one of the following:

- Use a [Cloud Foundry Community Buildpack](#).
- Use a [Heroku Third-Party Buildpack](#).
- Customize an existing buildpack or create your own [custom buildpack](#). A common development practice for custom buildpacks is to fork existing buildpacks and sync subsequent patches from upstream. For information about customizing an existing buildpack or creating your own, see the following:
  - [Creating Custom Buildpacks](#)
  - [Packaging Dependencies for Offline Buildpacks](#)

## Maintaining Buildpacks

After you have modified an existing buildpack or created your own, it is necessary to maintain it. Refer to the following when maintaining your own buildpacks:

- [Merging from Upstream Buildpacks](#)
- [Upgrading Dependency Versions](#)



**Note:** To configure a production server for your web app, see the [Configuring a Production Server](#) topic.

## Using CI for Buildpacks

For information about updating and releasing a new version of a Cloud Foundry buildpack through the Cloud Foundry Buildpacks Team Concourse pipeline, see [Using CI for Buildpacks](#). You can use this as a model when working with Concourse to build and release new versions of your own buildpacks.

## Creating Custom Buildpacks

Page last updated:

This topic describes how to create custom buildpacks for Pivotal Application Service (PAS).

For more information about how buildpacks work, see the [Buildpacks](#) topic.

## Package Custom Buildpacks

PAS buildpacks can work with limited or no Internet connectivity. The [buildpack-packager](#) gives the same flexibility to custom buildpacks, enabling them to work in partially or completely disconnected environments.

### Use the Buildpack Packager

1. Ensure that you have installed the [buildpack-packager](#).
2. Create a manifest.yml in your buildpack.
3. Run the packager in cached mode:

```
$ buildpack-packager build -cached -any-stack
```


The packager will add (almost) everything in your buildpack directory into a zip file. It will exclude anything marked for exclusion in your manifest.

In cached mode, the packager downloads and adds dependencies as described in the manifest.

For more information, see the documentation in the [buildpack-packager Github repository](#).

### Use and Share the Packaged Buildpack

After you have packaged your buildpack using `buildpack-packager` you can use the resulting `.zip` file locally, or share it with others by uploading it to any network location that is accessible to the CLI. Users can then specify the buildpack with the `-b` option when they push apps. See [Deploying Apps with a Custom Buildpack](#) for details.

 **Note:** Offline buildpack packages may contain proprietary dependencies that require distribution licensing or export control measures. For more information about offline buildpacks, refer to [Packaging Dependencies for Offline Buildpacks](#).

You can also use the `cf create-buildpack` command to upload the buildpack into your Cloud Foundry deployment, making it accessible without the `-b` flag:

```
$ cf create-buildpack BUILDPACK_PATH POSITION [--enable|--disable]
```

You can find more documentation in the [Managing Custom Buildpacks](#) topic.

### Specify a Default Version

As of [buildpack-packager version 2.3.0](#), you can specify the default version for a dependency by adding a `default_versions` object to the `manifest.yml` file. The `default_versions` object has two properties, `name` and `version`. For example:

```
default_versions:
- name: go
 version: 1.6.3
- name: other-dependency
 version: 1.1.1
```

To specify a default version:

1. Add the `default_version` object to your manifest, following the [rules](#) below. You can find a complete example manifest in the PAS [go-buildpack](#) repository.
2. Run the `default_version_for` script from the [compile-extensions](#) repository, passing the path of your `manifest.yml` and the dependency name as arguments. The following command uses the example manifest from step 1:

```
$./compile-extensions/bin/default_version_for manifest.yml go 1.6.3
```

## Rules for Specifying a Default Version

The `buildpack-packager` script validates this object according to the following rules:

- You can create at most one entry under `default_versions` for a single dependency. The following example causes `buildpack-packager` to fail with an error because the manifest specifies two default versions for the same `go` dependency.

```
Incorrect; will fail to package
default_versions:
- name: go
 version: 1.6.3
- name: go
 version: 1.7.5
```

- If you specify a `default_version` for a dependency, you must also list that dependency and version under the `dependencies` section of the manifest. The following example causes `buildpack-packager` to fail with an error because the manifest specifies `version: 1.9.2` for the `go` dependency, but lists `version: 1.7.5` under `dependencies`.

```
Incorrect; will fail to package
default_versions:
- name: go
 version: 1.9.2

dependencies:
- name: go
 version: 1.7.5
 uri: https://storage.googleapis.com/golang/go1.7.5.linux-amd64.tar.gz
 md5: c8cb76e2308c792e2705c2eb1b55de95
 cf_stacks:
 - cflinuxfs2
```

## Core Buildpack Communication Contract

This section describes the communication contract followed by the PAS core buildpacks. This contract enables buildpacks to interact with one another, so that developers can use multiple buildpacks with their applications.

Buildpack developers must ensure their custom buildpacks follow the contract.

This section uses the following placeholders:

- `IDX` is the zero-padded index matching the position of the buildpack in the priority list.
- `MD5` is the MD5 checksum of the buildpack's URL.

For all buildpacks that supply dependencies via `/bin/supply`:

- The buildpack must create `/tmp/deps/IDX/config.yml` to provide a name to subsequent buildpacks. This file may also contain miscellaneous configuration for subsequent buildpacks.
- The `config.yml` file should be formatted as follows, replacing `BUILDPACK` with the name of the buildpack providing dependencies and `YAML-OBJECT` with the YAML object that contains buildpack-specific configuration: `name: BUILDPACK config: YAML-OBJECT`
- The following directories may be created inside of `/tmp/deps/IDX/` to provide dependencies to subsequent buildpacks:
  - `/bin`: Contains binaries intended for `$PATH` during staging and launch
  - `/lib`: Contains libraries intended for `$LD_LIBRARY_PATH` during staging and launch
  - `/include`: Contains header files intended for compilation during staging
  - `/pkgconfig`: Contains `pkgconfig` files intended for compilation during staging
  - `/env`: Contains environment vars intended for staging, loaded as `FILENAME=FILECONTENTS`
  - `/profile.d`: Contains scripts intended for `/app/.profile.d`, sourced before launch

- The buildpack may make use of previous non-final buildpacks by scanning `/tmp/deps/` for index-named directories containing `config.yml`.

For the last buildpack:

- To make use of dependencies provided by the previously applied buildpacks, the last buildpack must scan `/tmp/deps/` for index-named directories containing `config.yml`.
- To make use of dependencies provided by previous buildpacks, the last buildpack:
  - May use `/bin` during staging, or make it available in `$PATH` during launch
  - May use `/lib` during staging, or make it available in `$LD_LIBRARY_PATH` during launch
  - May use `/include`, `/pkgconfig`, or `/env` during staging
  - May copy files from `/profile.d` to `/tmp/app/.profile.d` during staging
  - May use the supplied config object in `config.yml` during the staging process

## Deploy Apps with a Custom Buildpack

Once a custom buildpack has been created and pushed to a public git repository, the git URL can be passed via the cf CLI when pushing an app.

For example, for a buildpack that has been pushed to Github:

```
$ cf push my-new-app -b git://github.com/johndoe/my-buildpack.git
```

Alternatively, you can use a private git repository, with https and username/password authentication, as follows:

```
$ cf push my-new-app -b https://username:password@github.com/johndoe/my-buildpack.git
```


By default, PAS uses the default branch of the buildpack's git repository. You can specify a different branch using the git url as shown in the following example:

```
$ cf push my-new-app -b https://github.com/johndoe/my-buildpack.git#my-branch-name
```

Additionally, you can use tags in a git repository, as follows:


```
$ cf push my-new-app -b https://github.com/johndoe/my-buildpack#v1.4.2
```

The app will then be deployed to PAS, and the buildpack will be cloned from the repository and applied to the app.

 **Note:** If a buildpack is specified using `cf push -b` the `detect` step will be skipped and as a result, no buildpack `detect` scripts will be run.

## Disable Custom Buildpacks

Operators can choose to disable custom buildpacks. For more information, see [Disabling Custom Buildpacks](#).

 **Note:** A common development practice for custom buildpacks is to fork existing buildpacks and sync subsequent patches from upstream. To merge upstream patches to your custom buildpack, use the approach that Github recommends for [syncing a fork](#).



## Packaging Dependencies for Offline Buildpacks

Page last updated:

This topic describes the dependency storage options available to developers creating offline buildpacks.

### About Offline Buildpacks

Online, or uncached, buildpacks require an Internet connection to download dependencies, such as language interpreters and compilers. Alternatively, you can create offline, or cached, buildpacks that are packaged with their dependencies. These offline buildpacks do not connect to the Internet when they are used to deploy Cloud Foundry apps.

 **Note:** Offline buildpacks may contain proprietary dependencies that require distribution licensing or export control measures.

You can find instructions for building the offline packages in the `README.md` file of each buildpack repository. For example, see the [Java buildpack](#).

### Package Dependencies in the Buildpack

The simplest way to package dependencies in a custom buildpack is to keep the dependencies in your buildpack source. However, this is strongly discouraged. Keeping the dependencies in your source consumes unnecessary space.

To avoid keeping the dependencies in source control, load the dependencies into your buildpack and provide a script for the operator to create a zipfile of the buildpack.

For example, the operator might complete the following process:

```
$ # Clones your buildpack
$ git clone http://YOUR-GITHUB-REPOSITORY.example.com/repository
$ cd SomeBuildPacName

$ # Creates a zipfile using your script
$./SomeScriptName
----> downloading-dependencies.... done
----> creating zipfile: ZippedBuildPacName.zip

$ # Adds the buildpack zipfile to the Cloud Foundry instance
$ cf create-buildpack SomeBuildPacName ZippedBuildPacName.zip 1
```

#### Pros


- Least complicated process for operators
- Least complicated maintenance process for buildpack developers

#### Cons

- Cloud Foundry admin buildpack uploads are limited to 1 GB, so the dependencies might not fit
- Security and functional patches to dependencies require updating the buildpack

### Package Selected Dependencies in the Buildpack

This is a variant of the [package dependencies in the buildpack](#) method described above. In this variation, the administrator edits a configuration file such as `dependencies.yml` to include a limited subset of the buildpack dependencies, then packages and uploads the buildpack.

 **Note:** This approach is strongly discouraged. Please see the Cons section below for more information.

The administrator completes the following steps:

```
$ # Clones your buildpack
$ git clone http://YOUR-GITHUB-REPOSITORY.example.com/repository
$ cd SomeBuildPacName

$ # Selects dependencies
$ vi dependencies.yml # Or copy in a preferred config

$ # Builds a package using your script
$./package
----> downloading-dependencies.... done
----> creating zipfile: cobol_buildpack.zip

$ # Adds the buildpack to the Cloud Foundry instance
$ cf create-buildpack cobol-buildpack cobol_buildpack.zip 1

$ # Pushes an app using your buildpack
$ cd ~/my_app
$ cf push my-cobol-webapp -b cobol-buildpack
```

## Pros

- Possible to avoid the Cloud Foundry admin buildpack upload size limit in one of two ways:
  - If the administrator chooses a limited subset of dependencies
  - If the administrator maintains different packages for different dependency sets

## Cons

- More complex for buildpack maintainers
- Security updates to dependencies require updating the buildpack
- Proliferation of buildpacks that require maintenance:
  - For each configuration, there is an update required for each security patch
  - Culling orphan configurations may be difficult or impossible
  - Administrators need to track configurations and merge them with updates to the buildpack
  - May result in with a different config for each app

## Rely on a Local Mirror

In this method, the administrator provides a compatible file store of dependencies. When running the buildpack, the administrator specifies the location of the file store. The buildpack should handle missing dependencies gracefully.

The administrator completes the following process:

```
$ # Clones your buildpack
$ git clone http://YOUR-GITHUB-REPOSITORY.example.com/repository
$ cd SomeBuildPacName

$ # Builds a package using your script
$./package https://dependency/repository
----> creating zipfile: cobol_buildpack.zip

$ # Adds the buildpack to the Cloud Foundry instance
$ cf create-buildpack cobol-buildpack cobol_buildpack.zip 1

$ # Pushes an app using your buildpack
$ cd ~/my_app
$ cf push my-cobol-webapp -b cobol-buildpack
----> deploying app
----> downloading dependencies:
 https://OUR-INTERNAL-SITE.example.com/dependency/repository/dep1.tgz.... done
 https://OUR-INTERNAL-SITE.example.com/dependency/repository/dep2.tgz.... WARNING: dependency not found!
```

## Pros

- Avoids the Cloud Foundry admin buildpack upload size limit
- Leaves the administrator completely in control of providing dependencies
- Security and functional patches for dependencies can be maintained separately on the mirror given the following conditions:
  - The buildpack is designed to use newer semantically versioned dependencies
  - Buildpack behavior does not change with the newer functional changes

## Cons

- The administrator needs to set up and maintain a mirror
- The additional config option presents a maintenance burden

## Merging from Upstream Buildpacks

Page last updated:

This topic describes how to maintain your forked buildpack by merging it with the upstream buildpack. This allows you to keep your fork updated with changes from the original buildpack, providing patches, updates, and new features.

The following procedure assumes that you are maintaining a custom buildpack that was forked from a Cloud Foundry system buildpack. However, you can use the same procedure to update a buildpack forked from any upstream buildpack.

To sync your forked buildpack with an upstream Cloud Foundry buildpack:

1. Navigate to your forked repository on GitHub and click **Compare** in the upper right to display the **Comparing changes** page. This page shows the unmerged commits between your forked buildpack and the upstream buildpack.
2. Inspect the unmerged commits and confirm that you want to merge them all.
3. In a terminal window, navigate to the forked repository and set the upstream remote as the Cloud Foundry buildpack repository.

```
$ cd ~/workspace/ruby-buildpack
$ git remote add upstream git@github.com:cloudfoundry/ruby-buildpack.git
```

4. Pull down the remote upstream changes.

```
$ git fetch upstream
```

5. Merge the upstream changes into the intended branch. You may need to resolve merge conflicts. This example shows merging the `master` branch of the upstream buildpack into the `master` branch of the forked buildpack.

```
$ git checkout master
$ git merge upstream/master
```



**Note:** When merging upstream buildpacks, do not use `git rebase`. This approach is not sustainable because you confront the same merge conflicts repeatedly.

6. Run the buildpack test suite to ensure that the upstream changes do not break anything.

```
$ BUNDLE_GEMFILE=cf.Gemfile buildpack-build
```

7. Push the updated branch.

```
$ git push
```

Your forked buildpack is now synced with the upstream Cloud Foundry buildpack.

For more information about syncing forks, see the Github topic [Syncing a Fork](#).

## Upgrading Dependency Versions

Page last updated:

This topic describes how to upgrade a dependency version in a custom buildpack. These procedures enable Cloud Foundry (CF) operators to maintain custom buildpacks that contain dependencies outside of the dependencies in the CF system buildpacks.

## Cloud Foundry Buildpacks Team Process

**Note:** The procedures in this topic refer to the tools used by the CF buildpacks team, but they do not require the specific tools listed below. You can use any continuous integration (CI) system and workflow management tool to update dependencies in custom buildpacks.

The CF buildpacks team uses the following tools to update dependencies:

- A [Concourse](#) deployment of the [buildpacks-ci](#) pipelines
- The [public-buildpacks-ci-robots](#) GitHub repository
- [Pivotal Tracker](#) for workflow management

When the [New Releases](#) job in the [notifications pipeline](#) detects a new version of a tracked dependency in a buildpack, it creates a [Tracker](#) story about building and including the new version of the dependency in the buildpack manifests. It also posts a message as the `dependency-notifier` to the [#buildpacks channel](#) in the Cloud Foundry Slack channel.

## Build the Binaries

For all dependencies, you must build the binary from source or acquire the binary as a tarball from a trusted source. For most dependencies, the CF buildpacks team builds the binaries from source.

**Note:** The steps below assume you are using a Concourse deployment of the `buildpacks-ci` pipelines and Pivotal Tracker.

To build the binary for a dependency, perform the following steps:

1. Navigate to the `public-buildpacks-ci-robots` directory and verify no uncommitted changes exist.

```
$ cd ~/workspace/public-buildpacks-ci-robots
$ git status
```

2. Run the `git pull` command in the directory to ensure it contains most recent version of the contents.

```
$ git pull -r
```

3. Navigate to the `binary-builds` directory.

```
$ cd binary-builds
```

4. Locate the YAML file for the buildpack you want to build a binary for. The directory contains YAML files for all the packages and dependencies tracked by the CF buildpacks team. Each YAML file correlates to the build queue for one dependency or package, and uses the naming format `DEPENDENCY-NAME.yml`. For example, the YAML file tracking the build queue for Ruby is named `ruby-builds.yml` and contains the following contents:

```

ruby: []
```

5. Different buildpacks use different signatures for verification. Determine which signature your buildpack requires by consulting the list in the [buildpacks](#) section of this topic and run follow the instructions to locate the SHA256, MD5, or GPG signature for the binary:
  - For the SHA256 of a file, run `shasum -a 256 FILE-NAME`.
  - For the MD5 of a file, run `md5 FILE-NAME`.
  - For the GPG signature (for Nginx), see the [Nginx Downloads](#) page.
6. Add the version and verification for the new binary to the YAML file as attributes of an element under the dependency name. For example, to build

the Ruby 2.3.0 binary verified with SHA256, add the following to the YAML file:

```

ruby:
 - version: 2.3.0
 sha256: ba5ba60e5f1aa21b4ef8e9bf35b9ddb57286cb546aac4b5a28c71f459467e507
```



**Note:** Do not preface the version number with the name of the binary or language. For example, specify `2.3.0` for `version` instead of `ruby-2.3.0`.

You can enqueue builds for multiple versions at the same time. For example, to build both the Ruby 2.3.0 binary and the Ruby 2.3.1 binary, add the following to the YAML file:

```

ruby:
 - version: 2.3.0
 sha256: ba5ba60e5f1aa21b4ef8e9bf35b9ddb57286cb546aac4b5a28c71f459467e507
 - version: 2.3.1
 sha256: b87c738cb2032bf4920fef8e3864dc5cf8eae9d89d8d523ce0236945c5797dcd
```

7. Use the `git add` command to stage your changes:

```
$ git add .
```

8. Use the `git commit -m "YOUR-COMMIT-MESSAGE [#STORY-NUMBER]"` command to commit your changes using the Tracker story number. Replace `YOUR-COMMIT-MESSAGE` with your commit message, and `STORY-NUMBER` with the number of your Tracker story.

```
$ git commit -m "make that change [#1234567890]"
```

9. Run `git push` to push your changes to the remote origin.

```
$ git push
```

10. Pushing your changes triggers the binary building process, which you can monitor at the [binary-builder pipeline](#) of your own `buildpacks-ci` Concourse deployment. When the build completes, it adds a link to the Concourse build run to the Tracker story specified in the commit message for the new release.



**Note:** Binary builds are executed by the Cloud Foundry [Binary Builder](#) and the [binary-builder pipeline](#).

## Update Buildpack Manifests

After you build the binary for a dependency that you can access and download from a URL, follow the instructions below to add the dependency version to the buildpack manifest.

**Note:** The steps below assume you are using a Concourse deployment of the `buildpacks-ci` pipelines and Pivotal Tracker.

1. Navigate to the directory of the buildpack for which you want to update dependencies and run `git checkout develop` to check out the `develop` branch.

```
$ cd ~/workspace/ruby-buildpack
$ git checkout develop
```


2. Edit the `manifest.yml` file for the buildpack to add or remove dependencies.


```
dependencies:
 - name: ruby
 version: 2.3.0
 md5: 535342030a11abeb11497824bf642bf2
 uri: https://pivotal-buildpacks.s3.amazonaws.com/concourse-binaries/ruby/ruby-2.3.0-linux-x64.tgz
 cf_stacks:
 - cflinuxfs2
```

- Follow the current structure of the manifest. For example, if the manifest includes the two most recent patch versions for each minor version of

the language, you should also include the two most recent patch versions for each minor version of the language, such as both `ruby-2.1.9` and `ruby-2.1.8`.

- Copy the `uri` and the `md5` from the `build-BINARY-NAME` job that ran in the Concourse binary-builder pipeline and add them to the manifest.

 **Note:** In the PHP buildpack, you may see a `modules` line for each PHP dependency in the manifest. Do not include this `modules` line in your new PHP dependency entry. The `modules` line will be added to the manifest by the `ensure-manifest-has-modules` Concourse job in the `php-buildpack` when you commit and push your changes. You can see this in the output logs of the `build-out` task.

3. Replace any other mentions of the old version number in the buildpack repository with the new version number. The CF buildpack team uses [Ag](#)  for text searching.

```
$ ag OLD-VERSION
```

4. Run the following command to package and upload the buildpack, set up the org and space for tests in the specified CF deployment, and run the CF buildpack tests.

```
$ BUNDLE_GEMFILE=cf.Gemfile buildpack-build
```

If the command fails, you may need to fix or change the tests, fixtures, or other parts of the buildpack.

5. Once the test suite completely passes, use git commands to stage, commit, and push your changes:

```
$ git add .
$ git commit -m "YOUR-MESSAGE[#TRACKER-STORY-ID]"
$ git push
```



6. Monitor the `LANGUAGE-buildpack` pipeline in Concourse. Once the test suite builds, the `specs-lts-develop` job and `specs-edge-develop` job, pass for the buildpack, you can deliver the Tracker story for the new Dependency release. Copy and paste links for the successful test suite builds into the Tracker story.

## Buildpacks



The following list contains information about the buildpacks maintained by the CF buildpacks team.




### Go Buildpack

Go:

- **Built from:** A tarred binary, `GO-VERSION.linux-amd64.tar.gz`, provided by [Google on the Go Downloads](#)  page
- **Verified with:** The MD5 of the tarred binary
- **Example:** [Using the Google Tarred Binary for Go 1.6.2](#) 



Godep:

- **Built from:** A source code `.tar.gz` file from the [Godep Github releases](#)  page
- **Verified with:** The SHA256 of the source **Example:** [Automated enqueueing of binary build for Godep 72](#) 

 **Note:** The [buildpacks-ci](#)  [binary-builder](#)  pipeline automates the process of detecting, uploading, and updating Godep in the manifest.

### Node.js Buildpack

Node:

- **Verified with:** The SHA256 of the `node-vVERSION.tar.gz` file listed on <https://nodejs.org/dist/vVERSION/SHASUMS256.txt> For example, for Node version 4.4.6, the CF buildpacks team verifies with the SHA256 for `node-v4.4.6.tar.gz` on its [SHASUMS256](#)  page.
- **Example:** [Enqueueing binary builds for Node 4.4.5 and 6.2.0](#) 

## Python Buildpack

Python:

- **Verified with:** The MD5 of the `Gzipped source tarball`, listed on `https://www.python.org/downloads/release/python-VERSION/`, where `VERSION` has no periods. For example, for Python version `2.7.12`, use the MD5 for the `Gzipped source tarball` on its [downloads](#) page.
- **Example:** [Enqueuing binary build for Python 2.7.12](#)

## Java Buildpack

OpenJDK:

- **Built from:** The tarred [OpenJDK files](#) managed by the CF Java Buildpack team
- **Verified with:** The MD5 of the tarred OpenJDK files

## Ruby Buildpack

JRuby:

- **Verified with:** The MD5 of the Source `.tar.gz` file from the [JRuby Downloads](#) page
- **Example:** [Enqueuing binary build for JRuby 9.1.2.0](#)

Ruby:

- **Verified with:** The SHA256 of the source from the [Ruby Downloads](#) page
- **Example:** [Enqueuing binary builds for Ruby 2.2.5 and 2.3.1](#)

Bundler:

- **Verified with:** The SHA256 of the `.gem` file from [Rubygems](#)
- **Example:** [Enqueuing binary build for Bundler 1.12.5](#)

## PHP Buildpack

PHP:

- **Verified with:** The SHA256 of the `.tar.gz` file from the [PHP Downloads](#) page.
- To enqueue builds for PHP, you need to edit a file in the `public-buildpacks-ci-robots` repository. For PHP5 versions, the CF buildpacks team enqueues builds in the `binary-builds/php-builds.yml` file. For PHP7 versions, the CF buildpacks team enqueues builds in the `binary-builds/php7-builds.yml` file.
- **Example:** [Enqueuing binary builds for PHP 7.2.5 and 7.0.30](#)

Nginx:

- **Verified with:** The `gpg-rsa-key-id` and `gpg-signature` of the version. The `gpg-rsa-key-id` is the same for each version/build, but the `gpg-signature` will be different. This information is located on the [Nginx Downloads](#) page.
- **Example:** [Enqueuing binary build for Nginx 1.11.0](#)


HTTPD:

- **Verified with:** The MD5 of the `.tar.bz2` file from the [HTTPD Downloads](#) page
- **Example:** [Enqueuing binary build for HTTPD 2.4.20](#)

Composer:

- **Verified with:** The SHA256 of the `composer.phar` file from the [Composer Downloads](#) page
- For Composer, there is no build process as the `composer.phar` file is the binary. In the manual process, connect to the appropriate S3 bucket using the correct AWS credentials. Create a new directory with the name of the composer version, for example `1.0.2`, and put the appropriate `composer.phar` file into that directory. For Composer `v1.0.2`, connect and create the `php/binaries/trusty/composer/1.0.2` directory. Then place the `composer.phar` file into that directory so the binary is available at `php/binaries/trusty/composer/1.0.2/composer.phar`.



 **Note:** The [buildpacks-ci](#) [binary-builder](#) pipeline automates the process of detecting, uploading, and updating Composer in the manifest.

- **Example:** [Automated enqueueing of binary build for Composer 1.1.2](#)

## Staticfile Buildpack

Nginx:

- **Verified with:** The `gpg-rsa-key-id` and `gpg-signature` of the version. The `gpg-rsa-key-id` is the same for each version/build, but the `gpg-signature` will be different. This information is located on the [Nginx Downloads](#) page.
- **Example:** [Enqueueing binary build for Nginx 1.11.0](#)

## Binary Buildpack

The Binary buildpack has no dependencies.

## Using CI for Buildpacks

The Cloud Foundry (CF) Buildpacks team and other CF buildpack development teams use [Concourse continuous integration \(Concourse CI\)](#) [↗](#) pipelines to integrate new buildpack releases. This topic provides links to information that describes how to release new versions of Cloud Foundry buildpacks using Concourse CI, and how to update Ruby gems used for CF buildpack development.

Each of the following are applicable to all supported buildpack languages and frameworks:

- [Releasing a New Buildpack Version](#)
- [Updating Buildpack-Related Gems](#)

## Releasing a New Buildpack Version

Page last updated:

This topic describes how to update and release a new version of a Cloud Foundry (CF) buildpack through the CF Buildpacks Team Concourse [pipeline](#). Concourse is a continuous integration (CI) tool for software development teams. This is the process used by the CF Buildpacks Team and other CF buildpack development teams. You can use this process as a model for using Concourse to build and release new versions of your own buildpacks.

The Concourse pipelines for Cloud Foundry buildpacks are located in the [buildpacks-ci](#) Github repository.

## Release a New Buildpack Version

To release a new buildpack version, perform the following:

1. Ensure you have downloaded the `buildpacks-ci` repository:

```
$ git clone https://github.com/cloudfoundry/buildpacks-ci.git
```

2. From the buildpack directory, check out the `develop` branch of the buildpack:

```
$ cd /system/path/to/buildpack
$ git checkout develop
```

3. Ensure you have the most current version of the repository:

```
$ git pull -r
```

4. Run `bump` to update the version in the buildpack repository:

```
$ /system/path/to/buildpacks-ci/scripts/bump
```

5. Modify the `CHANGELOG` file manually to condense recent commits into relevant changes. For more information, see [Modify Changelogs](#).

6. Add and commit your changes:

```
$ git add VERSION CHANGELOG
$ git commit -m "Bump version to $(cat VERSION) [insert story #]"
```

7. Push your changes to the `develop` branch:

```
$ git push origin develop
```


## Concourse Buildpack Workflow

If `buildpacks-ci` is not deployed to Concourse, manually add a Git tag to the buildpack and mark the tag as a release on Github.

If `buildpacks-ci` is deployed to Concourse, the buildpack update passes through the following life cycle:

1. Concourse triggers the `buildpack-to-master` job in the pipeline for the updated buildpack. This job merges develop onto the master branch of the buildpack.
2. The `detect-new-buildpack-and-upload-artifacts` job triggers in the pipeline for the updated buildpack. This job creates a cached and uncached buildpack and uploads them to an AWS S3 bucket.
3. The `specs-lts-master` and `specs-edge-master` jobs trigger and run the buildpack test suite and the buildpack-specific tests of the [Buildpack Runtime Acceptance Tests \(BRATS\)](#).
4. If you are using [Pivotal Tracker](#), paste the links for the `specs-edge-master` and `specs-lts-master` builds in the related buildpack release story and deliver that story.

5. Your project manager can manually trigger the `buildpack-to-github` job on Concourse as part of the acceptance process. This releases the buildpack to Github.
6. After the buildpack has been released to Github, the `cf-release` pipeline is triggered using the manual trigger of the `recreate-bosh-lite` job on that pipeline. If the new buildpack has been released to Github, the CF that is deployed for testing in the `cf-release` pipeline is tested against that new buildpack.
7. After the `cats` job has successfully completed, your project manager can ship the new buildpacks to the `cf-release` repository and create the new buildpack BOSH release by manually triggering the `ship-it` job.

 **Note:** If errors occur during this workflow, you may need to remove unwanted tags. For more information, see [Handle Unwanted Tags](#).

## Modify Changelogs

The [Ruby Buildpack changelog](#) shows an example layout and content of a changelog. In general, changelogs follow these conventions:

- Reference public tracker stories whenever possible.
- Exclude unnecessary files
- Combine and condense commit statements into individual stories containing valuable changes.

## Handle Unwanted Tags

If you encounter problems with the commit that contains the new version, change the target of the release tag by performing the following:

1. Ensure the repository is in a valid state and is building successfully.
2. Remove the tag from your local repository and from Github.
3. Start a build. The pipeline build script should re-tag the build if it is successful.

## Updating Buildpack-Related Gems

Page last updated:

This topic describes how to update [buildpack-packager](#) and [machete](#), used for CF system buildpack development.

`buildpack-packager` packages buildpacks and `machete` provides an integration test framework.

The CF Buildpacks team uses the [gems-and-extensions pipeline](#) to:

1. Run the integration tests for `buildpack-packager` and `machete`
2. Update the gems in the buildpacks managed by the team

## Running the Update Process



**Note:** The steps below assume you are using a Concourse deployment of the `buildpacks-ci` pipelines

At the end of the process, there will be a new Github release and updates will be applied to the buildpacks.

To update the version of either gem in a buildpack:

1. Confirm that the test job `<gemname>-specs` for the gem to be updated successfully ran on the commit you plan to update.
2. Manually trigger the `<gemname>-tag` job to update (“bump”) the version of the gem.
3. The `<gemname>-release` job will trigger. This will create a new Github release of the gem.
4. Each of the buildpack pipelines (e.g. the [go-buildpack pipeline](#)) has a job which watches for new releases of the gem. When a new release is detected, the buildpack’s `cf.Gemfile` is updated to that release version.
5. The commit made to the buildpack’s `cf.Gemfile` triggers the full integration test suite for that buildpack.



**Note:** The final step will trigger all buildpack test suites simultaneously, causing contention for available shared BOSH-lite test environments.

## Services

Page last updated:

The documentation in this section is intended for developers and operators interested in creating Managed Services for Cloud Foundry. Managed Services are defined as having been integrated with Cloud Foundry via APIs, and enable end users to provision reserved resources and credentials on demand. For documentation targeted at end users, such as how to provision services and integrate them with applications, see [Services Overview](#).

To develop Managed Services for Cloud Foundry, you'll need a Cloud Foundry instance to test your service broker with as you are developing it. You must have admin access to your CF instance to manage service brokers and the services marketplace catalog. For local development, we recommend using [BOSH Lite](#) to deploy your own local instance of Cloud Foundry.

## Table of Contents

- [Overview](#)
- **Service Broker API**
  - [Open Service Broker API](#)
  - [Platform Profiles](#)
  - [Catalog Metadata](#)
  - [Volume Services](#)
  - [Release Notes](#)
- [Managing Service Brokers](#)
- [Access Control](#)
- [Dashboard Single Sign-On](#)
- [Example Service Brokers](#)
- [Binding Credentials](#)
- [Enabling Service Instance Sharing](#)
- [Application Log Streaming](#)
- [Route Services](#)
- [Supporting Multiple Cloud Foundry Instances](#)

## Overview

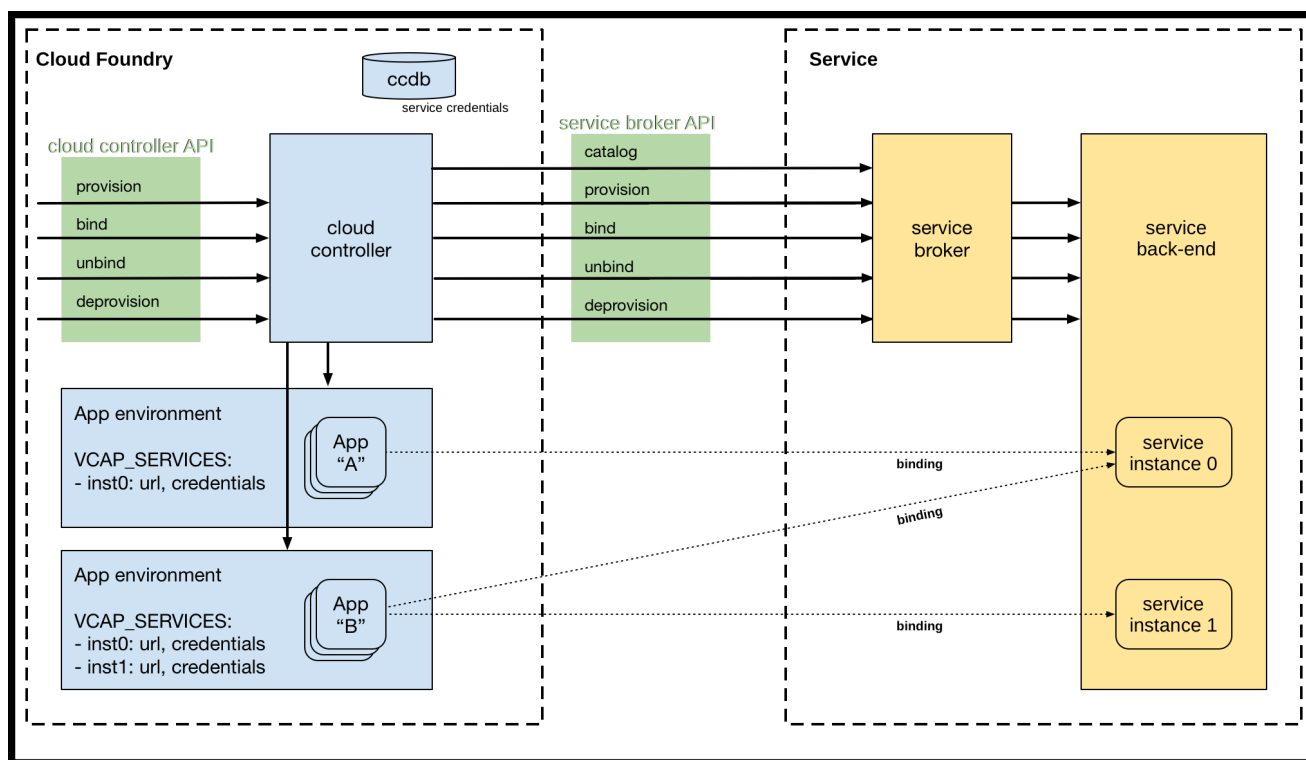
Page last updated:

## Architecture & Terminology

Services are integrated with Cloud Foundry by implementing a documented API for which the cloud controller is the client; we call this the Service Broker API. This should not be confused with the cloud controller API, often used to refer to the version of Cloud Foundry itself; when one refers to “Cloud Foundry v2” they are referring to the version of the cloud controller API. The services API is versioned independently of the cloud controller API.

Service Broker is the term we use to refer to a component of the service which implements the service broker API. This component was formerly referred to as a Service Gateway, however as traffic between applications and services does not flow through the broker we found the term gateway caused confusion. Although gateway still appears in old code, we use the term broker in conversation, in new code, and in documentation.

Service brokers advertise a catalog of service offerings and service plans, as well as interpreting calls for provision (create), bind, unbind, and deprovision (delete). What a broker does with each call can vary between services; in general, ‘provision’ reserves resources on a service and ‘bind’ delivers information to an application necessary for accessing the resource. We call the reserved resource a Service Instance. What a service instance represents can vary by service; it could be a single database on a multi-tenant server, a dedicated cluster, or even just an account on a web application.



[View a larger version of this image.](#)

## Implementation & Deployment

How a service is implemented is up to the service provider/developer. Cloud Foundry only requires that the service provider implement the service broker API. A broker can be implemented as a separate application, or by adding the required http endpoints to an existing service.

Because Cloud Foundry only requires that a service implements the broker API in order to be available to Cloud Foundry end users, many deployment models are possible. The following are examples of valid deployment models.

- Entire service packaged and deployed by BOSH alongside Cloud Foundry
- Broker packaged and deployed by BOSH alongside Cloud Foundry, rest of the service deployed and maintained by other means
- Broker (and optionally service) pushed as an application to Cloud Foundry user space
- Entire service, including broker, deployed and maintained outside of Cloud Foundry by other means





## Managing Service Brokers

Page last updated:

This page assumes you are using cf CLI v6.16 or later.

In order to run many of the commands below, you must be authenticated with Cloud Foundry as an admin user or as a space developer.

### Quick Start

Given a service broker that has implemented the [Service Broker API](#), two steps are required to make its services available to end users in all orgs or a limited number of orgs by service plan.

1. [Register a Broker](#)
2. [Make Plans Public](#)

### Register a Broker

Registering a broker causes Cloud Controller to fetch and validate the catalog from your broker, and save the catalog to the Cloud Controller database. The basic auth username and password which are provided when adding a broker are encrypted in Cloud Controller database, and used by the Cloud Controller to authenticate with the broker when making all API calls. Your service broker should validate the username and password sent in every request; otherwise, anyone could curl your broker to delete service instances. When the broker is registered with an URL having the scheme `https`, Cloud Controller will make all calls to the broker over HTTPS.

As of cf-release 229, CC API 2.47.0, Cloud Foundry supports two types of brokers: *standard brokers* and *space-scoped brokers*. A list of their differences follows:

#### Standard Brokers

- Publish service plans to specific orgs or all orgs in the deployment. Can also keep plans unavailable, or *private*.
- Created by admins, with the command `cf create-service-broker`


```
$ cf create-service-broker mybrokername someuser somethingsecure https://mybroker.example.com/
```

- Managed by admins
- Service plans are created private. Before anyone can use them, an admin must explicitly [make them available](#) within an org or across all orgs.

#### Space-Scoped Brokers

- Publish service plans only to users within the space they are created. Plans are unavailable outside of this space.
- Created by space developers using the command `cf create-service-broker` with the `--space-scoped` flag

```
$ cf create-service-broker mybrokername someuser somethingsecure https://mybroker.example.com/ --space-scoped
```

 **Note:** If a space developer runs `cf create-service-broker` without the `--space-scoped` flag, they receive an error.

- Managed by space developers
- Newly-created plans automatically publish to all users in their space.

### Make Plans Public

After an admin creates a new service plan from a standard broker, no one can use it until the admin explicitly makes it available to users within a specific org or all orgs in the deployment.

See the [Access Control](#) topic for how to make standard broker service plans available to users.

## Multiple Brokers, Services, Plans

Many service brokers may be added to a Cloud Foundry instance, each offering many services and plans. The following constraints should be kept in mind:

- It is not possible to have multiple brokers with the same name
- It is not possible to have multiple brokers with the same base URL
- The service ID and plan IDs of each service advertised by the broker must be unique across Cloud Foundry. GUIDs are recommended for these fields.

See [Possible Errors](#) below for error messages and what to do when you see them.

## List Service Brokers

```
$ cf service-brokers
Getting service brokers as admin...Cloud Controller
OK

Name URL
my-service-broker https://mybroker.example.com
```

## Update a Broker

Updating a broker is how to ingest changes a broker author has made into Cloud Foundry. Similar to adding a broker, update causes Cloud Controller to fetch the catalog from a broker, validate it, and update the Cloud Controller database with any changes found in the catalog.

Update also provides a means to change the basic auth credentials cloud controller uses to authenticate with a broker, as well as the base URL of the broker's API endpoints.

```
$ cf update-service-broker mybrokername someuser somethingsecure https://mybroker.example.com/
```

## Rename a Broker


A service broker can be renamed with the `rename-service-broker` command. This name is used only by the Cloud Foundry operator to identify brokers, and has no relation to configuration of the broker itself.

```
$ cf rename-service-broker mybrokername mynewbrokername
```

## Remove a Broker

Removing a service broker will remove all services and plans in the broker's catalog from the Cloud Foundry Marketplace.


```
$ cf delete-service-broker mybrokername
```

 **Note:** Attempting to remove a service broker will fail if there are service instances for any service plan in its catalog. When planning to shut down or delete a broker, make sure to remove all service instances first. Failure to do so will leave [orphaned service instances](#) in the Cloud Foundry database. If a service broker has been shut down without first deleting service instances, you can remove the instances with the CLI; see [Purge a Service](#). ### Purge a Service ### If a service broker has been shut down or removed without first deleting service instances from Cloud Foundry, you will be unable to remove the service broker or its services and plans from the Marketplace. In development environments, broker authors often destroy their broker deployments and need a way to clean up the Cloud Controller database. The following command will delete a service offering, all of its plans, as well as all associated service instances and bindings from the Cloud Controller database, without making any API calls to a service broker. Once all services for a broker have been purged, the broker can be removed normally.

```
$ cf purge-service-offering service-test
```

Warning: This operation assumes that the service broker responsible for this service offering is no longer available, and all service instances have been deleted, leaving orphan records in Cloud Foundry's database. All knowledge of the service will be removed from Cloud Foundry, including service instances and service bindings. No attempt will be made to contact the service broker; running this command without destroying the service broker will cause orphan service instances. After running this command you may want to run either `delete-service-auth-token` or `delete-service-broker` to complete the cleanup.

```
Really purge service offering service-test from Cloud Foundry? y
OK
```

 **Note:** To purge services from v1 brokers, you must append your `cf purge-service-offering` command with `-p PROVIDER`.

## Purge a Service Instance

The following command will delete a single service instance, its service bindings and its service keys from the Cloud Controller database, without making any API calls to a service broker. This can be helpful in instances a Service Broker is not conforming to the Service Broker API and not returning a 200 or 410 to requests to delete the service instance.

```
$ cf purge-service-instance mysql-dev
```

WARNING: This operation assumes that the service broker responsible for this service instance is no longer available or is not responding with a 200 or 410, and the service instance has been deleted, leaving orphan records in Cloud Foundry's database. All knowledge of the service instance will be removed from Cloud Foundry, including service bindings and service keys.

```
Really purge service instance mysql-dev from Cloud Foundry?> y
Purging service mysql-dev...
OK
```

`purge-service-instance` requires cf-release v218 and cf CLI 6.14.0.

## Catalog Validation Behaviors

When Cloud Foundry fetches a catalog from a broker, it will compare the broker's id for services and plans with the `unique_id` values for services and plans in the Cloud Controller database.

| Event                                                                                                                                      | Action                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| The catalog fails to load or validate.                                                                                                     | Cloud Foundry will return a meaningful error that the broker could not be reached or the catalog was not valid.                          |
| A service or plan in the broker catalog has an ID that is not present among the <code>unique_id</code> values in the marketplace database. | A new record must be added to the marketplace database.                                                                                  |
| A service or plan in the marketplace database are found with a <code>unique_id</code> that matches the broker catalog's ID.                | The marketplace must update the records to match the broker's catalog.                                                                   |
| The database has plans that are not found in the broker catalog, and there are no associated service instances.                            | The marketplace must remove these plans from the database, and then delete services that do not have associated plans from the database. |
| The database has plans that are not found in the broker catalog, but there are provisioned instances.                                      | The marketplace must mark the plan inactive and no longer display it or allow it to be provisioned.                                      |

## Possible Errors

If incorrect basic auth credentials are provided:

```
Server error, status code: 500, error code: 10001, message: Authentication
failed for the service broker API.
Double-check that the username and password are correct:
https://github-broker.a1-app.example.com/v2/catalog
```

If you receive the following errors, check your broker logs. You may have an internal error.

```
Server error, status code: 500, error code: 10001, message:
The service broker response was not understood
```

```
Server error, status code: 500, error code: 10001, message:
The service broker API returned an error from
https://github-broker.a1-app.example.com/v2/catalog: 404 Not Found
```

```
Server error, status code: 500, error code: 10001, message:
The service broker API returned an error from
https://github-broker.primo.example.com/v2/catalog: 500 Internal Server Error
```

If your broker's catalog of services and plans violates validation of presence, uniqueness, and type, you will receive meaningful errors.

```
Server error, status code: 502, error code: 270012, message: Service broker catalog is invalid:
Service service-name-1
 service id must be unique
 service description is required
 service "bindable" field must be a boolean, but has value "true"
Plan plan-name-1
 plan metadata must be a hash, but has value [{"bullets"=>["bullet1", "bullet2"]}]
```

## Managing Access to Service Plans

Page last updated:

All new service plans from standard brokers are private by default. This means that when adding a new broker, or when adding a new plan to an existing broker's catalog, service plans won't immediately be available to end users. This lets an admin control which service plans are available to end users, and manage limited service availability.

Space-scoped brokers are registered to a specific space, and all users within that space can automatically access the broker's service plans. With space-scoped brokers, service visibility is not managed separately.

### Prerequisites

- CLI v6.4.0
- Cloud Controller API v2.9.0 (cf-release v179)
- Admin user access; the following commands can be run only by an admin user

### Display Access to Service Plans

The `service-access` CLI command enables an admin to see the current access control setting for every service plan in the marketplace, across all service brokers.

```
$ cf service-access
getting service access as admin...
broker: elasticsearch-broker
 service plan access orgs
 elasticsearch standard limited

broker: p-mysql
 service plan access orgs
 p-mysql 100mb-dev all
```

The `access` column shows values `all`, `limited`, or `none`, defined as follows:

- `all` - The service plan is available to all users, or *public*.
- `none` - No one can use the service plan; it is *private*.
- `limited` - The plan is available only to users within the orgs listed.

The `-b`, `-e`, and `-o` flags let you filter by broker, service, and org.

```
$ cf help service-access
NAME:
 service-access - List service access settings

USAGE:
 cf service-access [-b BROKER] [-e SERVICE] [-o ORG]

OPTIONS:
 -b access for plans of a particular broker
 -e access for plans of a particular service offering
 -o plans accessible by a particular org
```

### Enable Access to Service Plans

Admins use the `cf enable-service-access` command to give users access to service plans. The command grants access at the org level or across all orgs.

When an org has access to a plan, its users see the plan in the services marketplace (`cf marketplace`) and its Space Developer users can provision instances of the plan in their spaces.

## Enable Access to a Subset of Users

The `-p` and `-o` flags to `cf enable-service-access` let the admin limit user access to specific service plans or orgs as follows:

- `-p PLAN` grants all users access to one service plan (access: `all` )
- `-o ORG` grants users in a specified org access to all plans (access: `limited` )
- `-p PLAN -o ORG` grants users in one org access to one plan (access: `limited` )

For example, the following command grants the org dev-user-org access to the p-mysql service.

```
$ cf enable-service-access p-mysql -o dev-user-org
Enabling access to all plans of service p-mysql for the org dev-user-org as admin...
OK

$ cf service-access
getting service access as admin...
broker: p-mysql
service plan access orgs
p-mysql dev-user-org
```

Run `cf help enable-service-access` to review these options from the command line.

Running `cf enable-service-access SERVICE-NAME` without any flags lets all users access every plan carried by the service. For example, the following command grants all-user access to all `p-mysql` service plans:

```
$ cf enable-service-access p-mysql
Enabling access to all plans of service p-mysql for all orgs as admin...
OK

$ cf service-access
getting service access as admin...
broker: p-mysql
service plan access orgs
p-mysql 100mb-dev all
```

## Disable Access to Service Plans

Admins use the `cf disable-service-access` command to disable user access to service plans. The command denies access at the org level or across all orgs.

### Disable Access to All Plans for All Users

Running `cf disable-service-access SERVICE-NAME` without any flags disables all user access to all plans carried by the service. For example, the following command denies any user access to all `p-mysql` service plans:

```
$ cf disable-service-access p-mysql
Disabling access to all plans of service p-mysql for all orgs as admin...
OK

$ cf service-access
getting service access as admin...
broker: p-mysql
service plan access orgs
p-mysql 100mb-dev none
```

### Disable Access for Specific Orgs or Plans

The `-p` and `-o` flags to `cf disable-service-access` let the admin deny access to specific service plans or orgs as follows:

- `-p PLAN` disables user access to one service plan
- `-o ORG` disables access to all plans for users in a specified org
- `-p PLAN -o ORG` prevents users in one org from accessing one plan

Run `cf help disable-service-access` to review these options from the command line.

## Limitations

- You cannot disable access to a service plan for an org if the plan is currently available to all orgs. You must first disable access for all orgs; then you can enable access for a particular org.

## Dashboard Single Sign-On

Page last updated:

### Introduction

Single Sign-On (SSO) enables Pivotal Cloud Foundry (PCF) users to authenticate with third-party service dashboards using their PCF credentials. Service dashboards are web interfaces which enable users to interact with some or all of the features the service offers. SSO provides a streamlined experience for users, limiting repeated logins and multiple accounts across their managed services. The user's credentials are never directly transmitted to the service since the OAuth protocol handles authentication.

### Service Broker Responsibilities

#### Registering the Dashboard Client

1. A service broker must include the `dashboard_client` field in the JSON response from its [catalog endpoint](#) for each service implementing this feature. A valid response would appear as follows:

```
{
 "services": [
 {
 "id": "44b26033-1f54-4087-b7bc-da9652c2a539",
 "dashboard_client": {
 "id": "p-mysql-client",
 "secret": "p-mysql-secret",
 "redirect_uri": "http://p-mysql.example.com"
 }
 }
]
}
```

The `dashboard_client` field is a hash containing three fields:

- `id` is the unique identifier for the OAuth client that will be created for your service dashboard on the token server (UAA), and will be used by your dashboard to authenticate with the token server (UAA). If the client id is already taken, PCF will return an error when registering or updating the broker.
- `secret` is the shared secret your dashboard will use to authenticate with the token server (UAA).
- `redirect_uri` is used by the token server as an additional security precaution. UAA will not provide a token if the callback URL declared by the service dashboard doesn't match the domain name in `redirect_uri`. The token server matches on the domain name, so any paths will also match; e.g. a service dashboard requesting a token and declaring a callback URL of `http://p-mysql.example.com/manage/auth` would be approved if `redirect_uri` for its client is `http://p-mysql.example.com/`.

2. When a service broker which advertises the `dashboard_client` property for any of its services is [added or updated](#), Cloud Controller will create or update UAA clients as necessary. This client will be used by the service dashboard to authenticate users.

#### Dashboard URL

A service broker should return a URL for the `dashboard_url` field in response to a [provision request](#). Cloud Controller clients should expose this URL to users. `dashboard_url` can be found in the response from Cloud Controller to create a service instance, enumerate service instances, space summary, and other endpoints.

Users can then navigate to the service dashboard at the URL provided by `dashboard_url`, initiating the OAuth login flow.


### Service Dashboard Responsibilities



## OAuth Flow

When a user navigates to the URL from `dashboard_uri`, the service dashboard should initiate the OAuth login flow. A summary of the flow can be found in [section 1.2 of the OAuth RFC](#). OAuth expects the presence of an [Authorization Endpoint](#) and a [Token Endpoint](#). In PCF, these endpoints are provided by the UAA. Clients can discover the location of UAA from Cloud Controller's info endpoint; in the response the location can be found in the `token_endpoint` field.

```
$ curl api.example.com/info
{"name":"vcap","build":"2222","support":"http://support.example.com","version":
"2","description":"Cloud Foundry sponsored by Example Company","authorization_endpoint":
"https://login.example.com","token_endpoint":"https://uaa.example.com",
"allow_debug":true}
```

 To enable service dashboards to support SSO for service instances created from different PCF instances, the `/v2/info` url is sent to service brokers in the `X-Api-Info-Location` header of every API call. A service dashboard should be able to discover this URL from the broker, and enabling the dashboard to contact the appropriate UAA for a particular service instance.

A service dashboard should implement the OAuth Authorization Code Grant type ([UAA documentation](#), [RFC documentation](#)).

1. When a user visits the service dashboard at the value of `dashboard_uri`, the dashboard should redirect the user's browser to the Authorization Endpoint and include its `client_id`, a `redirect_uri` (callback URL with domain matching the value of `dashboard_client.redirect_uri`), and list of requested scopes.  
Scopes are permissions included in the token a dashboard client will receive from UAA, and which Cloud Controller uses to enforce access. A client should request the minimum scopes it requires. The minimum scopes required for this workflow are `cloud_controller_service_permissions.read` and `openid`. For an explanation of the scopes available to dashboard clients, see [On Scopes](#).
2. UAA authenticates the user by redirecting the user to the Login Server, where the user then approves or denies the scopes requested by the service dashboard. The user is presented with human readable descriptions for permissions representing each scope. After authentication, the user's browser is redirected back to the Authorization endpoint on UAA with an authentication cookie for the UAA.
3. Assuming the user grants access, UAA redirects the user's browser back to the value of `redirect_uri` the dashboard provided in its request to the Authorization Endpoint. The `Location` header in the response includes an authorization code.

```
HTTP/1.1 302 Found
Location: https://p-mysql.example.com/manage/auth?code=F45jH
```

4. The dashboard UI should then request an access token from the Token Endpoint by including the authorization code received in the previous step. When making the request the dashboard must authenticate with UAA by passing the client `id` and `secret` in a basic auth header. UAA will verify that the client id matches the client it issued the code to. The dashboard should also include the `redirect_uri` used to obtain the authorization code for verification.
5. UAA authenticates the dashboard client, validates the authorization code, and ensures that the redirect URI received matches the URI used to redirect the client when the authorization code was issued. If valid, UAA responds back with an access token and a refresh token.

## Checking User Permissions

UAA is responsible for authenticating a user and providing the service with an access token with the requested permissions. However, after the user has been logged in, it is the responsibility of the service dashboard to verify that the user making the request to manage an instance currently has access to that service instance.

The service can accomplish this with a GET to the `/v2/service_instances/:guid/permissions` endpoint on the Cloud Controller. The request must include a token for an authenticated user and the service instance guid. The token is the same one obtained from the UAA in response to a request to the Token Endpoint, described above.

Example Request:

```
curl -H 'Content-Type: application/json' \
-H 'Authorization: bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2V5X2lkIjoid' \
http://api.cloudfoundry.com/v2/service_instances/44b26033-1f54-4087-b7bc-da9652c2a539/permissions
```

Response:

```
{
 "manage": true,
 "read": true
}
```

The response includes the following fields which indicate the various user permissions for the given service instance: - `manage` - a `true` value indicates that the user has sufficient permissions to make changes to and update the service instance; `false` indicates insufficient permissions. - `read` - a `true` value indicates that the user has permission to access read-only diagnostic and monitoring information for the given service instance (e.g. permission to view a read-only dashboard); `false` indicates insufficient permissions.

Since administrators may change the permissions of users at any time, the service should check this endpoint whenever a user uses the SSO flow to access the service's UI.

## On Scopes

Scopes let you specify exactly what type of access you need. Scopes limit access for OAuth tokens. They do not grant any additional permission beyond that which the user already has.

### Minimum Scopes

The following two scopes are necessary to implement the integration. Most dashboard shouldn't need more permissions than these scopes enabled.

| Scope                                                  | Permissions                                                                                          |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <code>openid</code>                                    | Allows access to basic data about the user, such as email addresses                                  |
| <code>cloud_controller_service_permissions.read</code> | Allows access to the CC endpoint that specifies whether the user can manage a given service instance |

### Additional Scopes

Dashboards with extended capabilities may need to request these additional scopes:

| Scope                               | Permissions                                                                             |
|-------------------------------------|-----------------------------------------------------------------------------------------|
| <code>cloud_controller.read</code>  | Allows read access to all resources the user is authorized to read                      |
| <code>cloud_controller.write</code> | Allows write access to all resources the user is authorized to update / create / delete |

## Reference Implementation

The [MySQL Service Broker](#) is an example of a broker that also implements a SSO dashboard. The login flow is implemented using the [OmniAuth library](#) and a custom [UAA OmniAuth Strategy](#). See this [OmniAuth wiki page](#) for instructions on how to create your own strategy.




The UAA OmniAuth strategy is used to first get an authorization code, as documented in [this section](#) of the UAA documentation. The user is redirected back to the service (as specified by the `callback_path` option or the default `auth/cloudfoundry/callback` path) with the authorization code. Before the application / action is dispatched, the OmniAuth strategy uses the authorization code to [get a token](#) and uses the token to request information from UAA to fill the `omniauth.auth` environment variable. When OmniAuth returns control to the application, the `omniauth.auth` environment variable hash will be filled with the token and user information obtained from UAA as seen in the [Auth Controller](#).

## Restrictions

- UAA clients are scoped to services. There must be a `dashboard_client` entry for each service that uses SSO integration.
- Each `dashboard_client_id` must be unique across the CloudFoundry deployment.

## Resources

- [OAuth](#)

- [Example broker with SSO implementation](#) 
- [Cloud Controller API Docs](#) 
- [User Account and Authentication \(UAA\) Service APIs](#) 

## Example Service Brokers

Page last updated:

The following example service broker applications have been developed - these are a great starting point if you are developing your own service broker.

### Ruby

- [GitHub Repository service](#) - this is designed to be an easy-to-read example of a service broker, with complete documentation, and comes with a demo app that uses the service. The broker can be deployed as an application to any Cloud Foundry instance or hosted elsewhere. The service broker uses GitHub as the service back end.
- [MySQL database service](#) - this broker and its accompanying MySQL server are designed to be deployed together as a [BOSH](#) release. BOSH is used to deploy or upgrade the release, monitors the health of running components, and restarts or recreates unhealthy VMs. The broker code alone can be found [here](#).

### Java

- [Spring Cloud - Cloud Foundry Service Broker](#) - This implements the REST contract for service brokers and the artifacts are published to the Spring Maven repository. This greatly simplifies development: include a single dependency in Gradle, implement interfaces, and configure. A sample implementation has been provided for [MongoDB](#).
- [MySQL Java Broker](#) - a Java port of the Ruby-based [MySQL broker](#) above.

### Go


- [Asynchronous Service Broker for AWS EC2](#) - This broker implements support for [Asynchronous Service Operations](#), and calls AWS APIs to provision EC2 VMs.

## Binding Credentials

Page last updated:


A bindable service returns credentials that an application can consume in response to the `cf:bind` API call. Cloud Foundry writes these credentials to the `VCAP_SERVICES` environment variable. In some cases, buildpacks write a subset of these credentials to other environment variables that frameworks might need.

Choose from the following list of credential fields if possible, though you can provide additional fields as needed. Refer to the [Using Bound Services](#) section of the *Managing Service Instances with the CL* topic for information about how these credentials are consumed.

 **Note:** If you provide a service that supports a connection string, provide the `uri` key for buildpacks and application libraries to use.

| CREDENTIALS | DESCRIPTION                                                                                                                                                                             |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| uri         | Connection string of the form <code>DB-TYPE://USERNAME:PASSWORD@HOSTNAME:PORT/NAME</code> , where <code>DB-TYPE</code> is a type of database such as mysql, postgres, mongodb, or amqp. |
| hostname    | FQDN of the server host                                                                                                                                                                 |
| port        | Port of the server host                                                                                                                                                                 |
| name        | Name of the service instance                                                                                                                                                            |
| vhost       | Name of the messaging server virtual host - a replacement for a <code>name</code> specific to AMQP providers                                                                            |
| username    | Server user                                                                                                                                                                             |
| password    | Server password                                                                                                                                                                         |

The following is an example output of `ENV["VCAP_SERVICES"]`.

 **Note:** Depending on the types of databases you are using, each database might return different credentials.

```
VCAP_SERVICES=
{
 cleardb: [
 {
 name: "cleardb-1",
 label: "cleardb",
 plan: "spark",
 credentials: {
 name: "ad_c6f4446532610ab",
 hostname: "us-cdbr-east-03.cleardb.com",
 port: "3306",
 username: "b5d435f40dd2b2",
 password: "ebfc00ac",
 uri: "mysql://b5d435f40dd2b2:ebfc00ac@us-cdbr-east-03.cleardb.com:3306/ad_c6f4446532610ab",
 jdbcUrl: "jdbc:mysql://b5d435f40dd2b2:ebfc00ac@us-cdbr-east-03.cleardb.com:3306/ad_c6f4446532610ab"
 }
 }
],
 cloudamqp: [
 {
 name: "cloudamqp-6",
 label: "cloudamqp",
 plan: "lemur",
 credentials: {
 uri: "amqp://ksvyjmiv:IwN6dCdZmeQD400ZPKpulY0aLx1he8wo@lemur.cloudamqp.com/ksvyjmiv"
 }
 },
 {
 name: "cloudamqp-9dbc6",
 label: "cloudamqp",
 plan: "lemur",
 credentials: {
 uri: "amqp://vhuklnxa:9lNFxpTuJsAdTts98vQIdKHW3MoJyMyV@lemur.cloudamqp.com/vhuklnxa"
 }
 }
],
 rediscloud: [
 {
 name: "rediscloud-1",
 label: "rediscloud",
 plan: "20mb",
 credentials: {
 port: "6379",
```

```
 host: "pub-redis-6379.us-east-1-2.3.ec2.redislabs.com",
 password: "1M5zd3QfWi9nUyya"
 }
},
1,
}
```

## Enabling Service Instance Sharing

Page last updated:

This topic provides information about enabling service instance sharing in managed services.

### Overview

Service authors can allow instances of their services to be shared across spaces and orgs within Cloud Foundry. This enables apps running in different spaces and orgs to use the same service instance. Developers with Space Developer permissions in the space where the service instance was created are responsible for sharing, unsharing, updating, and deleting the service instance.

For more information about the developer and administrator tasks related to service instance sharing, see [Sharing Service Instances \(Beta\)](#).

## Enabling Service Instance Sharing

Service brokers must explicitly enable service instance sharing by setting a flag in their service-level metadata object. This allows service instances, of any service plan, to be shared across orgs and spaces. The `"shareable"` flag must be set to `true` in the service-level metadata to enable service instance sharing. If the flag is set to `false` or is absent, sharing is disabled.

An example catalog is shown below:

```
{
 "services": [{
 "id": "766fa866-a950-4b12-adff-c11fa4cf8fdc",
 "name": "example-service",
 "metadata": {
 "shareable": true
 }
 }]
}
```

## Binding Permissions Based on Instance Sharing

When a service instance is created in one space and shared into another, developers can bind their apps to the service instance from both spaces.

You may want to have the service broker return credentials with different permissions depending on which space an app is bound from. For example, a messaging service may permit writes from the originating space and only reads from any spaces that the service is shared into.

To determine whether the space of the app is the same as the originating space of the service instance, the service broker can compare the `context.space_guid` and `bind_resource.space_guid` fields in the binding request. The `context.space_guid` field represents the space where the service instance was created, and `bind_resource.space_guid` represents the space of the app involved in the binding.

## Security Considerations

Service authors must consider the following before enabling service instance sharing:

- [Service keys](#) can only be generated by users who have access to the space where the service instance was created. This ensures that only developers with access to this space have visibility into where and how many times the service instance is used.
- Consider the impact of giving out excessive permissions for service bindings, especially bindings that originate from spaces that the service instance has been shared into. For example, a messaging service may permit writes from the originating space and only reads from any shared spaces. For more information, see [Binding Permissions Based on Instance Sharing](#).
- You should generate unique credentials for each binding. This ensures that developers can unshare a service instance at any time. Unsharing an instance deletes any service bindings and revokes access for those credentials. Unsharing an instance prevents unauthorized future access from developers and apps that saved the credentials they were previously provided using the service binding.
- Consider the impact of a service instance dashboard being accessed by users of shared service instances. If authenticating through SSO, see [Dashboard Single Sign-On](#).





## Application Log Streaming

Page last updated:

By binding an application to an instance of an applicable service, Cloud Foundry will stream logs for the bound application to the service instance.

- Logs for all apps bound to a log-consuming service instance will be streamed to that instance
- Logs for an app bound to multiple log-consuming service instances will be streamed to all instances

To enable this functionality, a service broker must implement the following:

1. In the [catalog](#) endpoint, the broker must include `requires: syslog_drain`. This minor security measure validates that a service returning a `syslog_drain_url` in response to the [bind](#) operation has also declared that it expects log streaming. If the broker does not include `requires: syslog_drain`, and the bind request returns a value for `syslog_drain_url`, Cloud Foundry will return an error for the bind operation.
2. In response to a [bind](#) request, the broker should return a value for `syslog_drain_url`. The syslog URL has a scheme of syslog, syslog-tls, or https and can include a port number. For example:  
`"syslog_drain_url": "syslog://logs.example.com:1234"`

## How does it work?

1. Service broker returns a value for `syslog_drain_url` in response to bind
2. Loggregator periodically polls an internal Cloud Controller endpoint for updates
3. Upon discovering a new `syslog_drain_url`, Loggregator identifies the associated app
4. Loggregator streams app logs for that app to the locations specified by the service instances' `syslog_drain_urls`

Users can manually configure app logs to be streamed to a location of their choice using User-provided Service Instances. For details, see [Using Third-Party Log Management Services](#).

## Route Services

This documentation is intended for service authors who are interested in offering a service to a Cloud Foundry (CF) services marketplace. Developers interested in consuming these services can read the [Manage Application Requests with Route Services](#) topic.

## Introduction

Cloud Foundry application developers may wish to apply transformation or processing to requests before they reach an application. Common examples of use cases include authentication, rate limiting, and caching services. Route Services are a kind of Marketplace Service that developers can use to apply various transformations to application requests by binding an application's route to a service instance. Through integrations with service brokers and, optionally, with the Cloud Foundry routing tier, providers can offer these services to developers with a familiar, automated, self-service, and on-demand user experience.

**Note:** The procedures in this topic use the Cloud Foundry Command Line Interface (cf CLI). You can also manage route services using Apps Manager. For more information, see the [Manage Route Services](#) section of the *Managing Apps and Service Instances Using Apps Manager* topic.

## Architecture

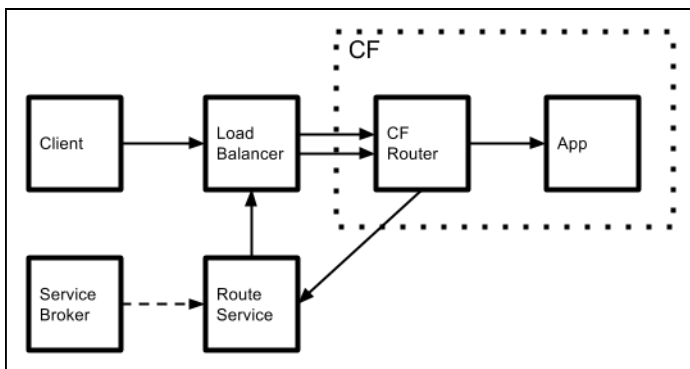
Cloud Foundry supports the following three models for Route Services:

- [Fully-brokered services](#)
- [Static, brokered services](#)
- [User-provided services](#)

In each model, you configure a route service to process traffic addressed to an app.

### Fully-Brokered Service

In the fully-Brokered Service model, the CF router receives all traffic to apps in the deployment before any processing by the route service. Developers can bind a route service to any app, and if an app is bound to a route service, the CF router sends its traffic to the service. After the route service processes requests, it sends them back to the load balancer in front of the CF router. The second time through, the CF router recognizes that the route service has already handled them, and forwards them directly to app instances.



The route service can run inside or outside of CF, so long as it fulfills the [Service Instance Responsibilities](#) to integrate it with the CF router. A service broker publishes the route service to the CF marketplace, making it available to developers. Developers can then create an instance of the service and bind it to their apps with the following commands:

```
cf create-service BROKER-SERVICE-PLAN SERVICE-INSTANCE
```

```
cf bind-route-service YOUR-APP-DOMAIN SERVICE-INSTANCE [--hostname HOSTNAME] [--path PATH]
```

Developers configure the service either through the service provider's web interface or by passing [arbitrary parameters](#) to their `cf create-service` call through the `-c` flag.

**Advantages:**

- Developers can use a Service Broker to dynamically configure how the route service processes traffic to specific applications.
- Adding route services requires no manual infrastructure configuration.
- Traffic to apps that do not use the service makes fewer network hops because requests for those apps do not pass through the route service.

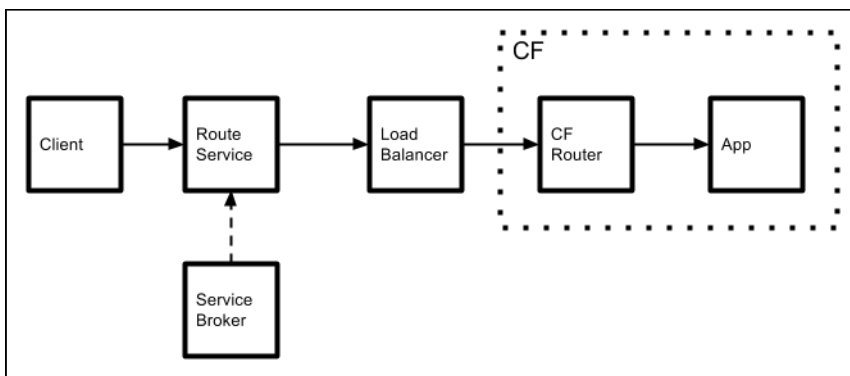
#### Disadvantages:

- Traffic to apps that use the route service makes additional network hops, as compared to the static model.

## Static, Brokered Service

In the static, brokered service model, an operator installs a static routing service, which might be a piece of hardware, in front of the load balancer. The routing service runs outside of Cloud Foundry and receives traffic to all apps running in the CF deployment. The service provider creates a service broker to publish the service to the CF marketplace. As with a [fully-brokered service](#), a developer can use the service by instantiating it with `cf create-service` and

binding it to an app with `cf bind-route-service`.



In this model, you configure route services on an app-by-app basis. When you bind a service to an app, the service broker directs the routing service to process that app's traffic rather than pass the requests through unchanged.

#### Advantages:

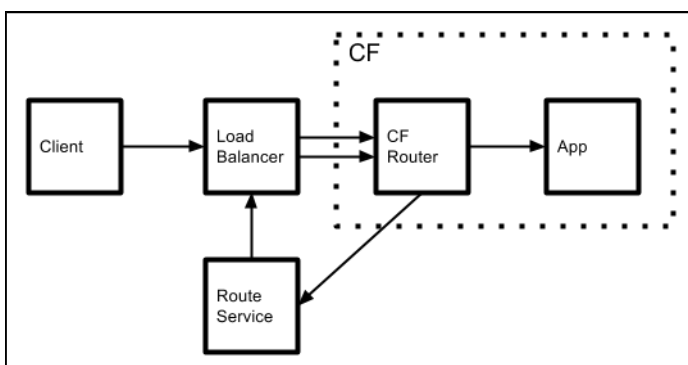
- Developers can use a Service Broker to dynamically configure how the route service processes traffic to specific applications.
- Traffic to apps that use the route service takes fewer network hops.

#### Disadvantages:

- Adding route services requires manual infrastructure configuration.
- Traffic to apps that do not use the route service make unnecessary network hops. Requests for all apps hosted by the deployment pass through the route service component.

## User-Provided Service

If a route service is not listed in the CF marketplace by a broker, a developer can still bind it to their app as a user-provided service. The service can run anywhere, either inside or outside of CF, but it must fulfill the integration requirements described in [Service Instance Responsibilities](#). The service also needs to be reachable by an outbound connection from the CF router.



This model is identical to the [fully-brokered service](#) model, except without the broker. Developers configure the service manually, outside of Cloud Foundry. They can then create a user-provided service instance and bind it to their application with the following commands, supplying the URL of their route service:

```
cf create-user-provided-service SERVICE-INSTANCE -r ROUTE-SERVICE-URL
```

```
cf bind-route-service DOMAIN SERVICE-INSTANCE [--hostname HOSTNAME]
```

### Advantages:

- Adding route services requires no manual infrastructure configuration.
- Traffic to apps that do not use the service makes fewer network hops because requests for those apps do not pass through the route service.

### Disadvantages:

- Developers must manually provision and configure route services out of the context of Cloud Foundry because no service broker automates these operations.
- Traffic to apps that use the route service makes additional network hops, as compared to the static model.

## Architecture Comparison

The models above require the [broker](#) and [service instance](#) responsibilities summarized in the following table:

| Route Services Architecture | Fulfills CF <a href="#">Service Instance Responsibilities</a> | Fulfills CF <a href="#">Broker Responsibilities</a> |
|-----------------------------|---------------------------------------------------------------|-----------------------------------------------------|
| Fully-Brokered              | Yes                                                           | Yes                                                 |
| Static Brokered             | No                                                            | Yes                                                 |
| User-Provided               | Yes                                                           | No                                                  |

## Enabling Route Services in Pivotal Cloud Foundry

You configure Route Services for your deployment in the PAS tile, under **Settings > Networking**. Depending on your infrastructure, refer to the PAS configuration topics for [AWS](#), [OpenStack](#), or [vSphere](#).

## Service Instance Responsibilities

The following applies only when a broker returns `route_service_url` in the bind response.

### How It Works

Binding a service instance to a route associates the `route_service_url` with the route in the CF router. All requests for the route are proxied to the URL specified by `route_service_url`.

Once a route service completes its function it may choose to forward the request to the originally requested URL or to another location, or it may choose to reject the request; rejected requests will be returned to the originating requestor. The CF router includes a header that provides the originally requested URL, as well as two headers that are used by the router itself to validate the request sent by the route service. These headers are described below in [Headers](#).

### Headers

The following HTTP headers are added by the Gorouter to requests forwarded to route services.

#### X-CF-Forwarded-Url

The `X-CF-Forwarded-Url` header contains the originally requested URL. The route service may choose to forward the request to this URL or to another.

## X-CF-Proxy-Signature

The `X-CF-Proxy-Signature` header contains an encrypted value which only the Gorouter can decrypt.

The header contains the originally requested URL and a timestamp. When this header is present, the Gorouter will reject the request if the requested URL does not match that in the header, or if a timeout has expired.

`X-CF-Proxy-Signature` also signals to the Gorouter that a request has transited a route service. If this header is present, the Gorouter will not forward the request to a route service, preventing recursive loops. For this reason, route services should not strip off the `X-CF-Proxy-Signature` and `X-CF-Proxy-Metadata` headers.

If the route service forwards the request to a URL different from the originally requested one, and the URL resolves to a route for an application on Cloud Foundry, the route must not have a bound route service or the request will be rejected, as the requested URL will not match the one in the `X-CF-Proxy-Signature` header.

## X-CF-Proxy-Metadata

The `X-CF-Proxy-Metadata` header aids in the encryption and description of `X-CF-Proxy-Signature`.

## SSL Certificates

When Cloud Foundry is deployed in a development environment, certificates hosted by the load balancer are self-signed, and not signed by a trusted certificate authority. When the route service finishes processing an inbound request and makes a call to the value of `X-CF-Forwarded-Url`, be prepared to accept the self-signed certificate when integrating with a non-production deployment of Cloud Foundry.

## Timeouts

Route services must forward the request to the application route within 60 seconds.

In addition, all requests must respond in 900 seconds.

# Broker Responsibilities

## Catalog Endpoint

Brokers must include `requires: ["route_forwarding"]` for a service in the catalog endpoint. If this is not present, Cloud Foundry will not permit users to bind an instance of the service to a route.

## Binding Endpoint

When users bind a route to a service instance, Cloud Foundry sends a [bind request](#) to the broker, including the route address with `bind_resource.route`. A route is an address used by clients to reach apps mapped to the route. The broker may return `route_service_url`, containing a URL where Cloud Foundry should proxy requests for the route. This URL must have an `https` scheme, otherwise the Cloud Controller rejects the binding. `route_service_url` is optional, and not returning this field enables a broker to dynamically configure a network component already in the request path for the route, requiring no change in the CF router.

# Example Route Services

- [Logging Route Service](#): This route service can be pushed as an app to Cloud Foundry. It fulfills the service instance responsibilities above and logs requests received and sent. It can be used to see the route service integration in action by tailing its logs.
- [Rate Limiting Route Service](#): This example route service is a simple Cloud Foundry app that provides rate limiting to control the rate of traffic to an application.
- [Spring Boot Example](#): Logs requests received and sent; written in Spring Boot

## Tutorial

The following instructions show how to use the [Logging Route Service](#) described in [Example Route Services](#) to verify that when a route service is bound to a route, requests for that route are proxied to the route service.

A video of this tutorial is available on [Youtube](#).

These commands requires the Cloud Foundry Command Line Interface (cf CLI) version 6.16 or later.

1. Push the [Logging Route Service](#) as an app.

```
$ cf push logger
```

2. Create a user-provided service instance, and include the route of the [Logging Route Service](#) you pushed as `route_service_url`. Be sure to use `https` for the scheme.

```
$ cf create-user-provided-service mylogger -r https://logger.cf.example.com
```

3. Push a sample app like [Spring Music](#). By default this creates a route `spring-music.cf.example.com`.

```
$ cf push spring-music
```

4. Bind the user-provided service instance to the route of your sample app. The `bind-route-service` command takes a route and a service instance; the route is specified in the following example by domain `cf.example.com` and hostname `spring-music`.

```
$ cf bind-route-service cf.example.com mylogger --hostname spring-music
```

5. Tail the logs for your route service.

```
$ cf logs logger
```

6. Send a request to the sample app and view in the route service logs that the request is forwarded to it.

```
$ curl spring-music.cf.example.com
```

## Supporting Multiple Cloud Foundry Instances

Page last updated:

It is possible to register a service broker with multiple Cloud Foundry instances. It may be necessary for the broker to know which Cloud Foundry instance is making a given request. For example, when using [Dashboard Single Sign-On](#), the broker is expected to interact with the authorization and token endpoints for a given Cloud Foundry instance.

There are two strategies that can be used to discover which Cloud Foundry instance is making a given request.

### Routing & Authentication

The broker can use unique credentials and/or a unique url for each Cloud Foundry instance. When registering the broker, different Cloud Foundry instances can be configured to use different base urls that include a unique id. For example:

- On Cloud Foundry instance 1, the service broker is registered with the url `broker.example.com/123`
- On Cloud Foundry instance 2, the service broker is registered with the url `broker.example.com/456`

### X-API-Info-Location Header

All calls to the broker from Cloud Foundry include an `X-API-Info-Location` header containing the `/v2/info` url for that instance. The `/v2/info` endpoint will return further information, including the location of that Cloud Foundry instance's UAA.

Support for this header was introduced in cf-release v212.

## Logging and Metrics

This documentation describes logging and metrics in Cloud Foundry (CF). It includes topics related to monitoring, event logging, CF data sources, and viewing logs and metrics. It also includes information about the Loggregator system, which aggregates and streams logs and metrics from apps and platform components in Pivotal Application Service.

## Contents

### Logging and Metrics

- [Overview of Logging and Metrics](#): This topic provides an overview of logging and metrics in CF.
- [Application Logging in Cloud Foundry](#): This topic describes log types and their messages. It also explains how to view logs from the cf CLI.
- [Customizing Platform Log Forwarding](#): This topic describes how to modify log forwarding rules.

### Loggregator

- [Loggregator Architecture](#): This topic describes the architecture of the Loggregator system.
- [Loggregator Guide for Cloud Foundry Operators](#): The topic provides information about configuring Loggregator to avoid data loss with high volumes of logging and metrics data.
- [Deploying a Nozzle to the Loggregator Firehose](#): This topic describes deploying a nozzle application to the Loggregator Firehose.
- [Installing the Loggregator Firehose Plugin for cf CLI](#): This topic describes how to use the Loggregator Firehose Plugin for cf CLI to access the output of the Firehose.

## See Also

For more information about logging, monitoring, and reporting, see the topics below.

- [Configuring Logging in PAS](#) [↗](#): This topic describes how to forward system logs to an external service, scale Loggregator component VMs, and manage app traffic logging.
- [Security Event Logging](#): This topic describes how to enable and interpret security event logging for the Cloud Controller, the User Account and Authentication (UAA) server, and CredHub.
- [Monitoring Pivotal Cloud Foundry](#) [↗](#): This topic describes how operators can monitor their deployments. It includes information about selecting and configuring a monitoring system.
- [Reporting Instance Usage with Apps Manager](#) [↗](#): This topic describes how to retrieve app, task, and service instance usage information.
- [Reporting App, Task, and Service Instance Usage](#) [↗](#): This topic describes how to use the cf CLI to retrieve system and org level usage information about apps, tasks, and service instances.
- [Monitoring PCF VMs from Ops Manager](#) [↗](#): This topic describes how to check current VM status.



## Overview of Logging and Metrics

Page last updated:

This topic provides an overview of logging and metrics in Cloud Foundry (CF). It includes information about logs and metrics sources and transport systems. It also lists products for viewing logs and metrics.

## Sources of Logs and Metrics

There are two sources of CF logs and metrics:

- CF platform components, such as a Diego Cell, MySQL Server, or Cloud Controller
- Apps and app containers deployed on CF

The table below describes the data included in logs and metrics from each source.

| Source              | Logs Data               | Metrics Data                                                                                                                                                                                                                                                                                                                  |
|---------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Platform components | Logs from CF components | <ul style="list-style-type: none"> <li>• Health metrics from BOSH-deployed VMs*</li> <li>• Platform metrics from CF components. For example, cell capacity remaining and router throughput.</li> <li>• Metrics for any service tile that self-publishes to the Loggregator Firehose. For example, Redis and MySQL.</li> </ul> |
| Apps                | Logs from apps **       | <ul style="list-style-type: none"> <li>• App container metrics. For example, CPU, memory, and disk usage.</li> <li>• Custom metrics ***</li> </ul>                                                                                                                                                                            |

\* For more information about using the BOSH Health Monitor to collect health metrics on VMs, see [Configuring a Monitoring System](#).

\*\* For more information about app logging, see [Application Logging in Cloud Foundry](#).

\*\*\* For more information about configuring an application to stream custom metrics to Loggregator, see [Metrics Forwarder for PCF](#).

## Transport Systems for Logs and Metrics

The following transport systems deliver logs and metrics from their source to an observability product for viewing:

- **Loggregator:** Loggregator is the transport system for both logs and metrics on apps deployed on CF as well as metrics on CF platform components. For more information about the Loggregator system, including Loggregator architecture and components, see [Overview of the Loggregator System](#).
- **rsyslogd on CF component VMs:** rsyslogd is the transport system for CF component logs. Users can configure rsyslogd to transport component logs to a third-party syslog server.

The table below lists the transport system for logs and metrics on CF platform components and apps.

| Source              | Logs Transport System        | Metrics Transport System |
|---------------------|------------------------------|--------------------------|
| Platform components | rsyslogd on CF component VMs | Loggregator              |
| Apps                | Loggregator                  | Loggregator              |

## Viewing Logs and Metrics

The table below lists the products and tools for viewing CF logs and metrics.

| Source | Products and Tools for Viewing Logs                                                                    | Products and Tools for Viewing Metrics                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | To view system logs from CF components, configure rsyslogd to transport logs to a third-party product. | <p>You can use the following products or tools to view platform component and VM metrics:</p> <ul style="list-style-type: none"> <li>• Loggregator Firehose CLI Plugin. See <a href="#">Installing the</a></li> </ul> |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Platform components |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="#">Loggregator Firehose Plugin for CLI</a> . <ul style="list-style-type: none"> <li>Loggregator Log Cache CLI Plugin. See <a href="#">Cloud Foundry Community cf CLI Plugins</a>.</li> <li>PCF Healthwatch. See <a href="#">PCF Healthwatch</a>.</li> </ul>                                                                                                                             |
| Apps                | <p>You can use the following products or tools to view app logs:</p> <ul style="list-style-type: none"> <li>cf CLI cf logs command. See <a href="#">Cloud Foundry CLI Reference Guide</a>.</li> <li>Apps Manager. See <a href="#">Managing Apps and Service Instances Using Apps Manager</a>.</li> <li>Syslog forwarding. See <a href="#">Streaming Application Logs to Log Management Services</a>.</li> <li>Loggregator Firehose CLI Plugin. See <a href="#">Installing the Loggregator Firehose Plugin for CLI</a>.</li> <li>Loggregator Log Cache CLI Plugin. See <a href="#">Cloud Foundry Community cf CLI Plugins</a>.</li> </ul> | <p>You can use the following products or tools to view app metrics:</p> <ul style="list-style-type: none"> <li>Loggregator Firehose CLI Plugin. See <a href="#">Installing the Loggregator Firehose Plugin for CLI</a>.</li> <li>Loggregator Log Cache CLI Plugin. See <a href="#">Cloud Foundry Community cf CLI Plugins</a>.</li> <li>PCF Metrics. See <a href="#">PCF Metrics</a>.</li> </ul> |

## Loggregator Architecture

Page last updated:

This topic describes the Loggregator architecture and components. It also describes the Pivotal Cloud Foundry (PCF) components that send BOSH-reported VM metrics to Loggregator.

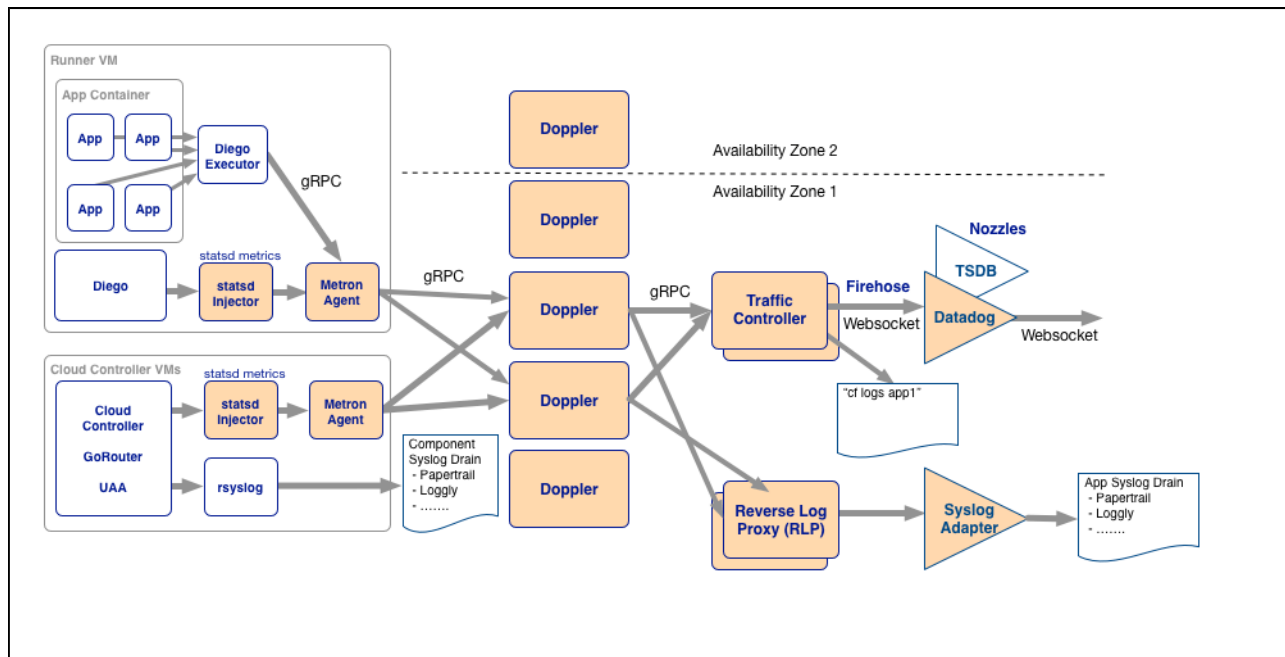
### Overview

Loggregator gathers and streams logs and metrics from user apps in a PCF deployment. It also gathers and streams metrics from PCF components and health metrics from BOSH-deployed VMs. Loggregator allows you to view these logs and metrics through the Loggregator CLI plugins or through a third-party service. For more information, see [loggregator](#) in GitHub.

The Loggregator architecture includes components for collecting, storing, and forwarding logs and metrics.

### Loggregator Architecture and Components

The diagram below shows the architecture of Loggregator, including the PCF components with which it interacts.



[View a larger version of this image.](#)

The following are Loggregator components, as shown in the diagram above:

- **Metron Agent:** Loggregator Agents run on both PCF component VMs and Diego cell VMs. They receive logs and metrics from the apps and PCF components located on those VMs. Loggregator Agents then forward the logs and metrics to Dopplers.
- **Doppler:** Dopplers receive logs and metrics from Loggregator Agents, store them in temporary buffers, and forward them to Traffic Controllers.
- **Traffic Controller:** Traffic Controllers poll Doppler servers for logs and metrics, then translate these messages from the Doppler servers as necessary for external and legacy APIs. The Loggregator Firehose is located on the Traffic Controller.
- **Reverse Log Proxy:** Reverse Log Proxies (RLPs) collect logs and metrics from Dopplers and forward them to Syslog Adapters for syslog drains. Operators can scale up the number of RLPs based on overall log volume.
- **Syslog Adapter:** Syslog Adapters manage connections with and write to syslog drains. Operators can scale the Syslog Adapter component based on the number of syslog drains.
- **Firehose:** The Firehose is a WebSocket endpoint that streams all the event data from a PCF deployment. The data stream includes HTTP events, app logs, container metrics from apps, and metrics from PCF platform components. The Firehose cf CLI plugin allows you to view the output of the Firehose. For more information about the Firehose plugin, see [Installing the Loggregator Firehose Plugin for cf CLI](#).
- **Log Cache:** The Log Cache allows you to view logs and metrics from the Firehose over a specified period of time. The Log Cache includes API endpoints

and a CLI plugin to query and filter logs and metrics. To download the Log Cache CLI plugin, see [Cloud Foundry Plugins](#). The Log Cache API endpoints are available by default. For more information about using the Log Cache API, see [Log Cache](#) on GitHub.

- **Nozzles:** Nozzles are programs that consume data from the Loggregator Firehose. Nozzles can be configured to select, buffer, and transform data, and to forward it to other apps and services. For more information about creating and deploying nozzles, see [Deploying a Nozzle to the Loggregator Firehose](#).

## Related BOSH Components

This section describes the PCF components that forward BOSH-reported VM metrics to Loggregator. BOSH-reported VM metrics measure the health of BOSH-deployed VMs on which apps and PCF components are deployed. Loggregator streams BOSH-reported VM metrics through the Firehose.

The following are the PCF components that send BOSH-reported VM metrics to Loggregator:

- **BOSH Agent:** BOSH Agents are located on component VMs and Diego cell VMs. They collect metrics, such as cell capacity remaining, from the VM and forward them to the BOSH Health Monitor.
- **BOSH Health Monitor:** The BOSH Health Monitor receives metrics from the BOSH Agents. It then forwards the metrics to a third-party service or to the BOSH System Metrics Forwarder.
- **BOSH System Metrics Plugin:** This plugin reads health events, such as VM heartbeats and alerts from the BOSH Health Monitor, and streams them to the BOSH System Metrics Server.
- **BOSH System Metrics Server:** The BOSH System Metrics Server streams metrics and heartbeat events to the BOSH System Metrics Forwarder over gRPC.
- **BOSH System Metrics Forwarder:** The BOSH System Metrics Forwarder is located on the Loggregator Traffic Controller. It forwards heartbeat events from the BOSH System Metrics Server as envelopes to Loggregator through a Loggregator Agent.

## Loggregator Guide for Cloud Foundry Operators

Page last updated:

This topic contains information for Cloud Foundry deployments operators about how to configure the [Loggregator system](#) to avoid data loss with high volumes of logging and metrics data.

### Loggregator Message Throughput and Reliability

For determining the message throughput and reliability rates of your Loggregator system, see the section below.

#### Measuring Message Throughput

To measure the message throughput of the Loggregator system, you can monitor the total number of egress messages from all Metrons on your platform using the `metron.egress` metric.

If you do not use a monitoring platform, you can follow the instructions below to measure the overall message throughput of your Loggregator system:

1. Log in to the Cloud Foundry Command Line Interface (cf CLI) with your admin credentials:

```
$ cf login
```

2. [Install](#) the Cloud Foundry Firehose plugin.

3. Install Pipe Viewer:

```
$ apt-get install pv
```

4. Run the following command:

```
$ cf nozzle -n | pv -l -i 10 -r > /dev/null
```

#### Measuring Message Reliability

To measure the message reliability rate of your Loggregator system, you can run black-box tests. If you want to use this method, see the open-source [cf-logmon](#) app and the configuration instructions provided in the README.md file.

### Scaling Loggregator

Most Loggregator configurations use preferred resource defaults. For more information about customizing these defaults and planning the capacity of your Loggregator system, see [Key Capacity Scaling Indicators](#).

#### Scaling Nozzles

Nozzles are programs that consume data from the Loggregator Firehose. Nozzles can be configured to select, buffer, and transform data, and to forward it to other apps and services. You can scale a nozzle using the subscription ID specified when the nozzle connects to the Firehose. If you use the same subscription ID on each nozzle instance, the Firehose evenly distributes data across all instances of the nozzle.

For example, if you have two nozzle instances with the same subscription ID, the Firehose sends half of the data to one nozzle instance and half to the other. Similarly, if you have three nozzle instances with the same subscription ID, the Firehose sends one-third of the data to each instance.

If you want to scale a nozzle, the number of nozzle instances should match the number of Traffic Controller instances:

*Number of nozzle instances = Number of Traffic Controller instances*

Stateless nozzles should handle scaling gracefully. If a nozzle buffers or caches the data, the nozzle author must test the results of scaling the number of nozzle instances up or down.

## Slow Nozzle Alerts

The [Traffic Controller](#) alerts nozzles if they consume events too slowly. If a nozzle falls behind, Loggregator alerts the nozzle in two ways:

- **TruncatingBuffer** alerts: If the nozzle consumes messages more slowly than they are produced, the Loggregator system may drop messages. In this case, Loggregator sends the log message, `TB: Output channel too full. Dropped N messages`, where `N` is the number of dropped messages. Loggregator also emits a **CounterEvent** with the name `doppler_proxy.slow_consumer`. The nozzle receives both messages from the Firehose, alerting the operator to the performance issue.

## Forwarding Logs to an External Service

You can configure Pivotal Application Service to forward log data from apps to an external aggregator service. [Using Log Management Services](#) explains how to bind apps to the external service and configure it to receive logs from Pivotal Application Service.

## Log Message Size Constraints

When a Diego Cell emits app logs to Metron, Diego breaks up log messages greater than approximately 60 KiB into multiple envelopes.

## Deploying a Nozzle to the Loggregator Firehose

Page last updated:

This topic describes deploying a nozzle app to the Cloud Foundry (CF) Loggregator Firehose. For more information about nozzles and the Loggregator Firehose, see [Loggregator Architecture](#). The Cloud Foundry Loggregator team created an example nozzle application for use with this tutorial.


The procedure described below deploys this example nozzle to the Firehose of a Cloud Foundry installation deployed locally with BOSH Lite. For more information about BOSH Lite, see the [BOSH Lite GitHub repository](#).

To lighten the load on custom nozzles you develop, you can request Firehose subscriptions that emit only whitelisted metrics. For examples, see `rlpreader` and `rlptypereader` in the [loggregator-tools](#) repository, and see the *V2 Subscriptions* page of the [loggregator-release](#) repository for more information.

## Prerequisites

Before you deploy a nozzle to the Loggregator Firehose, you must have the following:

- BOSH CLI. See [BOSH CLI](#) installed locally.
- Spiff installed locally and added to the load path of your shell. See [Spiff on GitHub](#).
- BOSH Lite deployed locally using VirtualBox. See [BOSH Lite on GitHub](#).
- A working Cloud Foundry deployment, including Loggregator, deployed with your local BOSH Lite. This serves as the source of data. See [Deploying Cloud Foundry using BOSH Lite](#), or use the `provision_cf` script included in the BOSH Lite release. See [BOSH Lite](#) on GitHub.

 **Note:** Deploying Cloud Foundry can take several hours depending on your internet bandwidth, even when using the automated `provision_cf` script.

## Step 1: Download Cloud Foundry BOSH Manifest

To download the BOSH manifest, do the following:

1. Run `bosh -e MY-ENV deployments` to identify the names of all deployments in the environment you specify. Replace `MY-ENV` with the alias you set for your BOSH Director. For example:

```
$ bosh -e dev deployments
Using environment '192.168.15.4' as client 'admin'
```

| Name                                | Release(s)               | Stemcell(s)                                        | Team(s) | Cloud Config |
|-------------------------------------|--------------------------|----------------------------------------------------|---------|--------------|
| cf-example                          | binary-buildpack/1.0.9   | bosh-warden-boshlite-ubuntu-trusty-go_agent/3363.9 | -       | latest       |
|                                     | capi/1.21.0              |                                                    |         |              |
|                                     | cf-mysql/34              |                                                    |         |              |
|                                     | cf-smoke-tests/11        |                                                    |         |              |
|                                     | cflinuxfs2-rootfs/1.52.0 |                                                    |         |              |
|                                     | consul/155               |                                                    |         |              |
|                                     | diego/1.8.1              |                                                    |         |              |
|                                     | etcd/94                  |                                                    |         |              |
|                                     | garden-runc/1.2.0        |                                                    |         |              |
|                                     | loggregator/78           |                                                    |         |              |
|                                     | nats/15                  |                                                    |         |              |
|                                     | routing/0.145.0          |                                                    |         |              |
|                                     | statsd-injector/1.0.20   |                                                    |         |              |
|                                     | uaa/25                   |                                                    |         |              |
| service-instance_0d4140a0-42b7-.... | mysql/0.6.0              | bosh-warden-boshlite-ubuntu-trusty-go_agent/3363.9 | -       | latest       |

```
2 deployments
Succeeded
```

2. Run `bosh -e MY-ENV -d MY-DEPLOYMENT manifest > MY-MANIFEST.yml` to download and save the current BOSH deployment manifest. Replace `MY-ENV` with your BOSH Director alias, `MY-DEPLOYMENT` with the deployment name from the output of the previous step, and `MY-MANIFEST.yml` with a name you choose for the saved manifest file. You need this manifest to locate information about your databases.

```
$ bosh -e dev -d cf-example manifest > cf.yml
```

## Step 2: Add UAA Client

You must authorize the example nozzle as a UAA client for your CF deployment. To do this, add an entry for the example nozzle as `client` for `uaa` under the `properties` key in your CF deployment manifest YAML file. You must enter the example nozzle object in the correct location in the manifest, and with the correct indentation.

To add the nozzle as a UAA client for your deployment, do the following:

1. Open the deployment manifest in a text editor.
2. Locate the left-aligned `properties` key.
3. Under the `properties` key, locate `uaa` at the next level of indentation.
4. Under the `uaa` key, locate the `clients` key at the next level of indentation.
5. Enter properties for the `example-nozzle` at the next level of indentation, exactly as shown below. The `...` in the text below indicate other properties that may populate the manifest at each level in the hierarchy.

```
properties:
...
 uaa:
...
 clients:
...
 example-nozzle:
 access-token-validity: 1209600
 authorized-grant-types: client_credentials
 override: true
 secret: example-nozzle
 authorities: oauth.login,doppler.firehose
```

6. Save the deployment manifest file.

## Step 3: Redeploy Cloud Foundry

To deploy Cloud Foundry with BOSH, run the following command:

```
bosh -e MY-ENV deploy
```

WHERE `MY-ENV` is the alias you set for your BOSH Director.

For example:



```
$ bosh -e dev deploy
Acting as user 'admin' on deployment 'cf-warden' on 'Bosh Lite Director'
Getting deployment properties from director...

Detecting deployment changes

Releases
No changes

Compilation
No changes

Update
No changes

Resource pools
No changes

Disk pools
No changes

Networks
No changes

Jobs
No changes

Properties
uaa
clients
example-nozzle
+ access-token-validity: 1209600
+ authorized-grant-types: authorization_code,client_credentials,refresh_token
+ override: true
+ secret: example-nozzle
+ scope: openid,oauth.approvals,doppler.firehose
+ authorities: oauth.login,doppler.firehose

Meta
No changes

Please review all changes carefully

Deploying

Are you sure you want to deploy? (type 'yes' to continue):yes
```

## Step 4: Clone Example Release

The Cloud Foundry Loggregator team created an example nozzle app for use with this tutorial.

To clone the example nozzle release, do the following:

1. Run `git clone` to clone the main release repository from [GitHub](#).

```
$ git clone https://github.com/cloudfoundry-incubator/example-nozzle-release.git
Cloning into 'example-nozzle-release'...
```

2. Navigate to the `example-nozzle-release` directory.

```
$ cd example-nozzle-release
```

3. Run `git submodule update --init --recursive` to update all of the included submodules.

```
$ git submodule update --init --recursive
Submodule 'src/github.com/cloudfoundry-incubator/example-nozzle' (git@github.com:cloudfoundry-incubator/example-nozzle.git) registered for path 'src/github.com/cloudfoundry-incubator/example-nozzle'
Submodule 'src/github.com/cloudfoundry-incubator/uaago' (git@github.com:cloudfoundry-incubator/uaago.git) registered for path 'src/github.com/cloudfoundry-incubator/uaago'
...
Cloning into 'src/github.com/cloudfoundry-incubator/example-nozzle'...
...
```

## Step 5: Prepare Nozzle Manifest

To prepare the nozzle deployment manifest, do the following:

1. In the `example-nozzle-release` directory, navigate to the `templates` directory.

```
$ cd templates
```

Within this directory, examine the two YAML files. `bosh-lite-stub.yml` contains the values used to populate the missing information in `template.yml`. By combining these two files we create a deployment manifest for our nozzle.

2. Create a `tmp` directory for the compiled manifest.
3. Use [Spiff](#) to compile a deployment manifest from the template and stub, and save this manifest.


```
$ spiff merge templates/template.yml templates/bosh-lite-stub.yml > tmp/manifest_bosh_lite.yml
```

4. Run `bosh -e MY-ENV deployments` to identify the names of all deployments in the environment you specify. Replace `MY-ENV` with the alias you set for your BOSH Director.
5. Run `bosh -e MY-ENV env --column=uuid` to obtain your BOSH Director UUID. Replace `MY-ENV` with the alias you set for your BOSH Director. For example:

```
$ bosh -e dev env --column=uuid
```

6. In the compiled nozzle deployment manifest, locate the `director_uuid` property. Replace `PLACEHOLDER-DIRECTOR-UUID` with your BOSH Director UUID.

```
compilation:
cloud_properties:
 name: default
network: example-nozzle-net
reuse_compilation_vms: true
workers: 1
director_uuid: PLACEHOLDER-DIRECTOR-UUID # replace this
```

 **Note:** If you do not want to see the complete deployment procedure, run the following command to automatically prepare the manifest:

```
scripts/make_manifest_spiff_bosh_lite
```

## Step 6: Create Nozzle BOSH Release

To create a nozzle BOSH release, run the following command:

```
bosh -e MY-ENV create-release --name RELEASE-NAME
```

WHERE:

- `MY-ENV` is the alias you set for your BOSH Director.
- `RELEASE-NAME` is `example-nozzle` to match the UAA client that you created in the CF deployment manifest.

For example:

```
$ bosh -e dev create-release --name example-nozzle
Syncing blobs...
...
```

## Step 7: Upload Nozzle BOSH Release

Upload the nozzle BOSH release that you created as part of [Step 6: Create Nozzle BOSH Release](#).

To upload the BOSH release, run the following command:

```
bosh -e MY-ENV upload-release
```

WHERE `MY-ENV` is the alias you set for your BOSH Director.

For example:

```
$ bosh -e dev upload-release
Acting as user 'admin' on 'Bosh Lite Director'

Copying packages

example-nozzle
golang1.7

Copying jobs

example-nozzle

Generated /var/folders/4n/qs1rjbmd1c5gfb78m3_06j6r0000gn/T/d20151009-71219-17a5m49/d20151009-71219-rts928/release.tgz
Release size: 59.2M

Verifying release...
...
Release info

Name: nozzle-test
Version: 0+dev.2

Packages
- example-nozzle (b0944f95eb5a332e9be2adfb4db1bc88f9755894)
- golang1.7 (b68dc9557ef296cb21e577c31ba97e2584a5154b)

Jobs
- example-nozzle (112e01c6ee91e8b268a42239e58e8e18e0360f58)

License
- none

Uploading release
```

## Step 8: Deploy Nozzle

To deploy the nozzle, run the following command:

```
bosh -e MY-ENV deploy
```

WHERE `MY-ENV` is the alias you set for your BOSH Director.

For example:

```
$ bosh -e dev deploy
Acting as user 'admin' on deployment 'example-nozzle-lite' on 'Bosh Lite Director'
Getting deployment properties from director...
Unable to get properties list from director, trying without it...
Cannot get current deployment information from director, possibly a new deployment
Please review all changes carefully

Deploying

Are you sure you want to deploy? (type 'yes' to continue):yes
```

## Step 9: View Nozzle Output

The example nozzle outputs all of the data originating coming from the Firehose to its log files. To view this data, SSH into the example-nozzle VM and examine the logs.

To view nozzle output, do the following:

1. Run `bosh -e MY-ENV ssh` to access the nozzle VM at the IP configured in the nozzle's manifest template stub `./templates/bosh-lite-stub.yml`. Replace `MY-ENV` with the alias you set for your BOSH Director. For example:

```
$ bosh -e dev ssh example-nozzle
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.19.0-25-generic x86_64)
Documentation: https://help.ubuntu.com/
Last login: Wed Sep 23 21:29:50 2015 from 192.0.2.1
```

2. Use the `cat` command to output the `stdout` log file.

```
$ cat /var/vcap/sys/log/example-nozzle/example-nozzle.stdout.log
===== Streaming Firehose (will only succeed if you have admin credentials)
origin:"DopplerServer" eventType:ValueMetric timestamp:1443046217700750747 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910193187 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910360012 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910252169 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910294255 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910318582 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910339088 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910379199 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046218910394886 deployment:"cf-warden" job:"loggregator_trafficcontroller_z1" index:"0" ip:"203.0.113.146" counterE
origin:"router_0" eventType:HttpStartStop timestamp:1443046219105062148 deployment:"cf-warden" job:"router_z1" index:"0" ip:"203.0.113.22" httpStartStop: peerType:Client metho
origin:"api_z1_0" eventType:HttpStartStop timestamp:1443046219109842455 deployment:"cf-warden" job:"api_z1" index:"0" ip:"203.0.113.134" httpStartStop: peerType:Server method
origin:"router_0" eventType:HttpStartStop timestamp:1443046219110064368 deployment:"cf-warden" job:"router_z1" index:"0" ip:"203.0.113.22" httpStartStop: peerType:Client metho
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177165446 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177288325 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177346726 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177274975 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177310389 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177330214 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177353454 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177360052 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"syslog_drain_binder" eventType:ValueMetric timestamp:1443046219177481456 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" valueMetric:
origin:"DopplerServer" eventType:CounterEvent timestamp:1443046219880895040 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.146" counterEvent:
origin:"DopplerServer" eventType:CounterEvent timestamp:1443046219881017888 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" counterEvent:
origin:"DopplerServer" eventType:CounterEvent timestamp:1443046219880585603 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" counterEvent:
origin:"DopplerServer" eventType:CounterEvent timestamp:1443046219880929574 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" counterEvent:
origin:"DopplerServer" eventType:CounterEvent timestamp:1443046219881004417 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" counterEvent:
origin:"DopplerServer" eventType:CounterEvent timestamp:1443046219880929568 deployment:"cf-warden" job:"doppler_z1" index:"0" ip:"203.0.113.142" counterEvent:
origin:"MetronAgent" eventType:CounterEvent timestamp:1443046220058280679 deployment:"cf-warden" job:"api_z1" index:"0" ip:"203.0.113.134" counterEvent:
```

## Installing the Loggregator Firehose Plugin for cf CLI

Page last updated:

The Loggregator Firehose plugin for the Cloud Foundry Command Line Interface (cf CLI) allows Cloud Foundry (CF) administrators to access the output of the Loggregator Firehose. The output of the Firehose includes logs and metrics from apps deployed on CF as well as metrics from CF platform components. For more information about the Firehose, see [Overview of the Loggregator System](#).

For more information about using plugins with the cf CLI, see [Using cf CLI Plugins](#).

### Prerequisites

- Administrator access to the Cloud Foundry deployment that you want to monitor
- Cloud Foundry Command Line Interface (cf CLI) 6.12.2 or later

Refer to the [Installing the cf CLI](#) topic for information about downloading, installing, and uninstalling the cf CLI.

### Install the Plugin

1. Run `cf add-plugin-repo REPOSITORY-NAME URL` to add the CF Community plugin repository to your cf CLI plugins.

```
$ cf add-plugin-repo CF-Community https://plugins.cloudfoundry.org
```


2. Run `cf install-plugin -r PLUGIN-REPOSITORY PLUGIN-NAME` to install the Firehose plugin from the CF Community plugin repository.

```
$ cf install-plugin -r CF-Community "Firehose Plugin"
```

### View the Firehose

Run `cf nozzle --debug` to view the streaming output of the Firehose, which includes logging events and metrics from CF system components. For more information about logging and metrics in CF, see [Overview of the Loggregator System](#).

```
$ cf nozzle --debug
```

 **Note:** You must be logged in as a Cloud Foundry administrator to access the Firehose.

### Uninstall the Plugin

Run `cf plugins` to see a list of installed plugins.

```
$ cf plugins
Listing Installed Plugins...
OK
Plugin Name Version Command Name Command Help
FirehosePlugin 0.6.0 nozzle Command to print out messages from the firehose
```

Run `cf uninstall-plugin PLUGIN-NAME` to uninstall the plugin.

```
$ cf uninstall-plugin FirehosePlugin
```



## Application Logging in Cloud Foundry

Page last updated:

Loggregator, the Cloud Foundry component responsible for logging, provides a stream of log output from your app and from Cloud Foundry system components that interact with your app during updates and execution.

By default, Loggregator streams logs to your terminal. If you want to persist more than the limited amount of logging information that Loggregator can buffer, you can drain logs to a third-party log management service. See [Third-Party Log Management Services](#).

Cloud Foundry gathers and stores logs in a best-effort manner. If a client cannot consume log lines quickly enough, the Loggregator buffer may need to overwrite some lines before the client has consumed them. A syslog drain or a CLI tail can usually keep up with the flow of app logs.

## Contents of a Log Line

Every log line contains four fields:

- Timestamp
- Log type (origin code)
- Channel: either `OUT`, for logs emitted on `stdout`, or `ERR`, for logs emitted on `stderr`
- Message

Loggregator assigns the timestamp when it receives log data. The log data is opaque to Loggregator, which simply puts it in the message field of the log line. Apps or system components sending log data to Loggregator may include their own timestamps, which then appear in the message field.

Origin codes distinguish the different log types. Origin codes from system components have three letters. The app origin code is `APP` followed by slash and a digit that indicates the app instance.

Many frameworks write to an app log that is separate from `stdout` and `stderr`. This is not supported by Loggregator. Your app must write to `stdout` or `stderr` for its logs to be included in the Loggregator stream. Check the buildpack your app uses to determine whether it automatically ensures that your app correctly writes logs to `stdout` and `stderr` only. Some buildpacks do this, and some do not.

## Log Types and Their Messages

Different types of logs have different message formats, as shown in the examples below. The digit appended to the code indicates the instance index: 0 is the first instance, 1 is the second, and so on.

### API

Users make API calls to request changes in app state. Cloud Controller, the Cloud Foundry component responsible for the API, logs the actions that Cloud Controller takes in response.

For example:

```
2016-06-14T14:10:05.36-0700 [API/0] OUT Updated app with guid cdabc600-0b73-48e1-b7d2-26af2c63f933 ({"name"=>"spring-music", "instances"=>1, "memory"=>512, "environment_js
```

### STG

The Diego cell or the Droplet Execution Agent emits STG logs when staging or restaging an app. These actions implement the desired state requested by the user. After the droplet has been uploaded, STG messages end and CELL messages begin. For STG, the instance index is almost always 0.

For example:

```
2016-06-14T14:10:27.91-0700 [STG/0] OUT Staging...
```

## RTR

The Router emits RTR logs when it routes HTTP requests to the app. Router messages include the app name followed by a Router timestamp and then selections from the HTTP request.

For example:

```
2016-06-14T10:51:32.51-0700 [RTR/1] OUT www.example.com - [14/06/2016:17:51:32.459 +0000] "GET /user/ HTTP/1.1" 200 0 103455 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) Ap
```

## Zipkin Trace Logging

If Zipkin trace logging is enabled in Cloud Foundry, then Gorouter access log messages contain Zipkin HTTP headers.

The following is an example access log message containing Zipkin headers:

```
2016-11-23T16:04:01.49-0800 [RTR/0] OUT www.example.com - [24/11/2016:00:04:01.227 +0000] "GET / HTTP/1.1" 200 0 109 "-" "curl/7.43.0" 10.0.2.150:4070 10.0.48.66:60815 x_forv
```

For more information about Zipkin tracing, see [Zipkin Tracking in HTTP Headers](#).

## LGR

Loggregator emits LGR to indicate problems with the logging process. Examples include “can’t reach syslog drain url” and “dropped log messages due to high rate.”

## APP

Every app emits logs according to choices by the developer.

For example:

```
2016-06-14T14:10:15.18-0700 [APP/0] OUT Exit status 0
```

## SSH

The Diego cell emits SSH logs when a user accesses an application container through SSH by using the Cloud Foundry Command Line Interface (cf CLI) [cf ssh](#) command.

For example:

```
2016-06-14T14:16:11.49-0700 [SSH/0] OUT Successful remote access by 192.0.2.33:7856
```

## CELL

The Diego cell emits CELL logs when it starts or stops the app. These actions implement the desired state requested by the user. The Diego cell also emits messages when an app crashes.

For example:

```
2016-06-14T13:44:38.14-0700 [CELL/0] OUT Successfully created container
```

## Writing to the Log from Your App

Your app must write logs to `stderr` or `stdout`. Both are typically buffered, and you should flush the buffer before delivering the message to Loggregator.



Alternatively, you can write log messages to `stderr` or `stdout` synchronously. This approach is mainly used for debugging because it may affect app performance.

## Including Container Metrics in Syslog Drains

By default, app logs are included in syslog drains. To include container metrics in your syslog drain, an operator must first set `scalablesyslog.adapter.metrics_to_syslog_enabled` to `true`. In Pivotal Application Service (PAS) 2.1 and later, this property is set to true by default.

Follow the instructions below to include container metrics in your syslog drain.

1. Log in to Ops Manager.
2. Go to the **System Logging** pane, in the PAS tile.
3. Enable **Include container metrics in Syslog Drains**.
4. Run the following cf CLI command:

```
cf drain APP-NAME DRAIN-URL --type metrics --drain-name YOUR-SYSLOG-DRAIN
```

Where:

- `APP-NAME` is your app name
- `YOUR-SYSLOG-DRAIN` is the name of your syslog drain
- `DRAIN-URL` is the URL of your syslog drain

## Viewing Logs in the Command Line Interface

Use the cf CLI [cf logs](#) command to view logs. You can tail, dump, or filter log output.

### Tailing Logs

Run `cf logs APP-NAME` to stream Loggregator output to the terminal. Replace `APP-NAME` with the name of your app.

For example:

```
$ cf logs spring-music
Connected, tailing logs for app spring-music in org example / space development as admin@example.com...

2016-06-14T15:16:12.70-0700 [RTR/4] OUT www.example.com - [14/06/2016:22:16:12.582 +0000] "GET / HTTP/1.1" 200 0 103455 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5
2016-06-14T15:16:20.06-0700 [RTR/4] OUT www.example.com - [14/06/2016:22:16:20.034 +0000] "GET /test/ HTTP/1.1" 200 0 6879 "http://www.example.com/" "Mozilla/5.0 (Macintosh
2016-06-14T15:16:22.44-0700 [RTR/4] OUT www.example.com - [14/06/2016:22:17:22.415 +0000] "GET /test5/ HTTP/1.1" 200 0 5461 "http://www.example.com/test5" "Mozilla/5.0 (Mac
...
```

Use **Ctrl-C** (^C) to exit the real-time stream.

### Dumping Logs

Run `cf logs APP-NAME --recent` to display all the lines in the Loggregator buffer. Replace `APP-NAME` with the name of your app.

### Filtering Logs

To view some subset of log output, run `cf logs APP-NAME` in conjunction with filtering commands of your choice. Replace `APP-NAME` with the name of your app. In the example below, `grep -v RTR` excludes all Router logs:

```
grep -v
RTR
```

```
$ cf logs spring-music --recent | grep -v RTR
2016-06-14T14:10:05.36-0700 [API/0] OUT Updated app with guid cdabc604-0b73-47e1-a7d5-24af2c63f723 ({"name"=>"spring-music", "instances"=>1, "memory"=>512, "environment_js
2016-06-14T14:10:14.52-0700 [APP/0] OUT - Gracefully stopping, waiting for requests to finish
2016-06-14T14:10:14.52-0700 [CELL/0] OUT Exit status 0
2016-06-14T14:10:14.54-0700 [APP/0] OUT === puma shutdown: 2016-06-14 21:10:14 +0000 ===
2016-06-14T14:10:14.54-0700 [APP/0] OUT - Goodbye!
2016-06-14T14:10:14.56-0700 [CELL/0] OUT Creating container
...
```

## Log Ordering

Ensuring log ordering in drains can be an important consideration for both operators and developers.

- Diego uses a nanosecond-based timestamp that can be ingested properly by Splunk. For more information, see [TIME\\_FORMAT and subseconds](#) in the Splunk documentation.
- The Elastic Stack can ingest the nanosecond timestamps but only supports millisecond precision, so timestamps are truncated. For more information, see the [Date datatype](#) in the Elasticsearch documentation and the [Date type has not enough precision for the logging use case](#) GitHub issue.

If you are developing a client that displays a stream of Cloud Foundry logs to users, you can order the logs to improve the debugging experience for your user. The following are general tips for ordering logs:

- For CLIs, batch the logs and display the logs you have in that timeframe, sorted by timestamp.
- For web clients, use dynamic HTML to insert older logs into the sorting as they appear. This creates complete, ordered logs.
- Java app developers may want to convert stack traces into a single log entity. To simplify log ordering for Java apps, use the [multi-line Java message workaround](#) to convert your multi-line stack traces into a single log entity.

By modifying the Java log output, you can force your app to reformat stack trace messages, replacing newline characters with a token. Set your log parsing code to replace that token with newline characters again to display the logs properly in Kibana.

## Customizing Platform Log Forwarding

Page last updated:

You can configure Pivotal Application Service (PAS) to forward logs to remote endpoints using the Syslog protocol defined in [RFC 5424](#). For more information, see [Enable Syslog Forwarding](#) in *Configuring Logging in PAS*.

PAS annotates forwarded messages with structured data. This structured data identifies the originating BOSH Director, deployment, instance group, availability zone, and instance ID. All logs forwarded from BOSH jobs have their PRI set to `14`, representing **Facility: user-level messages** and **Warning: warning conditions**, as defined in [RFC 5424 Section 6.2.1](#). This PRI value may not reflect the originally intended PRI of the log.

Logs forwarded from other sources, such as kernel logs, retain their original PRI value.

The following table describes the log line Structured Data:

| Structured Data   | Description                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------|
| ENTERPRISE_NUMBER | Cloud Foundry's private enterprise number, <code>47450</code> , as defined in <a href="#">RFC 5424 Section 7.2.2</a> . |
| DIRECTOR          | The name of the BOSH Director managing the deployment.                                                                 |
| DEPLOYMENT        | The name of the BOSH deployment.                                                                                       |
| INSTANCE_GROUP    | The name of the BOSH instance_group.                                                                                   |
| AVAILABILITY_ZONE | The name of the BOSH availability zone.                                                                                |
| ID                | The BOSH GUID.                                                                                                         |

Log lines use the format below:

```
<$PRI>$VERSION $TIMESTAMP $HOST $APP_NAME $PROC_ID $MSG_ID
[instance@ENTERPRISE_NUMBER director="$DIRECTOR" deployment="$DEPLOYMENT"
group="$INSTANCE_GROUP" az="$AVAILABILITY_ZONE" id="$ID"] $MESSAGE
```

Example log messages:

```
<14>1 2017-01-25T13:25:03.18377Z 192.0.2.10 etcd - - [instance@47450
director="test-env" deployment="cf" group="diego_database" az="us-west1-a"
id="83bd66e5-3fdf-44b7-bdd6-508deae7c786"] [INFO] the leader is
[https://diego-database-0.etcd.service.cf.internal:4001]
<14>1 2017-01-25T13:25:03.184491Z 192.0.2.10 bbs - - [instance@47450
director="test-env" deployment="cf" group="diego_database" az="us-west1-a"
id="83bd66e5-3fdf-44b7-bdd6-508deae7c786"]
{"timestamp":"1485350702.539694548","source":"bbs","message":
"bbs.request.start-actual-lrp.starting","log_level":1,"data":
{"actual_lrp_instance_key":{"instance_guid":
"271f71c7-4119-4490-619f-4f44694717c0"},"cell_id":
"diego_cell-2-41f21178-d619-4976-901c-325bc2d0d11d"},"actual_lrp_key":
{"process_guid":"1545ce89-01e6-4b8f-9cb1-5654a3ecae10-137e7eb4-12de-457d-
8e3e-1258e5a74687","index":5,"domain":"cf-apps"},"method":"POST","net_info":
{"address":"192.0.2.12","ports":[{"container_port":8080,"host_port":61532},
{"container_port":2222,"host_port":61533}]}, "request":
"/v1/actual_lrps/start","session":"418.1"}}
```

## Modify Which Logs PAS Forwards

When you enable log forwarding, PAS forwards all log lines written to the `/var/vcap/sys/log` directories on all Cloud Foundry virtual machines (VMs) to your configured External Syslog Aggregator endpoint by default.


You can configure PAS to forward a subset of logs instead of forwarding all logs as follows.

1. In the PAS tile, select **System Logging**.
2. In the **Custom rsyslog Configuration** textbox, enter a custom syslog rule. See the example custom syslog rules below.
3. Click **Save**.

For more information about enabling and configuring syslog forwarding, see [Configuring Logging in PAS](#).

The custom rsyslog rules shown below are written in [RainerScript](#). The custom rules are inserted before the rule that forwards logs. The *stop* command, `stop`, prevents logs from reaching the forwarding rule. This filters out these logs.

Logs filtered out before forwarding remain on the local disk, where the BOSH job originally wrote them. These logs remain on the local disk only until BOSH Director recreates the VMs. You can access these logs from Ops Manager or through SSH.

 **Note:** PAS requires a valid custom rule to forward logs. If your custom rule contains syntax errors, PAS forwards no logs.

## Forward Only Logs From a Certain Job


This rule filters out logs unless they originate from the `uaa` job:

```
if ($app-name != "uaa") then stop
```

## Exclude Logs With Certain Content

This rule filters out logs that contain “DEBUG” in the body.

```
if ($msg contains "DEBUG") then stop
```

 **Note:** The above example contains “DEBUG” in the message body. Not all logs intended for debugging purposes contain the string “DEBUG” in the message body.

## Troubleshooting and Diagnostics

Navigate these topics to troubleshoot and diagnose issues you may encounter when installing or using Pivotal Cloud Foundry (PCF).

### Table of Contents

- [Diagnosing Problems in PCF](#)
- [Troubleshooting Problems in PCF](#)
- [Advanced Troubleshooting with the BOSH CLI](#)
- [Troubleshooting Slow Requests in Cloud Foundry](#)
- [Troubleshooting TCP Routing](#)
- [Recovering MySQL from PAS Downtime](#)
- [Troubleshooting BBR](#)
- [Troubleshooting PCF on Azure](#)
- [Troubleshooting PCF on GCP](#)
- [Troubleshooting Ops Manager for VMware vSphere](#)
- [Troubleshooting Windows Cells](#)
- [Running mysql-diag](#)

## Diagnosing Problems in PCF

Page last updated:

This guide provides help with diagnosing issues encountered during a [Pivotal Cloud Foundry](#) (PCF) installation.

Besides whether products install successfully or not, an important area to consider when diagnosing issues is communication between VMs deployed by Pivotal Cloud Foundry. Depending on what products you install, communication takes the form of messaging, routing, or both. If they go wrong, an installation can fail. For example, in an Pivotal Application Service (PAS) installation the PCF VM tries to push a test application to the cloud during post-installation testing. The installation fails if the resulting traffic cannot be routed to the HA Proxy load balancer.

## Viewing the Debug Endpoint

The debug endpoint is a web page that provides information useful for diagnostics. If you have superuser privileges and can view the Ops Manager Installation Dashboard, you can access the debug endpoint.

- In a browser, open the URL:

`https://OPS-MANAGER-FQDN/debug`

The debug endpoint offers three links:

- *Files* allows you to view the YAML files that Ops Manager uses to configure products that you install. The most important YAML file, `installation.yml`, provides networking settings and describes `microbosh`. In this case, `microbosh` is the VM whose BOSH Director component is used by Ops Manager to perform installations and updates of PAS and other products.
- *Components* describes the components in detail.
- *Rails log* shows errors thrown by the VM where the Ops Manager web application (a Rails application) is running, as recorded in the `production.log` file. See the next section to learn how to explore other logs.

## Logging Tips

### Identifying Where to Start

This section contains general tips for locating where a particular problem is called out in the log files. Refer to the later sections for tips regarding specific logs (such as those for PAS Components).

- Start with the largest and most recently updated files in the job log
- Identify logs that contain 'err' in the name
- Scan the file contents for a "failed" or "error" string

## Viewing Logs for PAS Components



To troubleshoot specific PAS components by viewing their log files, browse to the Ops Manager interface and follow the procedure below.

1. In Ops Manager, browse to the PAS **Status** tab. In the **Job** column, locate the component of interest.
2. In the **Logs** column for the component, click the download icon.

Installation Dashboard

Pivotal Elastic Runtime

Settings Status Credentials Logs

| JOB     | INDEX | IPS        | CID                                     | LOAD AVG15 | CPU  | MEMORY | SWAP | SYSTEM DISK | EPHEM. DISK | PERS. DISK | LOGS                                                                                |
|---------|-------|------------|-----------------------------------------|------------|------|--------|------|-------------|-------------|------------|-------------------------------------------------------------------------------------|
| HAProxy | 0     | 10.0.0.254 | vm-9985a13c-106a-48d1-a3de-d0e0e816c857 | 0.08%      | 0.1% | 8.7%   | 0.0% | 41%         | 5%          | N/A        |  |
| NATS    | 0     | 10.0.0.5   | vm-dee49615-aea8-4f4f-bf0f-b1060083ddef | 0.05%      | 0.2% | 8.9%   | 0.0% | 41%         | 19%         | N/A        |  |
|         |       |            | vm-6d43e59e-                            |            |      |        |      |             |             |            |                                                                                     |

3. Browse to the PAS Logs tab.

Installation Dashboard

Pivotal Elastic Runtime

Settings Status Credentials Logs

| FILENAME                                                                                                                                                                      | UPDATED AT              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Downloaded:                                                                                                                                                                   |                         |
| <a href="/tmp/jobs_logs/diego_cell-partition-ee0b66b1415c8591855d-0-150e690af6dd.zip">/tmp/jobs_logs/diego_cell-partition-ee0b66b1415c8591855d-0-150e690af6dd.zip</a>         | 2016-04-12 19:06:47 UTC |
| <a href="/tmp/jobs_logs/diego_database-partition-ee0b66b1415c8591855d-0-ab7bd3378ef2.zip">/tmp/jobs_logs/diego_database-partition-ee0b66b1415c8591855d-0-ab7bd3378ef2.zip</a> | 2016-04-12 19:09:30 UTC |
| Pending:                                                                                                                                                                      |                         |
| <a href="/tmp/jobs_logs/diego_brain-partition-ee0b66b1415c8591855d-0-196edf23631b.zip">/tmp/jobs_logs/diego_brain-partition-ee0b66b1415c8591855d-0-196edf23631b.zip</a>       | 2016-04-12 19:09:34 UTC |

4. Once the zip file corresponding to the component of interest moves to the **Downloaded** list, click the linked file path to download the zip file.

5. Once the download completes, unzip the file.

The contents of the log directory vary depending on which component you view. For example, the Diego cell log directory contains subdirectories for the `metron_agent`, `rep`, `monit`, and `garden` processes. To view the standard error stream for `garden`, download the Diego cell logs and open

```
diego.0.job > garden >
garden.stderr.log
```

## Viewing Web Application and BOSH Failure Logs in a Terminal Window

You can obtain diagnostic information from the Operations Manager by logging in to the VM where it is running. To log in to the Operations Manager VM, you need the following information:

- The IP address of the PCF VM shown in the `Settings` tab of the Ops Manager Director tile.
- Your **import credentials**. Import credentials are the username and password used to import the PCF `.ova` or `.ovf` file into your virtualization system.

Complete the following steps to log in to the Operations Manager VM:

1. Open a terminal window.

2. Run `ssh IMPORT-USERNAME@PCF-VM-IP-ADDRESS` to connect to the PCF installation VM.

3. Enter your import password when prompted.

4. Change directories to the home directory of the web application:

```
cd /home/tempest-web/tempest/web/
```

5. You are now in a position to explore whether things are as they should be within the web application.

You can also verify that the `microbosh` component is successfully installed. A successful MicroBOSH installation is required to install PAS and any products like databases and messaging services.


6. Change directories to the BOSH installation log home:

```
cd /var/tempest/workspaces/default/deployments/micro
```

7. You may want to begin by running a tail command on the `current` log:

```
cd /var/tempest/workspaces/default/deployments/micro
```

If you are unable to resolve an issue by viewing configurations, exploring logs, or reviewing common problems, you can troubleshoot further by running BOSH diagnostic commands with the BOSH Command Line Interface (CLI).

 **Note:** Do not manually modify the deployment manifest. Operations Manager will overwrite manual changes to this manifest. In addition, manually changing the manifest may cause future deployments to fail.

## Viewing the VMs in Your Deployment

To view the VMs in your PCF deployment, perform the following steps specific to your IaaS.

### Amazon Web Services (AWS)

1. Log in to the [AWS Console](#).
2. Navigate to the EC2 Dashboard.
3. Click **Running Instances**.
4. Click the gear icon in the upper right.
5. Select the following: **job**, **deployment**, **director**, **index**.
6. Click **Close**.

### OpenStack

1. Install the [novaclient](#).
2. Point novaclient to your OpenStack installation and tenant by exporting the following environment variables:

```
$ export OS_AUTH_URL=YOUR_KEYSTONE_AUTH_ENDPOINT
$ export OS_TENANT_NAME=TENANT_NAME
$ export OS_USERNAME=USERNAME
$ export OS_PASSWORD=PASSWORD
```

3. List your VMs by running the following command:

```
$ nova list --fields metadata
```

### vSphere

1. Log into vCenter.



2. Select **Hosts and Clusters**.
3. Select the top level object that contains your PCF deployment. For example, select **Cluster**, **Datastore** or **Resource Pool**.
4. In the top tab, click **Related Objects**.
5. Select **Virtual Machines**.
6. Right click on the **Table** heading and select **Show/Hide Columns**.
7. Select the following boxes: **job**, **deployment**, **director**, **index**.

## Viewing Apps Manager Logs in a Terminal Window

The [Apps Manager](#) provides a graphical user interface to help manage organizations, users, applications, and spaces.

When troubleshooting Apps Manager performance, you might want to view the Apps Manager application logs. To view the Apps Manager application logs, follow these steps:

1. Run `cf login -a api.MY-SYSTEM-DOMAIN -u admin` from a command line to log in to PCF using the UAA Administrator credentials. In Pivotal Ops Manager, refer to PAS **Credentials** for these credentials.

```
$ cf login -a api.example.com -u admin
API endpoint: api.example.com

Password>*****
Authenticating...
OK
```

2. Run `cf target -o system -s apps-manager` to target the `system` org and the `apps-manager` space.

```
$ cf target -o system -s apps-manager
```

3. Run `cf logs apps-manager` to tail the Apps Manager logs.

```
$ cf logs apps-manager
Connected, tailing logs for app apps-manager in org system / space apps-manager as
admin...
```

## Changing Logging Levels for the Apps Manager

The Apps Manager recognizes the `LOG_LEVEL` environment variable. The `LOG_LEVEL` environment variable allows you to filter the messages reported in the Apps Manager log files by severity level. The Apps Manager defines severity levels using the Ruby standard library [Logger class](#).

By default, the Apps Manager `LOG_LEVEL` is set to `info`. The logs show more verbose messaging when you set the `LOG_LEVEL` to `debug`.

To change the Apps Manager `LOG_LEVEL`, run `cf set-env apps-manager LOG_LEVEL` with the desired severity level.

```
$ cf set-env apps-manager LOG_LEVEL debug
```

You can set `LOG_LEVEL` to one of the six severity levels defined by the Ruby Logger class:

- **Level 5:** `unknown` – An unknown message that should always be logged
- **Level 4:** `fatal` – An unhandleable error that results in a program crash
- **Level 3:** `error` – A handleable error condition
- **Level 2:** `warn` – A warning
- **Level 1:** `info` – General information about system operation
- **Level 0:** `debug` – Low-level information for developers

Once set, the Apps Manager log files only include messages at the set severity level and above. For example, if you set `LOG_LEVEL` to `fatal`, the log includes `fatal` and `unknown` level messages only.

## Analyzing Disk Usage on Containers and Diego Cell VMs

To obtain disk usage statistics by Diego Cell VMs and containers, see [Examining GrootFS Disk Usage](#).

## Troubleshooting Problems in PCF

Page last updated:

This guide provides help with resolving issues encountered during a [Pivotal Cloud Foundry](#) (PCF) installation.

### Retrying the Deployment

Although an install or update can fail for many reasons, the system is self-healing, and can often automatically correct or work around hardware or network faults.

Click **Install** or **Apply Changes** again, and the system may resolve a problem on its own.

Some failures only produce generic errors like `Exited with 1`. In cases like this, where a failure is not accompanied by useful information, click **Install** or **Apply Changes** to retry.

When the system does provide informative evidence, review the [Common Problems](#) section at the end of this guide to see if your problem is covered there.

### Common Issues

Compare evidence that you have gathered to the descriptions below. If your issue is covered, try the recommended remediation procedures.

#### BOSH Does Not Reinstall

You might want to reinstall BOSH for troubleshooting purposes. However, if PCF does not detect any changes, BOSH does not reinstall. To force a reinstall of BOSH, select **BOSH Director > Resource Sizes** and change a resource value. For example, you could increase the amount of RAM by 4 MB.

#### Creating Bound Missing VMs Times Out

This task happens immediately following package compilation, but before job assignment to agents. For example:

```
cloud_controller/0: Timed out ping to f690db09-876c-475e-865f-2cece06aba79 after 600 seconds (00:10:24)
```

This is most likely a NATS issue with the VM in question. To identify a NATS issue, inspect the agent log for the VM. Since the BOSH director is unable to reach the BOSH agent, you must access the VM using another method. You will likely also be unable to access the VM using TCP. In this case, access the VM using your virtualization console.

To diagnose:

1. Access the VM using your virtualization console and log in.
2. Navigate to the **Credentials** tab of the Pivotal Application Service (PAS) tile and locate the VM in question to find the **VM credentials**.
3. Become root.
4. Run `cd /var/vcap/bosh/log`.
5. Open the file `current`.
6. First, determine whether the BOSH agent and director have successfully completed a handshake, represented in the logs as a “ping-pong”:

```
2013-10-03_14:35:48.58456 #[608] INFO: Message: {"method"=>"ping", "arguments"=>[],
"reply_to"=>"director.f4b7df14-cb8f.19719508-e0dd-4f53-b755-58b6336058ab"}

2013-10-03_14:35:48.60182 #[608] INFO: reply_to: director.f4b7df14-cb8f.19719508-e0dd-4f53-b755-58b6336058ab:
payload: {:value=>"pong"}
```

This handshake must complete for the agent to receive instructions from the director.

7. If you do not see the handshake, look for another line near the beginning of the file, prefixed `INFO: loaded new infrastructure settings`. For example:

```
2013-10-03_14:35:21.83222 #[608] INFO: loaded new infrastructure settings:
{"vm"=>{"name"=>"vm-4d80ede4-b0a5-4992-aea6a0386e18e", "id"=>"vm-360"},
"agent_id"=>"56aea4ef-6aa9-4c39-8019-7024ccfdde4",
"networks"=>{"default"=>{"ip"=>"192.0.2.19",
"netmask"=>"255.255.255.0", "cloud_properties"=>{"name"=>"VMNetwork"},
"default"=>{"dns", "gateway"},
"dns"=>["192.0.2.2", "192.0.2.17"], "gateway"=>"192.0.2.2",
"dns_record_name"=>"0.nats.default.cf-d729343071061.microbosh",
"mac"=>"00:50:56:9b:71:67"}}, "disks"=>{"system"=>0, "ephemeral"=>1,
"persistent"=>{}}, "ntp"=>[], "blobstore"=>{"provider"=>"dav",
"options"=>{"endpoint"=>"http://192.0.2.17:25250",
"user"=>"agent", "password"=>"agent"}},
"mbus"=>"nats://nats:nats@192.0.2.17:4222",
"env"=>{"bosh"=>{"password"=>"$6$40ftQ9K4rvvC/8ADZHW0"}}}
```

This is a JSON blob of key/value pairs representing the expected infrastructure for the BOSH agent. For this issue, the following section is the most important:

```
"mbus"=>"nats://nats:nats@192.0.2.17:4222"
```

This key/value pair represents where the agent expects the NATS server to be. One diagnostic tactic is to try pinging this NATS IP address from the VM to determine whether you are experiencing routing issues.

## Install Exits With a Creates/Updates/Deletes App Failure or With a 403 Error

**Scenario 1:** Your PCF install exits with the following 403 error when you attempt to log in to the Apps Manager:

```
{"type": "step_finished", "id": "apps-manager.deploy"}

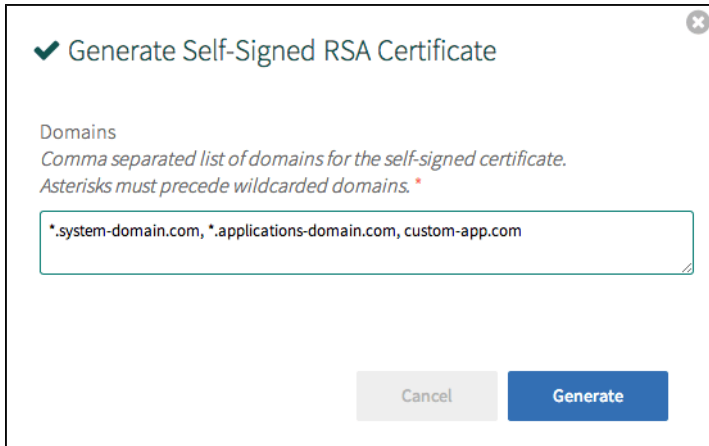
/home/tempest-web/tempest/web/vendor/bundle/ruby/1.9.1/gems/mechanize-2.7.2/lib/mechanize/http/agent.rb:306:in
`fetch': 403 => Net::HTTPForbidden for https://login.api.example.net/oauth/authorizereponse_type=code&client_id=portal&redirect_uri=https%3..
-- unhandled response (Mechanize::ResponseCodeError)
```

**Scenario 2:** Your PCF install exits with a `creates/updates/deletes an app (FAILED - 1)` error message with the following stack trace:

```
1) App CRUD creates/updates/deletes an app
Failure/Error: Unable to find matching line from backtrace
CFoundry::TargetRefused:
 Connection refused - connect(2)
```

In either of the above scenarios, ensure that you have correctly entered your domains in wildcard format:

1. Browse to the Operations Manager fully qualified domain name (FQDN).
2. Click the PAS tile.
3. Select **HAProxy** and click **Generate Self-Signed RSA Certificate**.
4. Enter your system and app domains in wildcard format, as well as optionally any custom domains, and click **Save**. Refer to **PAS Cloud Controller** for explanations of these domain values.



## Install Fails When Gateway Instances Exceed Zero

If you configure the number of Gateway instances to be greater than zero for a given product, you create a dependency on PAS for that product installation. If you attempt to install a product tile with an PAS dependency before installing PAS, the install fails.

To change the number of Gateway instances, click the product tile, then select **Settings > Resource sizes > INSTANCES** and change the value next to the product Gateway job.

To remove the PAS dependency, change the value of this field to `0`.

## Out of Disk Space Error

PCF displays an `Out of Disk Space` error if log files expand to fill all available disk space. If this happens, rebooting the PCF installation VM clears the tmp directory of these log files and resolves the error.

If users receive `Out of Disk Space` errors when trying to push apps, this can mean that Diego cells may be running out of disk space capacity.

To perform a detailed analysis of disk usage by containers and host VMs in your PAS deployment, see [Examining GrootFS Disk Usage](#).

## Installing BOSH Director Fails

If the DNS information for the PCF VM is incorrectly specified when deploying the PCF .ova file, installing BOSH Director fails at the “Installing Micro BOSH” step.

To resolve this issue, correct the DNS settings in the PCF Virtual Machine properties.

## Deleting Ops Manager Fails

Ops Manager displays an error message when it cannot delete your installation. This scenario might happen if the BOSH Director cannot access the VMs or is experiencing other issues. To manually delete your installation and all VMs, you must do the following:

1. Use your IaaS dashboard to manually delete the VMs for all installed products, with the exception of the Ops Manager VM.
2. SSH into your Ops Manager VM and remove the `installation.yml` file from `/var/tempest/workspaces/default/`.

**Note:** Deleting the `installation.yml` file does not prevent you from reinstalling Ops Manager. For future deploys, Ops Manager regenerates this file when you click **Save** on any page in the BOSH Director.

Your installation is now deleted.

## Installing PAS Fails

The following sections describe errors that may occur when installing PAS and how to resolve them.

## Ops Manager Cannot Verify App Push

If the DNS information for the PCF VM becomes incorrect after BOSH Director has been installed, installing PAS with Pivotal Operations Manager fails at the “Verifying app push” step.

To resolve this issue, correct the DNS settings in the PCF Virtual Machine properties.

## MySQL Monitor Not Running After Update

When MySQL cannot communicate with UAA, Ops Manager shows the following error:

**Error: ‘mysql\_monitor/12a3b456-cd7e-8fgh-9012-345678b90ijk (0)’ is not running after update. Review logs for failed jobs: replication-canary.**

If you see this error, create firewall rules that allow MySQL to reach UAA, using the [MySQL Network Communications](#) topic as a reference.

## Ops Manager Hangs During MicroBOSH Install or HAProxy States “IP Address Already Taken”

During an Ops Manager installation, you might receive the following errors:

- The Ops Manager GUI shows that the installation stops at the “Setting MicroBOSH deployment manifest” task.
- When you set the IP address for the HAProxy, the “IP Address Already Taken” message appears.

When you install Ops Manager, you assign it an IP address. Ops Manager then takes the next two consecutive IP addresses, assigns the first to MicroBOSH, and reserves the second. For example:

```
203.0.113.1 - Ops Manager (User assigned)
203.0.113.2 - MicroBOSH (Ops Manager assigned)
203.0.113.3 - Reserved (Ops Manager reserved)
```

To resolve this issue, ensure that the next two subsequent IP addresses from the manually assigned address are unassigned.

## Poor PCF Performance

If you notice poor network performance by your PCF deployment and your deployment uses a Network Address Translation (NAT) gateway, your NAT gateway may be under-resourced.

### Troubleshoot

To troubleshoot the issue, set a custom firewall rule in your IaaS console to route traffic originating from your private network directly to an S3-compatible object store. If you see decreased average latency and improved network performance, perform the solution below to scale up your NAT gateway.

### Scale Up Your NAT Gateway

Perform the following steps to scale up your NAT gateway:

1. Navigate to your IaaS console.
2. Spin up a new NAT gateway of a larger VM size than your previous NAT gateway.
3. Change the routes to direct traffic through the new NAT gateway.
4. Spin down the old NAT gateway.

The specific procedures will vary depending on your IaaS. Consult your IaaS documentation for more information.

## Common Issues Caused by Firewalls

This section describes various issues you might encounter when installing PAS in an environment that uses a strong firewall.

### DNS Resolution Fails

When you install PCF in an environment that uses a strong firewall, the firewall might block DNS resolution. To resolve this issue, refer to the [Troubleshooting DNS Resolution Issues](#) section of the Preparing Your Firewall for Deploying PCF topic.

## Advanced Troubleshooting with the BOSH CLI

Page last updated:

This topic describes using the BOSH CLI to help diagnose and resolve issues with your [Pivotal Cloud Foundry](#) (PCF) deployment. Before using the information and techniques in this topic, review [Diagnosing Problems in PCF](#).

To follow the steps in this topic, you must log in to the BOSH Director VM. The BOSH Director runs on the virtual machine (VM) that Ops Manager deploys on the first install of the BOSH Director tile.

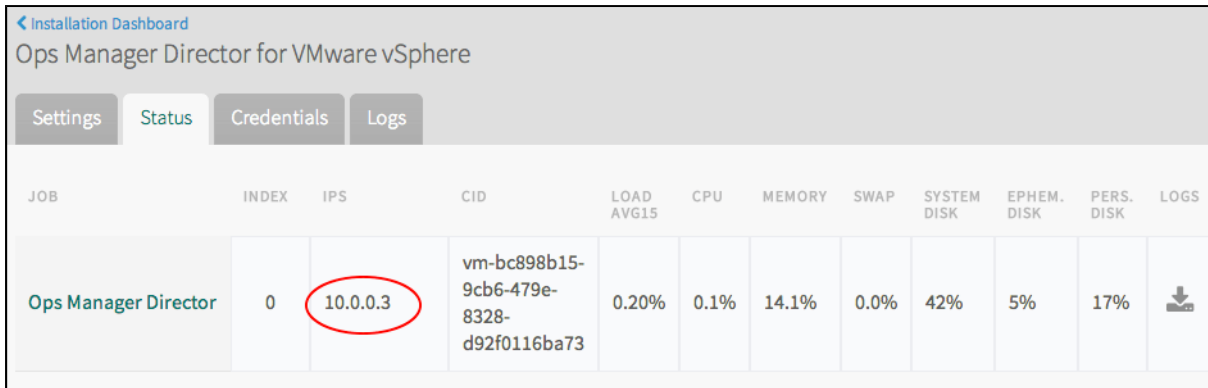
After authenticating into the BOSH Director, you can run specific commands using the BOSH Command Line Interface (BOSH CLI). BOSH Director diagnostic commands have access to information about your entire [Pivotal Cloud Foundry](#) (PCF) installation.


**Note:** Before running any BOSH CLI commands, verify that no BOSH Director tasks are running on the Ops Manager VM. See the *Tasks* section of [BOSH CLI commands](#) for more information.

## Gather Credential and IP Address Information

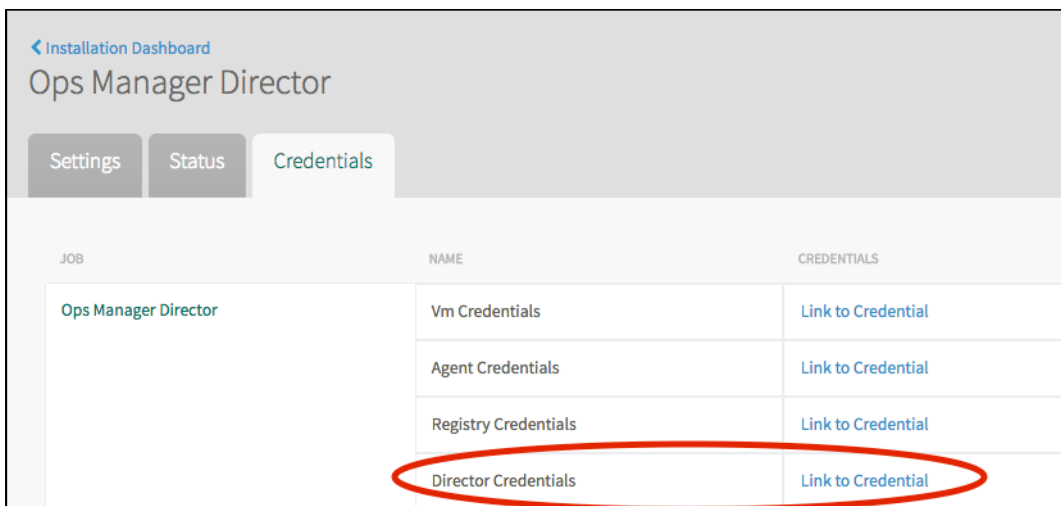
Before you begin troubleshooting with the BOSH CLI, follow the instructions below to collect the information you need from the Ops Manager interface.

1. Open the Ops Manager interface by navigating to the Ops Manager fully qualified domain name (FQDN) in a web browser.
2. Click the **BOSH Director** tile and select the **Status** tab.
3. Record the IP address for the Director job. This is the IP address of the VM where the BOSH Director runs.



| JOB                  | INDEX | IPS      | CID                                     | LOAD AVG15 | CPU  | MEMORY | SWAP | SYSTEM DISK | EPHEM. DISK | PERS. DISK | LOGS                                                                                  |
|----------------------|-------|----------|-----------------------------------------|------------|------|--------|------|-------------|-------------|------------|---------------------------------------------------------------------------------------|
| Ops Manager Director | 0     | 10.0.0.3 | vm-bc898b15-9cb6-479e-8328-d92f0116ba73 | 0.20%      | 0.1% | 14.1%  | 0.0% | 42%         | 5%          | 17%        |  |

4. Select the **Credentials** tab.
5. Click **Link to Credential** to view the **Director Credentials**. Record these credentials.




| JOB                  | NAME                 | CREDENTIALS                        |
|----------------------|----------------------|------------------------------------|
| Ops Manager Director | Vm Credentials       | <a href="#">Link to Credential</a> |
|                      | Agent Credentials    | <a href="#">Link to Credential</a> |
|                      | Registry Credentials | <a href="#">Link to Credential</a> |
|                      | Director Credentials | <a href="#">Link to Credential</a> |

6. Return to the **Installation Dashboard**.



7. **(Optional)** To prepare to troubleshoot the job VM for any other product, click the product tile and repeat the procedure above to record the IP address and VM credentials for that job VM.
8. Log out of Ops Manager.

 **Note:** Ensure that there are no Ops Manager installations or updates in progress while using the BOSH CLI.

## Log in to the Ops Manager VM with SSH

Use SSH to connect to the Ops Manager VM. Follow the instructions in one of the sections below to log in to the Ops Manager VM with SSH.

### AWS

To log in to the Ops Manager VM with SSH in AWS, you need the key pair you used when you created the Ops Manager VM. To see the name of the key pair, click on the Ops Manager VM and locate the `key pair name` in the properties.

To log in to the Ops Manager VM with SSH in AWS, do the following:

1. Locate the Ops Manager FQDN on the AWS **EC2 instances** page.
2. Run `chmod 600 ops_mgr.pem` to change the permissions on the `.pem` file to be more restrictive. For example:

```
$ chmod 600 ops_mgr.pem
```

3. Run `ssh -i ops_mgr.pem ubuntu@OPS-MANAGER-FQDN` to log in to the Ops Manager VM with SSH. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager. For example:

```
$ ssh -i ops_mgr.pem ubuntu@my-opsmanager-fqdn.example.com
```

### Azure

To log in to the Ops Manager VM with SSH in Azure, you need the key pair you used when creating the Ops Manager VM. If you need to reset the SSH key, locate the Ops Manager VM in the Azure portal and click **Reset Password**.

To log in to the Ops Manager VM with SSH in Azure, do the following:

1. Locate the Ops Manager FQDN by selecting the VM in the Azure portal.
2. Run `chmod 600 ops_mgr.pem` to change the permissions on the `.pem` file to be more restrictive. For example:

```
$ chmod 600 ops_mgr.pem
```

3. Run `ssh -i ops_mgr.pem ubuntu@OPS-MANAGER-FQDN` to log in to the Ops Manager VM with SSH. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager. For example:

```
$ ssh -i ops_mgr.pem ubuntu@my-opsmanager-fqdn.example.com
```

### GCP

To log in to the Ops Manager VM with SSH in GCP, do the following:

1. Confirm that you have installed the [Google Cloud SDK and CLI](#). See the [Google Cloud Platform documentation](#) for more information.
2. Initialize Google Cloud CLI, using a user account with Owner, Editor, or Viewer permissions to access the project. Ensure that the Google Cloud CLI can login to the project by running the command `gcloud auth login`.
3. From the GCP web console, navigate to **Compute Engine**.

4. Locate the Ops Manager VM in the **VM Instances** list.
5. Under **Remote access**, click the **SSH** dropdown and select **View gcloud command**.
6. Copy the SSH command that appears in the popup window.
7. Paste the command into your terminal window to SSH to the VM. For example:

```
$ gcloud compute ssh "YOUR-VM" --zone "YOUR-ZONE-ID"
```

8. Run `sudo su - ubuntu` to switch to the `ubuntu` user.

## OpenStack

To log in to the Ops Manager VM with SSH in OpenStack, you need the key pair that you created in *Step 2: Configure Security* of [Deploying Ops Manager to OpenStack](#). If you need to reset the SSH key, locate the Ops Manager VM in the OpenStack console and boot it in recovery mode to generate a new key pair.

To log in to the Ops Manager VM with SSH in OpenStack, do the following:

1. Locate the Ops Manager FQDN on the **Access & Security** page.
2. Run `chmod 600 ops_mgr.pem` to change the permissions on the `.pem` file to be more restrictive. For example:


```
$ chmod 600 ops_mgr.pem
```

3. Run `ssh -i ops_mgr.pem ubuntu@OPS-MANAGER-FQDN` to log in to the Ops Manager VM with SSH. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager. For example:

```
$ ssh -i ops_mgr.pem ubuntu@my-opsmanager-fqdn.example.com
```

## vSphere

To log in to the Ops Manager VM with SSH in vSphere, you need the credentials used to import the PCF .ova or .ovf file into your virtualization system. You set these credentials when you installed Ops Manager.

 **Note:** If you lose your credentials, you must shut down the Ops Manager VM in the vSphere UI and reset the password. See the [vSphere documentation](#) for more information.

1. From a command line, run `ssh ubuntu@OPS-MANAGER-FQDN` to log in to the Ops Manager VM with SSH. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
2. When prompted, enter the password that you set during the .ova deployment into vCenter. For example:

```
$ ssh ubuntu@my-opsmanager-fqdn.example.com
Password: *****
```

## Log in to the BOSH Director VM

Follow the steps below to log in to the BOSH Director VM.

### Create a Local BOSH Director Alias

1. Run the following command to create a local alias for the BOSH Director using the BOSH CLI: `bosh alias-env MY-ENV -e DIRECTOR-IP-ADDRESS --ca-cert /var/tempest/workspaces/default/root_ca_certificate`  
Replace the placeholder text with the following:
  - `MY-ENV`: Enter an alias for the BOSH Director, such as `gcp`.

- `DIRECTOR-IP-ADDRESS`: Enter the IP address of your BOSH Director VM. For example:

```
$ bosh alias-env gcp -e 10.0.0.3 --ca-cert /var/tempest/workspaces/default/root_ca_certificate
```

2. Log in to the BOSH Director VM using one of the following options:

- [Internal User Store Login through UAA](#): Log in to the BOSH Director VM using BOSH.
- [External User Store Login through SAML](#): Use an external user store to log in to the BOSH Director VM.

## Log in to the BOSH Director VM with UAA

1. Retrieve the Director password from the **BOSH Director > Credentials** tab. Alternatively, launch a browser and visit `https://OPS-MANAGER-FQDN/api/v0/deployed/director/credentials/director_credentials` to obtain the password. Replace `OPS-MANAGER-FQDN` with the fully qualified domain name of Ops Manager.
2. Run `bosh -e MY-ENV log-in` to log in to the BOSH Director VM. Replace `MY-ENV` with the alias for your BOSH Director. For example:

```
$ bosh -e gcp log-in
```


Follow the BOSH CLI prompts and enter the BOSH Director credentials to log in to the BOSH Director VM.

## Log in to the BOSH Director VM with SAML

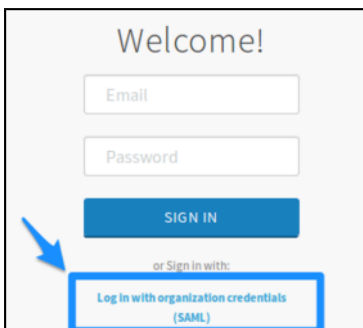
1. Log in to your identity provider and use the following information to configure SAML Service Provider Properties:
  - **Service Provider Entity ID**: `bosh-uaa`
  - **ACS URL**: `https://DIRECTOR-IP-ADDRESS:8443/saml/SSO/alias/bosh-uaa`
  - **Binding**: HTTP Post
  - **SLO URL**: `https://DIRECTOR-IP-ADDRESS:8443/saml/SSO/alias/bosh-uaa`
  - **Binding**: HTTP Redirect
  - **Name ID**: Email Address
2. Run `bosh -e MY-ENV log-in` to log in to the BOSH Director VM. Replace `MY-ENV` with the alias for your BOSH Director. For example:

```
$ bosh -e gcp log-in
```

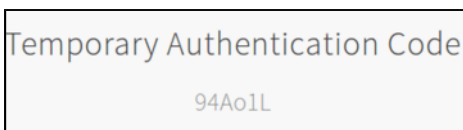
Follow the BOSH CLI prompts and enter your SAML credentials to log in to the BOSH Director VM.

 **Note:** Your browser must be able to reach the BOSH Director in order to log in with SAML.

3. Click **Log in with organization credentials (SAML)**.



4. Copy the **Temporary Authentication Code** that appears in your browser.




5. You see a login confirmation. For example:

Logged in as admin@example.org

## Log in to the BOSH Director VM with SSH


Do the following steps to log in to the BOSH Director VM with SSH:

1. From Ops Manager, open the BOSH Director tile.
2. Select the **Credentials** tab.
3. Next to **Bbr Ssh Credentials**, click **Link to Credential**. A tab opens containing a JSON credential structure.
4. Copy the `RSA PRIVATE KEY` and paste it into a file named `bbr.pem`. Include `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----`.

 **warning:** Pivotal recommends you keep the key secure. The key provides full access to the entire PCF environment.

5. Replace all `\n` characters in `bbr.pem` with a line break.
6. Copy `bbr.pem` to the `~/ssh/` directory on your machine.
7. Modify the permissions of the file by running `chmod 600 ~/ssh/bbr.pem`.
8. Log in to the BOSH Director VM with SSH from your machine.

```
ssh bbr@BOSH-DIRECTOR-IP -i ~/ssh/bbr.pem
```

 **Note:** If you are using GCP, ensure SSH port `22` is open for your BOSH Director VM in your GCP console. If the SSH port is not open, open it by creating a firewall rule.

9. Run `sudo -i` to get the root privilege.

## Use the BOSH CLI for Troubleshooting

This section describes three BOSH CLI commands commonly used during troubleshooting.

- **VMs:** Lists the VMs in a deployment
- **Cloud Check:** Runs a cloud consistency check and interactive repair
- **SSH:** Starts an interactive session or executes commands with a VM

### BOSH VMs

The `bosh vms` command provides an overview of the virtual machines that BOSH manages.


To use this command, run `bosh -e MY-ENV vms` to see an overview of all virtual machines managed by BOSH, or `bosh -e MY-ENV -d MY-DEPLOYMENT vms` to see only the virtual machines associated with a particular deployment. Replace `MY-ENV` with your environment, and, if using the `-d` flag, also replace `MY-DEPLOYMENT` with the name of a deployment.

When troubleshooting an issue with your deployment, `bosh vms` may show a VM in an **unknown** state. Run [bosh cloud-check](#) on a VM in an **unknown** state to instruct BOSH to diagnose problems with the VM.

You can also run `bosh vms` to identify VMs in your deployment, then use the [bosh ssh](#) command to log in to an identified VM with SSH for further troubleshooting.

`bosh vms` supports the following arguments:

- `--dns`: Report also includes the DNS A record for each VM
- `--vitals`: Report also includes load, CPU, memory usage, swap usage, system disk usage, ephemeral disk usage, and persistent disk usage for each

 **Note:** The **Status** tab of the Pivotal Application Service (PAS) product tile displays information similar to the `bosh vms` output.

## BOSH Cloud Check

Run the `bosh cloud-check` command to instruct BOSH to detect differences between the VM state database maintained by the BOSH Director and the actual state of the VMs. For each difference detected, `bosh cloud-check` can offer the following repair options:

- `Reboot VM`: Instructs BOSH to reboot a VM. Rebooting can resolve many transient errors.
- `Ignore problem`: Instructs BOSH to do nothing. You may want to ignore a problem in order to run `bosh ssh` and attempt troubleshooting directly on the machine.
- `Reassociate VM with corresponding instance`: Updates the BOSH Director state database. Use this option if you believe that the BOSH Director state database is in error and that a VM is correctly associated with a job.
- `Recreate VM using last known apply spec`: Instructs BOSH to destroy the server and recreate it from the deployment manifest that the installer provides. Use this option if a VM is corrupted.
- `Delete VM reference`: Instructs BOSH to delete a VM reference in the Director state database. If a VM reference exists in the state database, BOSH expects to find an agent running on the VM. Select this option only if you know that this reference is in error. Once you delete the VM reference, BOSH can no longer control the VM.

To use this command, run `bosh -e MY-ENV -d MY-DEPLOYMENT cloud-check`. Replace `MY-ENV` with your environment, and `MY-DEPLOYMENT` with your deployment.

## Example Scenarios

### Unresponsive Agent

```
$ bosh -e example-env -d example-deployment cloud-check
cdb/0 (vm-3e37133c-bc33-450e-98b1-f86d5b63502a) is not responding:

- Ignore problem
- Reboot VM
- Recreate VM using last known apply spec
- Delete VM reference (DANGEROUS!)
```

### Missing VM

```
$ bosh -e example-env -d example-deployment cloud-check
VM with cloud ID 'vm-3e37133c-bc33-450e-98b1-f86d5b63502a' missing:

- Ignore problem
- Recreate VM using last known apply spec
- Delete VM reference (DANGEROUS!)
```

### Unbound Instance VM

```
$ bosh -e example-env -d example-deployment cloud-check
VM 'vm-3e37133c-bc33-450e-98b1-f86d5b63502a' reports itself as 'cdb/0' but does not have a bound instance:

- Ignore problem
- Delete VM (unless it has persistent disk)
- Reassociate VM with corresponding instance
```

### Out of Sync VM

```
$ bosh -e example-env -d example-deployment cloud-check
VM 'vm-3e37133c-bc33-450e-98b1-f86d5b63502a' is out of sync:
expected 'cf-d7293430724a2c421061: cdb/0', got 'cf-d7293430724a2c421061: nats/0':

- Ignore problem
- Delete VM (unless it has persistent disk)
```

## BOSH SSH

Use `bosh ssh` to log in to the VMs in your deployment with SSH.

Follow the steps below to use `bosh ssh` :

1. Identify a VM to log in to with SSH. Run `bosh -e MY-ENV -d MY-DEPLOYMENT vms` to list the VMs in the given deployment. Replace `MY-ENV` with your environment alias and `MY-DEPLOYMENT` with the deployment name.
2. Run `bosh -e MY-ENV -d MY-DEPLOYMENT ssh VM-NAME/GUID`. For example:

```
$ bosh -e example-env -d example-deployment ssh diego-cell/abcd0123-a012-b345-c678-9def01234567
```

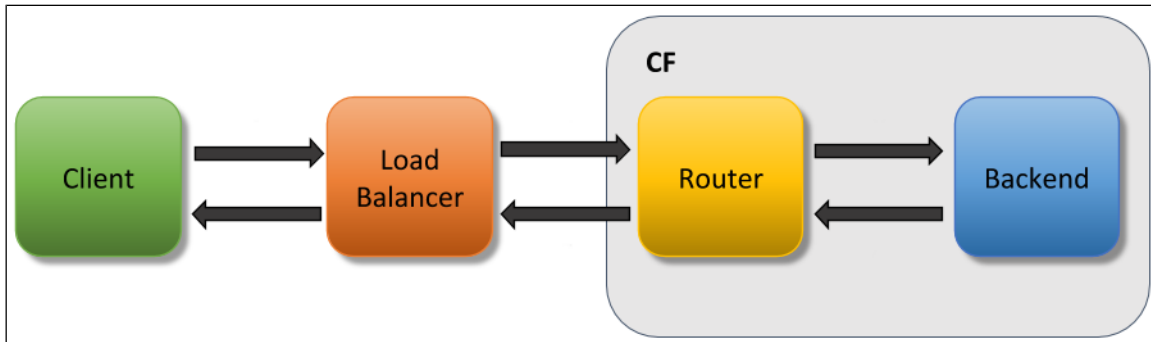
## Troubleshooting Slow Requests in Cloud Foundry

Page last updated:

This topic suggests ways that an operator of Cloud Foundry (CF) can diagnose the location of app request delays.

### App Request Path

App requests typically transit the following components. Only the router (Gorouter) and app are within the scope of Cloud Foundry. Operators may have the HAProxy load balancer that comes with CF deployed, instead of or in addition to, an infrastructure load balancer.



You can use `time` to measure a request's full round trip time from the client and back, examine `cf logs` output to measure the time just within Cloud Foundry, and add log messages to your app for fine-grained measurements of where the app itself takes time. By comparing these times, you can determine whether your delay comes from outside CF, inside the Gorouter, or in the app.

The following sections describe a scenario of diagnosing the source of delay for an app `app1`.

### Measure Total Round-Trip App Requests

On a command line, run `time curl -v APP-ENDPOINT` to measure the total round-trip time for deployed app `app1`. For example:

```

$ time curl -v http://app1.app_domain.com

GET /hello HTTP/1.1
Host: app1.app_domain.com
User-Agent: curl/7.43.0
Accept: */*

HTTP/1.1 200 OK
Content-Type: application/json;charset=utf-8
Date: Tue, 14 Dec 2016 00:31:32 GMT
Server: nginx
X-Content-Type-Options: nosniff
X-Vcap-Request-Id: c30fad28-4972-46eb-7da6-9d07dc79b109
Content-Length: 602
hello world!
real 2m0.707s
user 0m0.005s
sys 0m0.007s

```

The `real` time output shows that the request to `http://app1.app_domain.com` took approximately 2 minutes, round-trip. This seems like an unreasonably long time, so it makes sense to find out where the delay is occurring. To narrow it down, the next step measures the part of that request response time that comes from within Cloud Foundry.

**Note:** If your `curl` outputs an error like `Could not resolve host: NONEXISTENT.com` then DNS failed to resolve. If `curl` returns normally but lacks a `X-Vcap-Request-Id`, the request from the Load Balancer did not reach Cloud Foundry.

## Measure App Requests within Cloud Foundry

The `cf logs` command streams log messages from the Gorouter as well as from apps. To see the timestamps of Gorouter messages to and from your app, do the following:

1. If necessary, run `cf apps` to determine the name of the app.
2. Run `cf logs APP-NAME`. Replace `APP-NAME` with the name of the app.
3. From another terminal window, send a request to your app.
4. After your app returns a response, enter `Ctrl-C` to stop streaming `cf logs`.

For example:

```
$ cf logs app1


2016-12-14T00:33:32.35-0800 [RTR/0] OUT app1.app_domain.com - [14/12/2016:00:31:32.348 +0000] "GET /hello HTTP/1.1" 200 0 60 "-" "HTTPClient/1.0 (2.7.1, ruby 2.3.3 (2016-11-21))"
2016-12-14T00:32:32.35-0800 [APP/PROC/WEB/0]OUT app1 received request at [14/12/2016:00:32:32.348 +0000] with "vcap_request_id": "01144146-1e7a-4c77-77ab-49ae3e286fe9"
^C
```

In the example above, the first line contains timestamps from the Gorouter for both when it received the request and what was its response time processing the request:

- `14/12/2016:00:31:32.348` : Gorouter receives request
- `response_time:120.00641734` : Gorouter round-trip processing time

This output shows that it took 120 seconds for the Gorouter to process the request, which means that the 2-minute delay above takes place within CF, either within the Gorouter or within the app.

To determine whether the app is responsible, [add logging](#) to your app to measure where it is spending time.

 **Note:** Every incoming request should generate an access log message. If a request does not generate an access log message, it means the Gorouter did not receive the request.

## Use App Logs to Locate Delays in CF

To gain a more detailed picture of where delays exist in your request path, augment the logging that your app generates. For example, call your logging library from the request handler to generate log lines when your app receives a request and finishes processing it:

```
2016-12-14T00:33:32.35-0800 [RTR/0] OUT app1.app_domain.com - [14/12/2016:00:31:32.348 +0000] "GET /hello HTTP/1.1" 200 0 60 "-" "HTTPClient/1.0 (2.7.1, ruby 2.3.3 (2016-11-21))"
2016-12-14T00:32:32.35-0800 [APP/PROC/WEB/0]OUT app1 received request at [14/12/2016:00:32:32.348 +0000] with "vcap_request_id": "01144146-1e7a-4c77-77ab-49ae3e286fe9"
2016-12-14T00:32:32.50-0800 [APP/PROC/WEB/0]OUT app1 finished processing req at [14/12/2016:00:32:32.500 +0000] with "vcap_request_id": "01144146-1e7a-4c77-77ab-49ae3e286fe9"
```

Comparing the router access log messages from the [previous section](#) with the new app logs above, we can construct the following timeline:

- `14/12/2016:00:31:32.348` : Gorouter receives request
- `2016-12-14T00:32:32.35` : App receives request
- `2016-12-14T00:32:32.50` : App finishes processing request
- `2016-12-14T00:33:32.35` : Gorouter finishes processing request

The timeline indicates that the Gorouter took close to 60 seconds to send the request to the app and another 60 seconds to receive the response from the app. This suggests a delay either with the Gorouter, or in network latency between the Gorouter and Diego cells hosting the app.

## Time the Gorouter Processing

To determine whether a Gorouter delay comes from the Gorouter itself or network latency between the Gorouter and the app, log into the Gorouter and compare the response times from calling the app two different ways:

- Call the app through the router proxy to process requests through the Gorouter
- Directly call a specific instance of the app, bypassing Gorouter processing



To make this comparison, do the following:

1. Log in to the `router` using `bosh ssh`. See the [BOSH SSH documentation](#) for more information.
2. Use `time` and `curl` to measure the response time of an app request originating from and processing through the Gorouter, but not running through the client network or load balancer:

```
$ time curl -H "Host: app1.app_domain.com" http://IP-GOROUTER-VM:80"
```

3. Obtain the IP address and port of a specific app instance by running the following and recording associated `host` and `port` values:

```
$ cf curl /v2/apps/${cf app app1 --guid}/stats
{
 "0": {
 "state": "RUNNING",
 "stats": {
 [...]
 "host": "10.10.148.39",
 "port": 60052,
 [...]
 },
 [...]
 }
}
```

4. Use the IP address and port values to measure response time calling the app instance directly, bypassing Gorouter processing:

```
$ time curl http://APP-HOST-IP:APP-PORT
```

If the Gorouter and direct response times are similar, it suggests network latency between the Gorouter and the Diego cell. If the Gorouter time is much longer than the direct-to-instance time, the Gorouter is slow processing requests. The next section explains why the Gorouter might be slow.

## Potential Causes for Gorouter Latency

- Routers are under heavy load from incoming client requests.
- Apps are taking a long time to process requests. This increases the number of concurrent threads held open by the Gorouter, reducing capacity to handle requests for other apps.

## Operations Recommendations

- Monitor CPU load for Gorouters. At high CPU (70%+), latency increases. If the Gorouter CPU reaches this threshold, consider adding another Gorouter instance.
- Monitor latency of all routers using metrics from the Firehose. Do not monitor the average latency across all routers. Instead, monitor them individually on the same graph.
- Consider using [Pingdom](#) against an app on your Cloud Foundry deployment to monitor latency and uptime.
- Consider enabling access logs on your load balancer. See your load balancer documentation for how. Just as we used Gorouter access log messages above to determine latency from the Gorouter, you can compare load balancer logs to identify latency between the load balancer and the Gorouter. You can also compare load balancer response times with the client response times to identify latency between client and load balancer.
- [Deploy a nozzle to the Loggregator Firehose](#) to track metrics for the Gorouter. Available metrics include:
  - CPU utilization
  - Latency
  - Requests per second

## Troubleshooting TCP Routes

Page last updated:

The following topic provides steps to determine whether TCP routing issues are related to DNS and load balancer misconfiguration, the TCP routing tier, or the routing subsystem.

### Rule Out the App

If you are having TCP routing issues with an app, follow the procedure below to determine what to troubleshoot.

### Prerequisites

This procedure requires that you have the following:

- An app with TCP routing issues.
- A TCP domain. See [Routes and Domains](#) for more information about creating a TCP domain.
- A simple HTTP web app that you can use to curl.

### Procedure

1. Push a simple HTTP app using your TCP domain by entering the following command:

```
$ cf push MY-APP -d tcp.MY-DOMAIN --random-route
```

2. Curl your app on the port generated for the route. For example, if the port is 1024:

```
$ curl tcp.MY-DOMAIN:1024
```

3. If the curl request fails to reach the app, proceed to the next section: [Rule Out DNS and the Load Balancer](#).
4. If the curl request to your simple app succeeds, curl the app you are having issues with.
5. If you cannot successfully curl your problem app, TCP routing is working correctly. There is an issue with the app you cannot successfully curl.

### Rule Out DNS and the Load Balancer

1. Curl the TCP router healthcheck endpoint:

```
$ curl tcp.MY-DOMAIN:80/health -v
```

2. If you receive a `200 OK` response, proceed to the next section: [Rule Out the Routing Subsystem](#).
3. If you do not receive a `200 OK`, your load balancer may not be configured to pass through the healthcheck port. Continue following this procedure to test your load balancer configuration.
4. Confirm that your TCP domain name resolves to your load balancer:

```
$ dig tcp.MY-DOMAIN
...
tcp.MY-DOMAIN. 300 IN A 123.456.789.123
```

5. As an admin user, list the reservable ports configured for the `default-tcp` router group:

```
$ cf curl /routing/v1/router_groups
[
 {
 "guid": "d9b1db52-ea78-4bb9-7473-ec8e5d411b14",
 "name": "default-tcp",
 "type": "tcp",
 "reservable_ports": "1024-1123"
 }
]
```

- Choose a port from the `reservable_ports` range and curl the TCP domain on this port. For example, if you chose port 1024:

```
$ curl tcp.MY-DOMAIN:1024 -v
```

- If you receive an immediate rejection, then the TCP router likely rejected the request because there is no route for this port.
- If your connection times out, then you need to configure your load balancer to route all ports in `reservable_ports` to the TCP routers.

## Rule Out the Routing Subsystem

Send a direct request to the TCP router to confirm that it routes to your app.

- SSH into your TCP router.
- Curl the port of your route using the IP address of the router itself. For example, if the port reserved for your route is `1024`, and the IP address of the TCP router is `10.0.16.18`:

```
$ curl 10.0.16.18:1024
```

- If the curl is successful, then the load balancer either:
  - cannot reach the TCP routers, or
  - is not configured to route requests to the TCP routers from the `reservable_ports`
- If you cannot reach the app by curling the TCP router directly, perform the following steps to confirm that your TCP route is in the routing table.
  - Record the **Tcp Emitter Credentials** from the **UAA** row in the **PAS Credentials** tab. This OAuth client has permissions to read the routing table.
  - Install the UAA CLI `uaac`:

```
$ gem install cf-uaac
```

- Obtain a token for this OAuth client from UAA by providing the client secret:

```
$ uaac token client get tcp_emitter
Client secret:
```

- Obtain an access\_token:

```
$ uaac context
```

- Use the [routing API](#) to list TCP routes:

```
$ curl api.MY-DOMAIN/routing/v1/tcp_routes -H "Authorization: bearer TOKEN"
[{"router_group_guid":"f3518f7d-d8a0-4279-4e89-c058040d0000",
 "backend_port":60000,"backend_ip":"10.244.00.0","port":60000,"modification_tag":{"guid":"d4cc3bbe-c838-4857-7360-19f034440000",
 "index":1},"ttl":120}]
```

- In this output, each route mapping has the following:
  - port**: your route port
  - backend\_ip**: an app instance mapped to the route
  - backend\_port**: the port number for the app instance mapped to the route
- If your route port is not in the response, then the `tcp_emitter` may be unable to register TCP routes with the routing API. Look at the logs for `tcp_emitter` to see if there are any errors or failures.

- h. If the route is in the response, but you were not able to curl the port on the TCP route directly, then the TCP router may be unable to reach the routing API. Look at the logs for `tcp_router` to see if there are any errors or failures.

## Troubleshooting Router Error Responses

Page last updated:

This topic helps operators to better understand if 502's are a result of the Pivotal Application Service Platform or an application.

### Points of Failure

There are different points of failure in which 502's can come from:

1. Infrastructure
  - Load Balancer
  - Network
2. Platform - PCF
  - Gorouter
  - Diego Cell(s)
3. Application

In the **Infrastructure**, 502's can occur in the following way:

- From the Load Balancer, 502's can surface when the Gorouters are not receiving traffic at all.
  - This can be observed if the Load Balancer is logging 502's but the Gorouters are not.

In the **Platform**, 502's can occur in the following ways:

- If the Gorouter is unable to connect to the application container:
  - TCP dial issues (can't make an initial connection to the [backend](#)). The Gorouter will retry TCP dial errors up to three times, if it still fails then a 502 will be returned to the client and logged to the `access.log`. This may be due to:
    - An application that is unresponsive (which indicates an issue with the application)
    - The Gorouter has a stale route (which indicates an issue with the platform)
    - The application container is corrupted (which indicates a problem with the platform)
    - These types of errors may look like this within the `gorouter.log`:

```
[2018-07-05 17:59:10+0000] {"log_level":3,"timestamp":1530813550.92134,"message":
"backend-endpoint-failed", "source":"vcap.gorouter", "data":{"route-endpoint":
{"ApplicationId":"","Addr":"10.0.32.15:60099","Tags":null,"RouteServiceUrl":""},
"error":"dial tcp 10.0.32.15:60099: getsockopt: connection refused"}}
```

- If the Gorouter successfully dials the endpoint but an error occurs:
  - `read: connection reset by peer` errors can occur when the application closes the connection abruptly with a TCP RST packet and not the expected FIN-ACK. This will cause the Gorouter to retry the next endpoint. Note, Gorouter does not currently retry on `write: connection reset by peer` failures.
  - TLS Handshake errors. When these errors occur, the Gorouter will retry up to three times and if it's still failing then a 502 may be returned. These errors appear similar to the following in the `gorouter.log` (and a 502 will be logged in the `access.log`):

```
[2018-07-05 18:20:54+0000] {"log_level":3,"timestamp":1530814854.4359834,"message":
"backend-endpoint-failed", "source":"vcap.gorouter", "data":{"route-endpoint":
{"ApplicationId":"","Addr":"10.0.16.17:61002","Tags":null,"RouteServiceUrl":""},
"error":"x509:certificate is valid for 53079ca3-c4fe-4910-78b9-c1a6, not xxx"}}
```

- If the Gorouter successfully connects to the endpoint, but an error occurs while the request is in transport (i.e. Gorouter has not received a response from the endpoint):
- Prior to PCF 2.0, there was a bug that logged a 502 for requests canceled by clients before the server responded with headers. PCF 2.0 and beyond, if the same situation occurs, a 499 is returned.

In an **Application**, 502's can occur in the following ways (Note: the Gorouter will not retry any error response that is returned by the application):

- If 502's are only occurring from a particular application instance(s) and not all of the applications on the platform, then it is likely an application-related error (i.e. application is overloaded, unresponsive, can't connect to database, etc.).


- If all applications are experiencing 502's, then it could either be a platform issue (possible misconfiguration) or an application issue (i.e. all applications are unable to connect to an upstream database).

## General Debugging Steps

Here are general debugging steps for any issue resulting with 502 error codes:

- Gather the Gorouter logs & Diego Cell logs at the time of the incident. To SSH into the router VM, see [Advanced Troubleshooting with the BOSH CLI](#). To download the router VM logs from Ops Manager, see [Monitoring PCF VMs from Ops Manager](#).
- Review the logs and consider the following questions:
  1. Which errors are the Gorouters returning?
  2. Is the Gorouter's [routing table](#) accurate (are the endpoints for the route as expected)?
  3. Do the Diego Cell logs have anything interesting about unexpected app crashes and/or restarts?
  4. Is the application healthy and handling requests successfully? (try using [request tracing headers](#) to verify)
- Was there a recent platform change/upgrade that caused an increase in 502's?
- Are there any suspicious [metrics](#) spiking? How is CPU & Memory utilization?

## Gorouter Error Classification Table

| Error Type                    | Status Code | Source of Issue         | Evidence                                                                                                                                                                                                                                                                                                  |
|-------------------------------|-------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dial                          | 502         | Application or Platform | logs with error <code>dial tcp</code>                                                                                                                                                                                                                                                                     |
| ConnectionResetOnRead         | 502         | Application or Platform | logs with error <code>read: connection reset by peer</code>                                                                                                                                                                                                                                               |
| AttemptedTLSWithNonTLSBackend | 525         | Platform*               | - logs with error <code>tls: first record does not look like a TLS handshake</code><br>- <code>backend_tls_handshake_failed</code> metric increments                                                                                                                                                      |
| HostnameMismatch              | 503         | Platform                | - logs with error <code>x509: certificate is valid for &lt;x&gt; not &lt;y&gt;</code><br>- <code>backend_invalid_id</code> metric increments                                                                                                                                                              |
| UntrustedCert                 | 526         | Platform                | - logs with an error prefix <code>x509: certificate signed by unknown authority</code><br>- <code>backend_invalid_tls_cert</code> metric increments                                                                                                                                                       |
| RemoteFailedCertCheck         | 496         | Platform                | logs with error remote <code>error: tls: bad certificate</code>                                                                                                                                                                                                                                           |
| ContextCancelled              | 499         | Client/App              | logs with error <code>context canceled</code><br><br> <b>Note:</b> This status code is never returned to clients, only logged, as it occurs when the downstream client closes the connection before Gorouter responds. |
| RemoteHandshakeFailure        | 525         | Platform                | - logs with error remote <code>error: tls: handshake failure</code><br>- <code>backend_tls_handshake_failed</code> metric increments                                                                                                                                                                      |

\*Note: any platform issue could be the result of a misconfiguration

For each of the above errors, there will be a `backend-endpoint-failure` log line in `gorouter.log` and an error message in `gorouter.err.log`. Additionally, the `access.log` will record the request status codes.

## Troubleshooting Ops Manager for VMware vSphere

Page last updated:

This guide provides help with diagnosing and resolving issues that are specific to [Pivotal Cloud Foundry](#) (PCF) deployments on VMware vSphere.

For infrastructure-agnostic troubleshooting help, refer to [Diagnosing Problems in PCF](#).

### Common Issues

The following sections list common issues you might encounter and possible resolutions.

#### PCF Installation Fails

If you modify the vCenter Statistics Interval Duration setting from its default setting of 5 minutes, the PCF installation might fail at the MicroBOSH deployment stage, and the logs might contain the following error message: `The specified parameter is not correct, interval`. This failure happens because Ops

Manager expects a default value of 5 minutes, and the call to this method fails when the retrieved value does not match the expected default value.

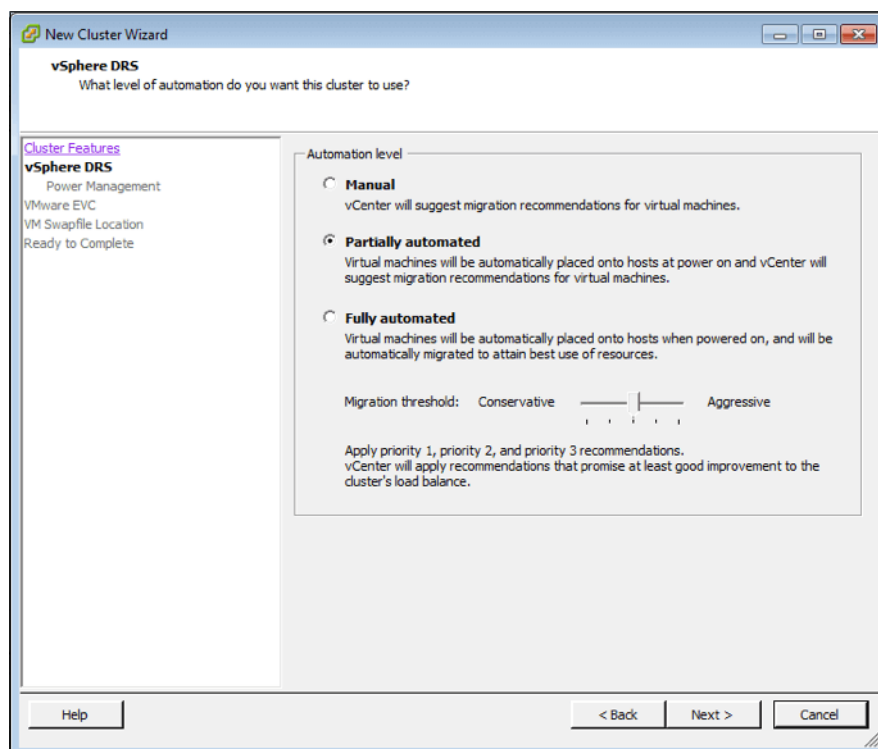
To resolve this issue, launch vCenter, navigate to **Administration > vCenter Server Settings > Statistics**, and reset the vCenter Statistics Interval Duration setting to 5 minutes.

#### BOSH Automated Installation Fails

Before starting an Pivotal Application Service (PAS) deployment, you must set up and configure a vSphere cluster.

If you enable vSphere DRS (Distributed Resource Scheduler) for the cluster, you must set the Automation level to **Partially automated** or **Fully automated**.

If you set the Automation level to **Manual**, the BOSH automated installation will fail with a `power_on_vm` error when BOSH attempts to create virtual VMs.



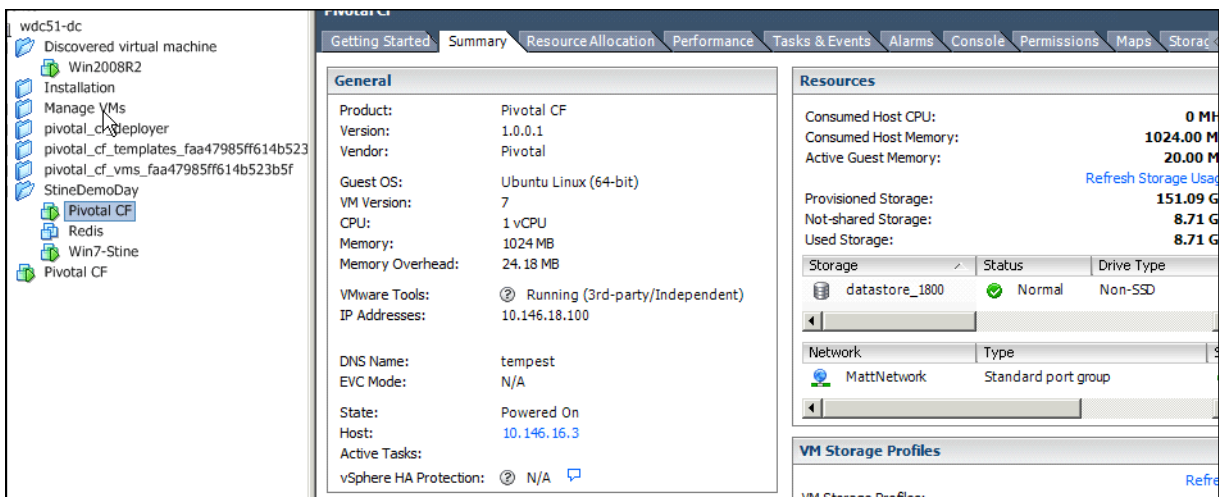
#### Ops Manager Loses Its IP Address After HA or Reboot

Ops Manager can lose its IP address and use DHCP due to an issue in the open source version of VMware Tools. For more information to troubleshoot this issue, see [IP is not Getting Assigned in vSphere after Ops Manager Restart](#) in the Pivotal Support Knowledge Base.

## Cannot Connect to the OVF in a Browser

If you deployed the OVF file but cannot connect to in a browser, check that the network settings you entered in the wizard are correct.

1. Access the PCF installation VM using the vSphere Console. If your network settings are misconfigured, you will not be able to SSH into the installation VM.
2. Log in using the credentials you provided when you imported the PCF .ova in vCenter.
3. Confirm that the network settings are correct by checking that the ADDRESS, NETMASK, GATEWAY, and DNS-NAMESERVERS entries are correct in `/etc/network/interfaces`.
4. If any of the settings are incorrect, run `sudo vi /etc/network/interfaces` and correct the incorrect entries.
5. In vSphere, navigate to the **Summary** tab for the VM and confirm that the network name is correct.



6. If the network name is incorrect, right click on the VM, select **Edit Settings > Network adapter 1**, and select the correct network.
7. Reboot the installation VM.

## Installation Fails with Failed Network Connection

If you experience a communication error while installing Ops Manager or MicroBOSH Director, check the following settings.

- Ensure that the routes are not blocked. vSphere environments use [NSX](#) for firewall and NAT/SNAT translation and load balancing. All communication between PCF VMs and vCenter or ESXi hosts route through the NSX firewall and are blocked by default.
- Open port 443. Ops Manager and MicroBOSH Director VMs require access to vCenter and all ESX through port 443.
- Allocate more IP addresses. BOSH requires that you allocate a sufficient number of additional dynamic IP addresses when configuring a reserved IP address range during installation. BOSH uses these IP addresses during installation to compile and deploy VMs, install PAS, and connect to services. We recommend that you allocate at least 36 dynamic IP addresses when deploying Ops Manager and PAS.

## Insufficient External Database Permissions

Upgrade issues can be caused when the external database user used for the network policy DB is given insufficient permissions. To avoid this upgrade issue, ensure that the networkpolicyserver database user has the `ALL PRIVILEGES` permission.