# Dell EMC Ready Bundle for Red Hat OpenStack Platform

## Deploying Pivotal Cloud Foundry 1.11
## Version 10.0.1

Dell EMC Converged Platforms and Solutions

# Contents

List of Figures....................iv

Trademarks....................6
Notes, Cautions, and Warnings....................7

Chapter 1: Executive Summary....................8
About the Dell EMC Ready Bundle for Red Hat OpenStack Platform....................9
About Pivotal Cloud Foundry on OpenStack....................9
About This Document....................9
Intended Audience....................10

Chapter 2: Pivotal Cloud Foundry Installation Preparation....................11
Prerequisites....................12
Update OpenStack Resource Quotas....................12
Add the DNS Name Server Address....................13

Chapter 3: Installation and Configuration....................14
Provision the OpenStack Infrastructure....................15
Log into OpenStack Horizon....................15
Create a Key Pair....................15
Configure Security....................16
Create an Ops Manager Image....................17
Launch the Ops Manager VM....................18
Associate a Floating IP Address....................19
Configure Ops Manager Director for OpenStack....................21
Access Ops Manager....................21
Complete the OpenStack Configuration Page....................23
Complete the Director Config Page....................24
Complete the Create Availability Zones Page....................25
Complete the Networks Page....................26
Complete the Assign AZs and Networks Page....................28
Complete the Ops Manager Director Installation....................28
Install and Configure Elastic Runtime....................29
Add Elastic Runtime to Ops Manager....................30
Assign Availability Zones and Networks....................31
Configure Elastic Runtime Domains....................32
Configure Networking....................33
Review Application Security Groups....................34
Configure UAA....................35
Configure Internal MySQL....................35
Enable Traffic to OpenStack Private Subnet....................35
Complete Elastic Runtime Installation....................36

Deploy JMX Bridge.......................................................................................... 37
Add JMX Bridge to Ops Manager.................................................................37
Assign Availability Zones and Networks.......................................................37
Configure JMX Provider..................................................................................37
Update Stemcell for JMX Provider............................................................... 38
Apply JMX Bridge Changes...........................................................................39
Find the JMX Provider IP Address............................................................... 39
Configure the Metrics IP Address..................................................................39
Complete JMX Bridge Installation..................................................................40

Chapter 4: Deploy a Sample Application............................................................ 41
Gather Credentials and API Endpoint Information.................................................42
Prepare to Deploy..........................................................................................42
Deploy a Sample Application..........................................................................43

Appendix A: Getting Help................................................................................... 45
Contacting Dell EMC.........................................................................................46
References........................................................................................................ 46
To Learn More.............................................................................................. 46

# List of Figures

Figure 1: Add the DNS Name Server Address....13

Figure 2: Horizon Login Screen....15

Figure 3: Create Key Pair....16

Figure 4: Create Security Group....16

Figure 5: Manage Rules.... 17

Figure 6: Add Access Rules.... 17

Figure 7: Create Image....18

Figure 8: Launch Instance.... 19

Figure 9: Instances.... 20

Figure 10: Manage Floating IP Associations....20

Figure 11: Associate Floating IP....20

Figure 12: Manage Floating IP Associations (Re-invoked)....21

Figure 13: Ops Manager Welcome Screen.... 22

Figure 14: Internal Authentication Screen.... 22

Figure 15: Access and Security Screen.... 23

Figure 16: OpenStack Management Console Config Page....24

Figure 17: Director Config Page....25

Figure 18: Availability Zones Page....26

Figure 19: Networks Page.... 26

Figure 20: Network Details Page....27

Figure 21: Create Networks Page.... 27

Figure 22: Assign Availability Zones....28

Figure 23: Ops Manager Install Error Message.... 29

Figure 24: Ops Manager Director Changes Applied Message....29

Figure 25: Ops Manager Director Change Log.... 29

Figure 26: Elastic Runtime Import Product Screen........................................................ 30

Figure 27: Ops Manager Add Product Screen.............................................................. 31

Figure 28: Ops Manager Product Added Screen.......................................................... 31

Figure 29: Elastic Runtime AZ and Network Assignments Page....................................32

Figure 30: Domains Page............................................................................................33

Figure 31: Generate RSA Certificate............................................................................34

Figure 32: Enable TCP Routing...................................................................................34

Figure 33: Floating IP Addresses................................................................................ 35

Figure 34: Allocate Floating IP Address.......................................................................36

Figure 35: Elastic Runtime Change Log.......................................................................36

Figure 36: JMX Bridge AZ and Network Assignments Page..........................................37

Figure 37: JMX Provider Page.................................................................................... 38

Figure 38: Stemcell Page............................................................................................ 38

Figure 39: JMX Provider Status...................................................................................39

Figure 40: Director Config Tab.................................................................................... 40

Figure 41: Application Pushed Output..........................................................................43

Figure 42: Application URL Output..............................................................................43

Figure 43: Application Opened.................................................................................... 44

# Trademarks

Copyright © 2014-2017 Dell Inc. or its subsidiaries. All rights reserved.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Red Hat®, Red Hat Enterprise Linux®, and Ceph are trademarks or registered trademarks of Red Hat, Inc., registered in the U.S. and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. Oracle® and Java® are registered trademarks of Oracle Corporation and/or its affiliates.

DISCLAIMER: The OpenStack® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries, and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community.

# Notes, Cautions, and Warnings

✎ A **Note** indicates important information that helps you make better use of your system.

△ A **Caution** indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ A **Warning** indicates a potential for property damage, personal injury, or death.

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

# Chapter 1

## Executive Summary

**Topics:**

- *About the Dell EMC Ready Bundle for Red Hat OpenStack Platform*
- *About Pivotal Cloud Foundry on OpenStack*
- *About This Document*
- *Intended Audience*

In order to meet the demands put on an organization by customers who require the agility, efficiency, and innovation of cloud-based services and applications, developers need a way to build, deploy, and manage applications in a containerized format, and deploy them in a cloud native manner.

IT Operations needs to be able to provide this with a secure, enterprise-grade environment that can have policy based control for automation of cluster services, scheduling and orchestration of the applications. By incorporating a Pivotal Cloud Foundry cloud native platform and OpenStack virtual machine clusters, these demands can be met quickly and effectively.

## About the Dell EMC Ready Bundle for Red Hat OpenStack Platform

The Dell EMC Ready Bundle for Red Hat OpenStack Platform is an integrated hardware and software solution for OpenStack cloud that has been jointly designed and validated by Dell EMC and Red Hat. The Ready Bundle enables organizations to easily and rapidly deploy a highly reliable, optimized, and scalable Infrastructure as a Service (IaaS) cloud solution.

The Ready Bundle architecture is built on Dell EMC PowerEdge servers for the Controller, Compute, and Storage nodes, with Red Hat OpenStack Platform and Red Hat Ceph Storage software, plus a number of validated extensions to the core architecture to enable capabilities such as Platform as a Service (PaaS), Containers as a Service (CaaS), and cloud native development and operations. This release of the Ready Bundle is based on Red Hat OpenStack Platform 10 (RHOSP 10), which is the OpenStack release called Newton.

## About Pivotal Cloud Foundry on OpenStack

Pivotal Cloud Foundry 1.11 is a Platform as a Service (PaaS) product. Its developer-centric approach enables developers to create and deploy applications with more predictability, greater ease, and less operator intervention. It manages deployments and provides application scalability services.

Integrating Pivotal Cloud Foundry with OpenStack allows your organization to leverage existing operational techniques and organizational policies, adding a layer of deployment and redeployment flexibility not common in non-virtual deployments. This solution provides an example demonstrating how to install and configure Pivotal Cloud Foundry 1.11, for a test lab or proof-of-concept, on a robust OpenStack infrastructure.

A production-ready reference architecture can be found at the Pivotal website, at *https://docs.pivotal.io/pivotalcf/refarch/openstack/openstack_ref_arch.html*.

## About This Document

This document describes installing and configuring Pivotal Cloud Foundry on the Dell EMC Ready Bundle for Red Hat OpenStack Platform. See *Installation and Configuration* on page 14.

It also describes the following procedures:

- *Pivotal Cloud Foundry Installation Preparation* on page 11
- *Deploy a Sample Application* on page 41

This document contains code and configuration samples in mono-space fonts. While it is tempting for the user to copy and paste those values from this document into their OpenStack environment, it is inadvisable and not supported. While we make every effort to ensure that the documentation is correct and complete, documents rendered via some client applications make unpredictable changes to the actual spacing of the data elements, and lose fidelity to what a proper code or configuration setting should actually be to work properly. We see very impactful changes, for example, between the Firefox PDF display and the Adobe Acrobat Reader PDF display.

Copy and paste from this document only with full understanding of the necessary formatting changes that you'll have to make. We have made efforts to provide online verbatim copies of the essential data, as well as pointing the user to appropriate external documentation to achieve the proper formatting.

## Intended Audience

This technical guide shows the administrator how to build and deploy Pivotal Cloud Foundry in their Dell EMC Ready Bundle for Red Hat OpenStack Platform. The end user is not directly addressed in this document.

Find out more about installing and deploying Pivotal Cloud Foundry by accessing the Pivotal documentation at the Pivotal website: *https://docs.pivotal.io/pivotalcf/1-11/installing/*.

# Chapter 2

# Pivotal Cloud Foundry Installation Preparation

**Topics:**

- *Prerequisites*
- *Update OpenStack Resource Quotas*
- *Add the DNS Name Server Address*

This chapter describes the prerequisites that must be satisfied, and the OpenStack environment verification procedures to perform, in order to install Pivotal Cloud Foundry on the Dell EMC Ready Bundle for Red Hat OpenStack Platform.

## Prerequisites

This topic provides a comprehensive list of prerequisites to be verified in your Dell EMC Ready Bundle for Red Hat OpenStack Platform environment **prior** to deploying Pivotal Cloud Foundry.

For detailed information, see *https://docs.pivotal.io/pivotalcf/customizing/openstack.html*.

Prerequisites include:

- Red Hat OpenStack Platform version 10
- A DNS server that has full forward and reverse lookup support, preferably outside the OpenStack environment
- A dedicated project in the default OpenStack domain
- Installation of Pivotal Cloud Foundry requires an administrative user with full rights in the OpenStack environment
- Before installing Pivotal Cloud Foundry, public and private networks for the Pivotal tenants must be created within the OpenStack environment
- Pivotal Cloud Foundry requires a dedicated private network with a full /24 addressable IP address range in a single subnet

In addition, the following procedures must be performed prior to deploying Red Hat OpenStack Platform:

- *Update OpenStack Resource Quotas* on page 12
- *Add the DNS Name Server Address* on page 13

## Update OpenStack Resource Quotas

To update OpenStack resource quotas assigned for deploying Pivotal Cloud Foundry in the OpenStack Overcloud:

1. Obtain user login credentials to the Director Node VM from your OpenStack administrator.

   **Note:** These credentials were created during the OpenStack deployment.
2. Log into the Director Node VM using the user name and password you obtained in step *1* on page 12.
3. Change to the user's home directory:

   ```
   $ cd ~/
   ```
4. Source the OpenStack Overcloud:

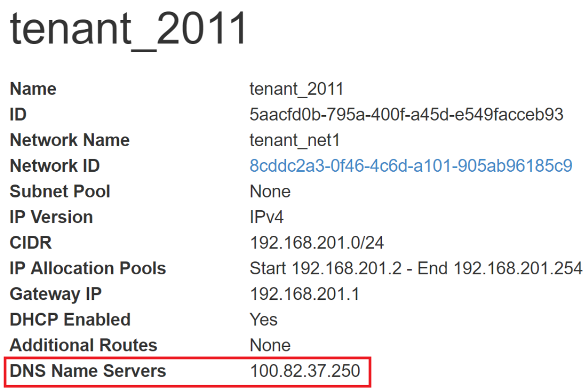
   ```
   $ source <overcloud>
   ```
5. Set the resource quotas:

   ```
   $ openstack quota set admin --cores 120 --instances 70 --volumes 30 \
     --ram 265280 --gigabytes 6500 --snapshots 50 --floating-ips 60 \
     --ports  100
   ```

## Add the DNS Name Server Address

To add your DNS name server address for Pivotal Cloud Foundry VM access to the private network:

1. Configure the DNS name server as in *Figure 1: Add the DNS Name Server Address* on page 13.



tenant_2011

| | |
|---|---|
| **Name** | tenant_2011 |
| **ID** | 5aacfd0b-795a-400f-a45d-e549facceb93 |
| **Network Name** | tenant_net1 |
| **Network ID** | 8cddc2a3-0f46-4c6d-a101-905ab96185c9 |
| **Subnet Pool** | None |
| **IP Version** | IPv4 |
| **CIDR** | 192.168.201.0/24 |
| **IP Allocation Pools** | Start 192.168.201.2 - End 192.168.201.254 |
| **Gateway IP** | 192.168.201.1 |
| **DHCP Enabled** | Yes |
| **Additional Routes** | None |
| **DNS Name Servers** | 100.82.37.250 |

**Figure 1: Add the DNS Name Server Address**

2. Make sure that the DNS server:

   a. Allows zone transfers to any server

   b. Allows both nonsecure *and* secure dynamic updates

# Chapter 3

## Installation and Configuration

**Topics:**

- *Provision the OpenStack Infrastructure*
- *Configure Ops Manager Director for OpenStack*
- *Install and Configure Elastic Runtime*
- *Deploy JMX Bridge*

This chapter provides instructions for installing Pivotal Cloud Foundry on the Dell EMC Ready Bundle for Red Hat OpenStack Platform.

# Provision the OpenStack Infrastructure

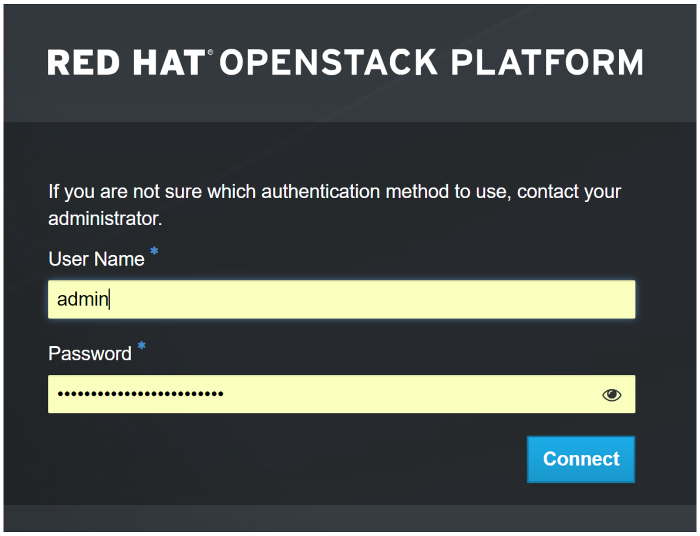
Perform the following procedures, in the order listed, to provision the OpenStack infrastructure for Pivotal Cloud Foundry:

1. *Log into OpenStack Horizon* on page 15
2. *Create a Key Pair* on page 15
3. *Configure Security* on page 16
4. *Create an Ops Manager Image* on page 17
5. *Launch the Ops Manager VM* on page 18
6. *Associate a Floating IP Address* on page 19

For detailed information about these steps, see *https://docs.pivotal.io/pivotalcf/customizing/openstack-setup.html*.

## Log into OpenStack Horizon

1. Log In to the OpenStack Horizon Dashboard as an *admin* user. See *Figure 2: Horizon Login Screen* on page 15.



RED HAT® OPENSTACK PLATFORM

If you are not sure which authentication method to use, contact your administrator.

User Name *: admin

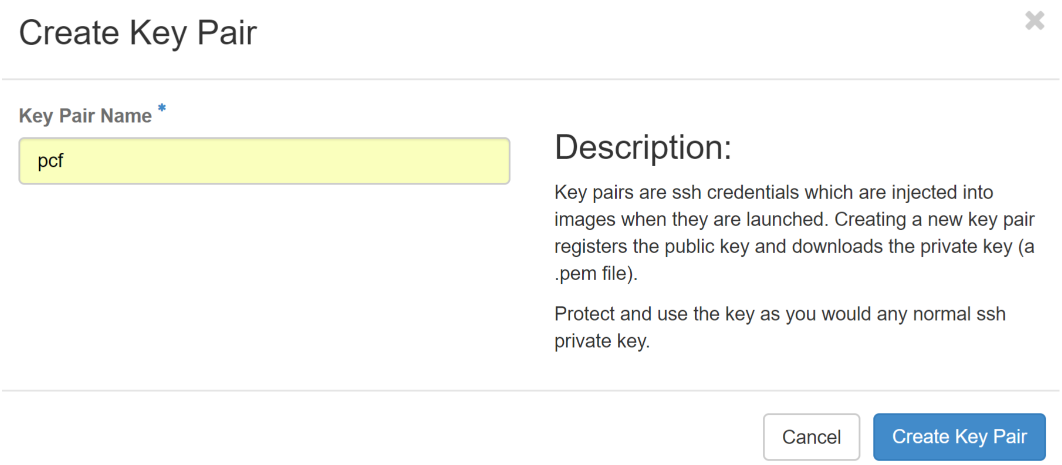
Password *: ••••••••••••••••••••••••

**Figure 2: Horizon Login Screen**

## Create a Key Pair

To create a key pair:

1. In the OpenStack dashboard's left-hand pane, navigate to **Project > Compute > Access & Security**.
2. Select the **Key Pairs** tab. See *Figure 3: Create Key Pair* on page 16.



Create Key Pair

Key Pair Name *: pcf

Description:

Key pairs are ssh credentials which are injected into images when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file).

Protect and use the key as you would any normal ssh private key.

**Figure 3: Create Key Pair**

3. Click on **Create Key Pair**.
4. Enter a **Key Pair Name**, and then click on **Create Key Pair**.

   **Note:** Our example uses the key pair name, *pcf*.

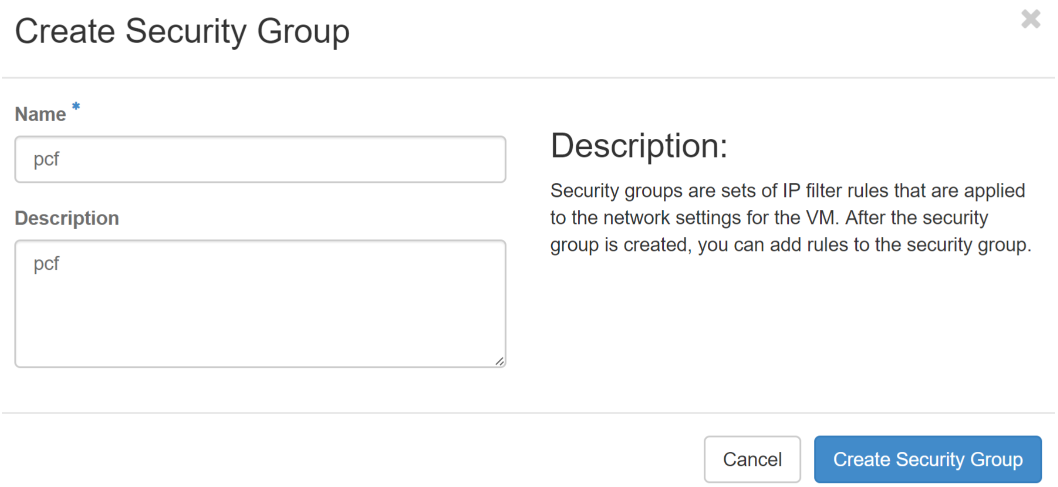
5. Save the *pcf.pem* **key pair PEM file**.

## Configure Security

To configure security:

1. In the left-hand pane, click on **Access & Security** to refresh the page.
2. Select the **Security Groups** tab.
3. Click on **Create Security Group** to create a group. See *Figure 4: Create Security Group* on page 16.

   **Note:** Our example uses the group name, *pcf*.



Create Security Group

Name *: pcf

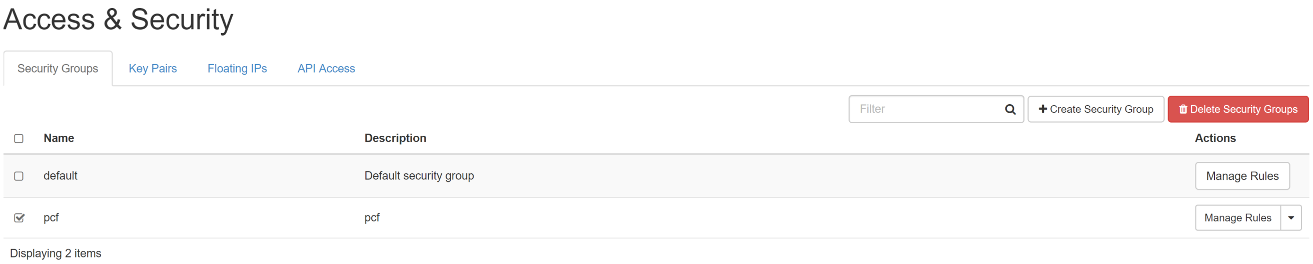
Description: pcf

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.

**Figure 4: Create Security Group**

4. Select the checkbox for the Security Group, and then click on **Manage Rules**. See *Figure 5: Manage Rules* on page 17.



| □ | Name | Description | Actions |
|---|---|---|---|
| □ | default | Default security group | Manage Rules |
| ☑ | pcf | pcf | Manage Rules |

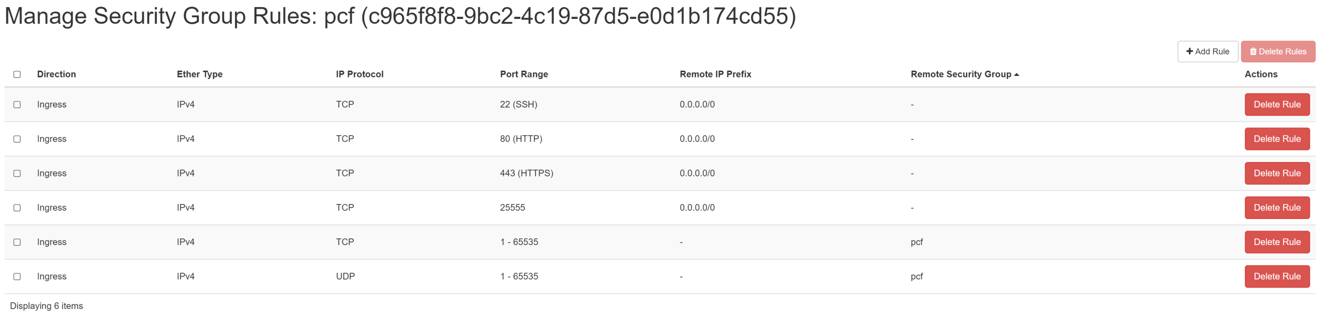
Displaying 2 items

**Figure 5: Manage Rules**

5. Add the access rules for the following types of network traffic:

   - HTTP
   - HTTPS
   - ICMP
   - SSH
   - TCP
   - UDP

   See *Figure 6: Add Access Rules* on page 17.



Manage Security Group Rules: pcf (c965f8f8-9bc2-4c19-87d5-e0d1b174cd55)

| □ | Direction | Ether Type | IP Protocol | Port Range | Remote IP Prefix | Remote Security Group | Actions |
|---|---|---|---|---|---|---|---|
| □ | Ingress | IPv4 | TCP | 22 (SSH) | 0.0.0.0/0 | - | Delete Rule |
| □ | Ingress | IPv4 | TCP | 80 (HTTP) | 0.0.0.0/0 | - | Delete Rule |
| □ | Ingress | IPv4 | TCP | 443 (HTTPS) | 0.0.0.0/0 | - | Delete Rule |
| □ | Ingress | IPv4 | TCP | 25555 | 0.0.0.0/0 | - | Delete Rule |
| □ | Ingress | IPv4 | TCP | 1 - 65535 | - | pcf | Delete Rule |
| □ | Ingress | IPv4 | UDP | 1 - 65535 | - | pcf | Delete Rule |

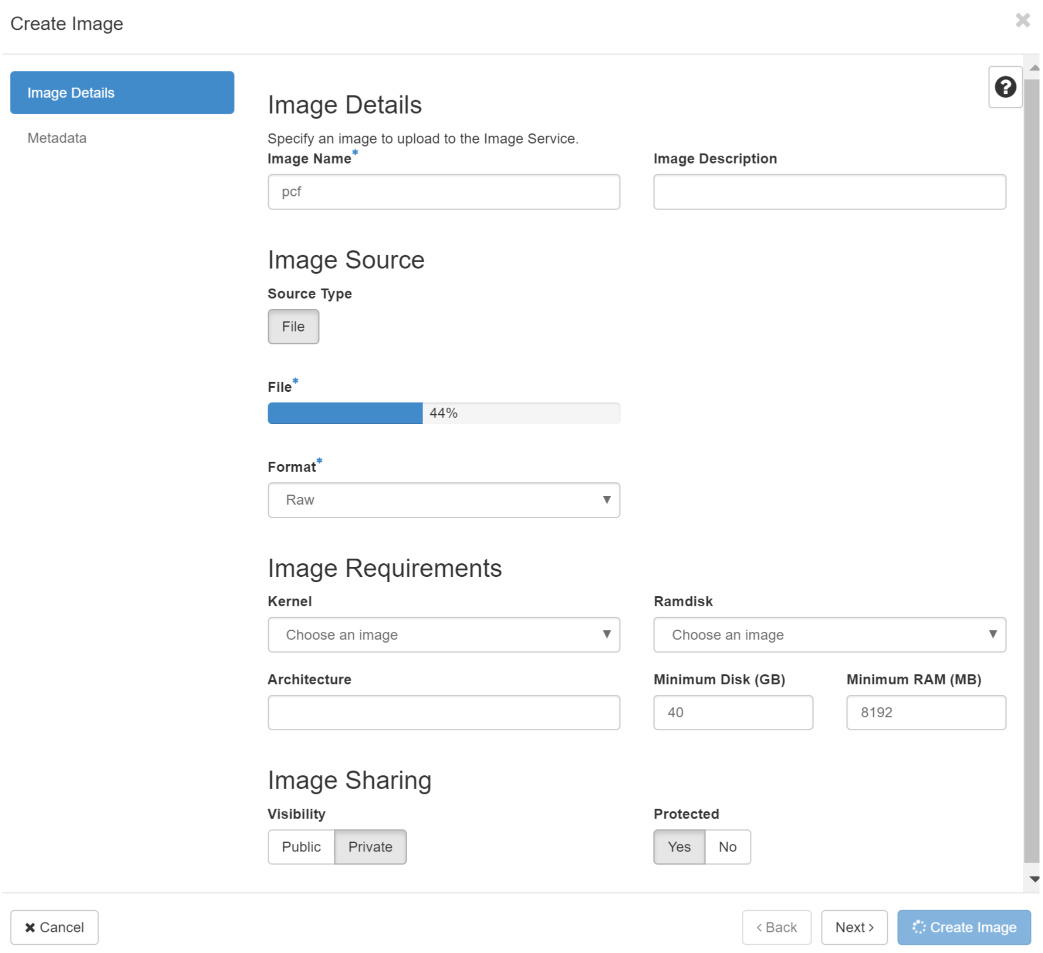
Displaying 6 items

**Figure 6: Add Access Rules**

## Create an Ops Manager Image

To create an Ops Manager image:

1. Create an account on *Pivotal Network*.
2. Download the **Pivotal Cloud Foundry Ops Manager for OpenStack** image file, `pcf-openstack-1.11.5.raw`.
3. In the left-hand pane of your OpenStack dashboard, click on **Project > Compute > Images**.
4. Click on **Create Image** to invole the *Create Image* page. See *Figure 7: Create Image* on page 18.



Create Image

Image Details

Specify an image to upload to the Image Service.

Image Name* pcf

Image Description

Image Source

Source Type: File

File* 44%

Format* Raw

Image Requirements

Kernel: Choose an image

Ramdisk: Choose an image

Architecture

Minimum Disk (GB): 40

Minimum RAM (MB): 8192

Image Sharing

Visibility: Public | Private (selected)

Protected: Yes (selected) | No

**Figure 7: Create Image**

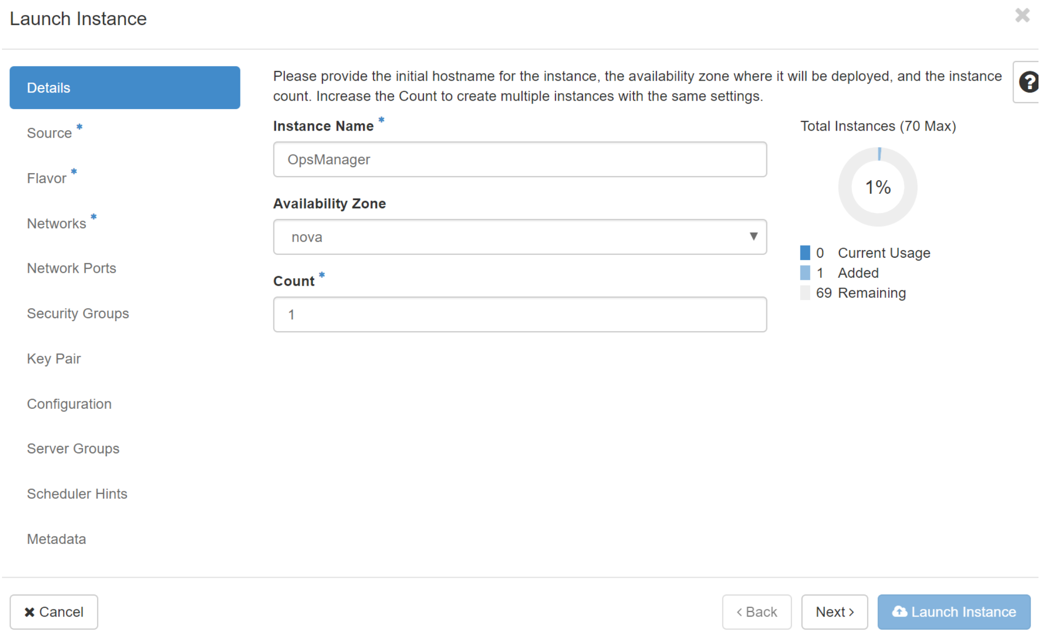
5. Complete the *Create Image* page with the following information:

   - **Image Name** — Enter *pcf*.
   - **Image Source** — Click on **Choose File**, and then browse to and select the *image file that you downloaded*.
   - **Format** — Select *Raw*.
   - **Minimum Disk (GB)** — Enter *40*.
   - **Minimum RAM (MB)** — Enter *8192*.
   - **Visibility** — Select *Private*.
   - **Protected** — Select *yes*.

## Launch the Ops Manager VM

To launch the Ops Manager VM:

1. In the left-hand pane of your OpenStack dashboard, click on **Project > Compute > Instances**.
2. Click on **Launch Instance**. See *Figure 8: Launch Instance* on page 19.



Launch Instance

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 * OpsManager

Availability Zone nova

Count * 1

Total Instances (70 Max)

1%

0 Current Usage
1 Added
69 Remaining

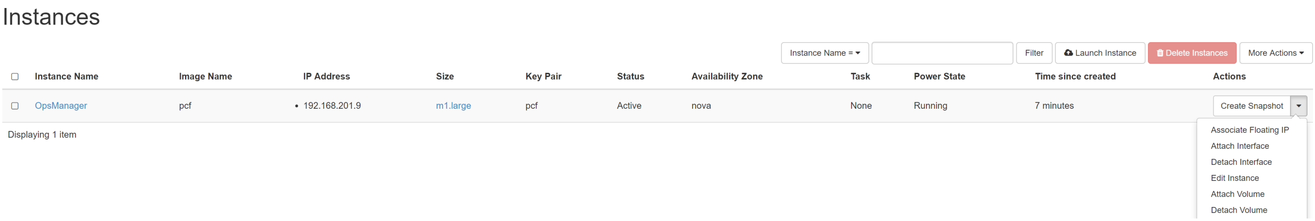
**Figure 8: Launch Instance**

3. Complete the **Details** tab with the information below:
   - **Instance Name** — *OpsManager*
   - **Availability Zone** — Use the drop-down menu to select an appropriate *availability zone*
   - **Count** — *1*
4. Complete the **Source** tab with the information below:
   - **Select Boot Source** — *Image*
   - **Create New Volume** — *No*
   - Select the *pcf* image
5. Complete the **Flavor** tab with the information below:
   - Select the *m1.large* flavor
6. Complete the **Networks** tab with the information below:
   - Select the *private tenant* network
7. Complete the **Security Groups** tab with the information below:
   - Select the *pcf* security group
8. Complete the **Key Pair** tab with the information below:
   - Select the *pcf* key pair
9. Click on **Launch Instance**.

## Associate a Floating IP Address

To associate a floating IP address with the Ops Manager Instance:

1. In the left-hand pane of your OpenStack dashboard, click on **Project > Compute > Instances**. See *Figure 9: Instances* on page 20.

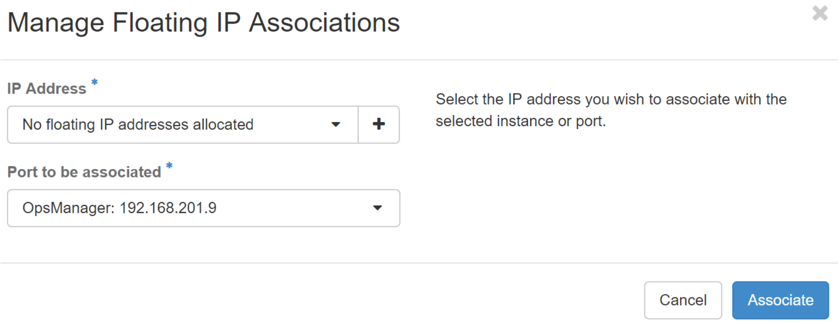


| □ | Instance Name | Image Name | IP Address | Size | Key Pair | Status | Availability Zone | Task | Power State | Time since created | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | OpsManager | pcf | • 192.168.201.9 | m1.large | pcf | Active | nova | None | Running | 7 minutes | Create Snapshot |

Displaying 1 item

**Figure 9: Instances**

2. Wait until the *Power State* of the Ops Manager instances displays **Running**.
3. Select the **Ops Manager** checkbox.
4. Click the **Actions** drop-down menu, and then select **Associate Floating IP** to invoke the *Manage Floating IP Associations* page. See *Figure 10: Manage Floating IP Associations* on page 20.



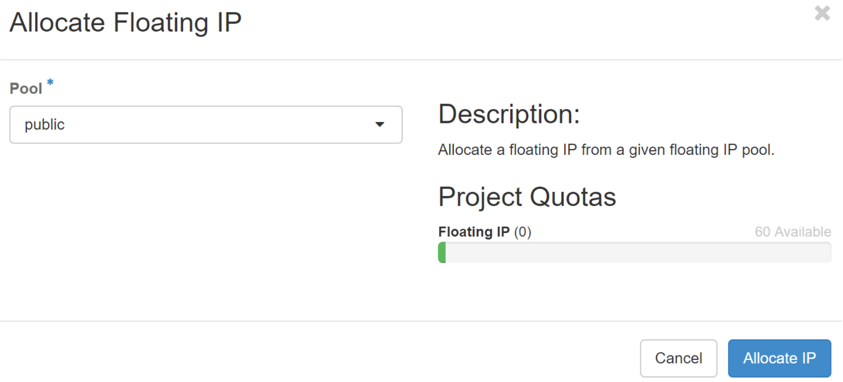
IP Address *
No floating IP addresses allocated

Port to be associated *
OpsManager: 192.168.201.9

Select the IP address you wish to associate with the selected instance or port.

**Figure 10: Manage Floating IP Associations**

5. Under *IP Address*, click on the **plus sign** (**+**) to invoke the Allocate Floating IP page. See *Figure 11: Associate Floating IP* on page 20.



Pool *
public

Description:

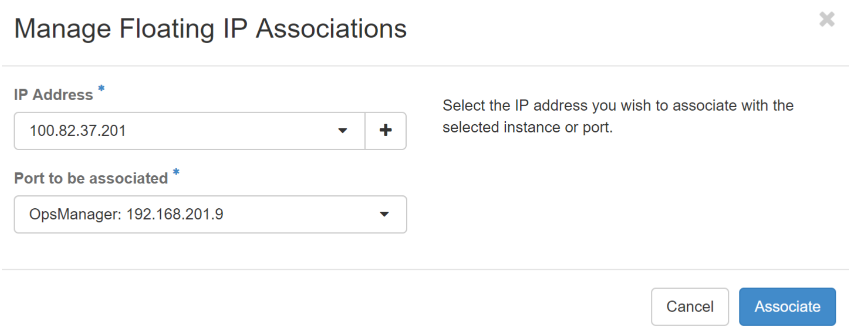
Allocate a floating IP from a given floating IP pool.

Project Quotas

Floating IP (0) 60 Available

**Figure 11: Associate Floating IP**

6. Under *Pool*, select an **IP Pool** and then click on **Allocate IP** to re-invoke the Manage Floating IP Associations page. See *Figure 12: Manage Floating IP Associations (Re-invoked)* on page 21.



Manage Floating IP Associations

IP Address *

100.82.37.201

Select the IP address you wish to associate with the selected instance or port.

Port to be associated *

OpsManager: 192.168.201.9

**Figure 12: Manage Floating IP Associations (Re-invoked)**

7. Under *Port to be associated*, select your **Ops Manager instance**, and then click on **Associate**.

## Configure Ops Manager Director for OpenStack

Perform the following procedures, in the order listed, to configure Ops Manager for OpenStack:

1. Create an (A) Record DNS entry for the Ops Manager floating IP address.
   a. Allow both forward and reverse lookups.
2. *Access Ops Manager* on page 21
3. *Complete the OpenStack Configuration Page* on page 23
4. *Complete the Director Config Page* on page 24
5. *Complete the Create Availability Zones Page* on page 25
6. *Complete the Networks Page* on page 26
7. *Complete the Assign AZs and Networks Page* on page 28
8. *Complete the Ops Manager Director Installation* on page 28

For detailed information about these steps, see *https://docs.pivotal.io/pivotalcf/customizing/openstack-om-config.html*.

### Access Ops Manager

To access Pivotal Ops Manager:

1. In a web browser, navigate to the IP address you associated to the Ops Manager instance in *Associate a Floating IP Address* on page 19. See *Figure 13: Ops Manager Welcome Screen* on page 22.

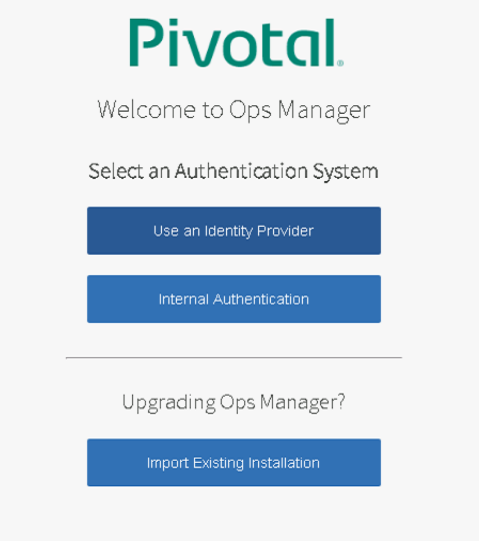
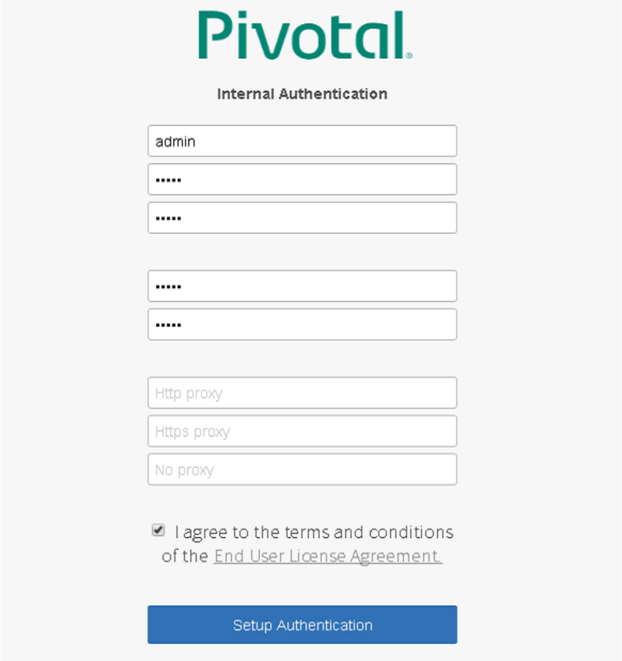


**Figure 13: Ops Manager Welcome Screen**

2. When Ops Manager starts for the first time, you must choose **Internal Authentication** where Pivotal Cloud Foundry (PCF) maintains your user database. See *Figure 14: Internal Authentication Screen* on page 22.



admin

•••••

•••••

•••••

•••••

☑ I agree to the terms and conditions of the End User License Agreement.

**Figure 14: Internal Authentication Screen**

3. When redirected to the **Internal Authentication** page, you must complete the following steps:
   a) Enter a **Username**, **Password**, and **Password Confirmation** to create an Admin user.
   b) Enter a **Decryption Passphrase** and the **Decryption Passphrase Confirmation**.

   **Note:** This passphrase encrypts the Ops Manager data store, and *is not recoverable*.

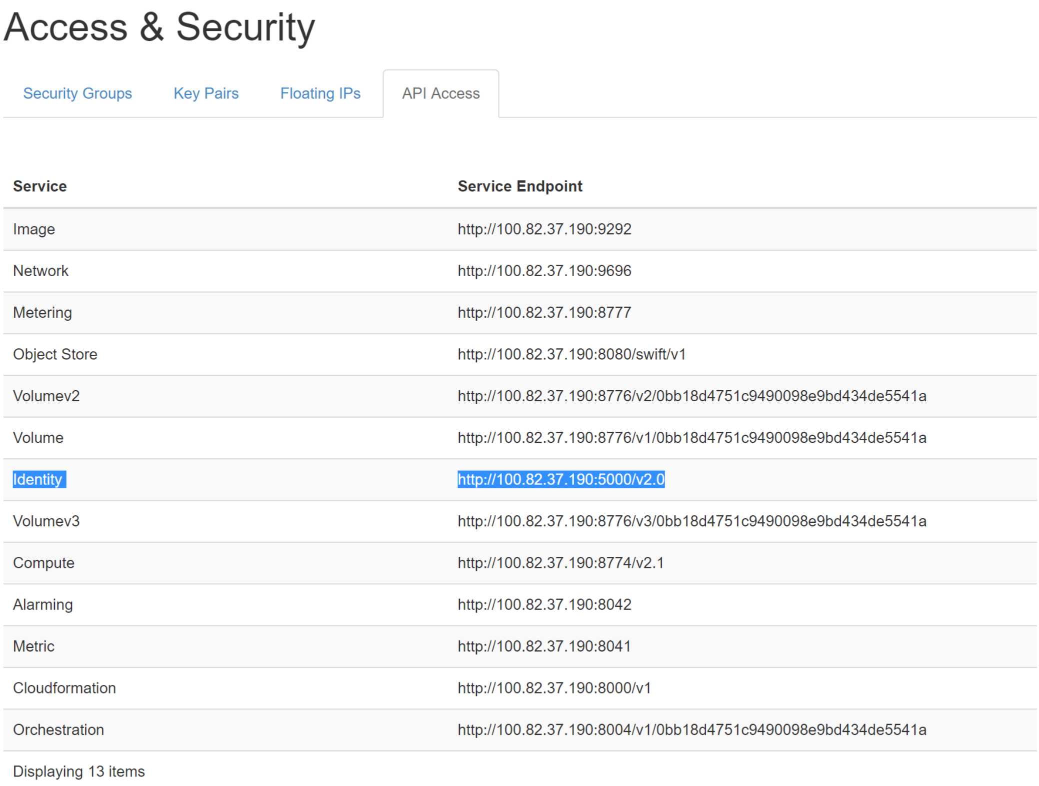
   c) Read the **End User License Agreement**, and then click on the **checkbox** to accept the terms.
   d) Click on **Setup Authentication**.
4. Enter the *Admin* username and password you created in step *3* on page 22.

5. Click on **SIGN IN** to access Ops Manager.

## Complete the OpenStack Configuration Page

To complete the *OpenStack Configuration* Page:

1. In the left-hand pane of your OpenStack dashboard, click **Project > Compute > Access & Security**. See *Figure 15: Access and Security Screen* on page 23.



Access & Security

| Service | Service Endpoint |
|---|---|
| Image | http://100.82.37.190:9292 |
| Network | http://100.82.37.190:9696 |
| Metering | http://100.82.37.190:8777 |
| Object Store | http://100.82.37.190:8080/swift/v1 |
| Volumev2 | http://100.82.37.190:8776/v2/0bb18d4751c9490098e9bd434de5541a |
| Volume | http://100.82.37.190:8776/v1/0bb18d4751c9490098e9bd434de5541a |
| Identity | http://100.82.37.190:5000/v2.0 |
| Volumev3 | http://100.82.37.190:8776/v3/0bb18d4751c9490098e9bd434de5541a |
| Compute | http://100.82.37.190:8774/v2.1 |
| Alarming | http://100.82.37.190:8042 |
| Metric | http://100.82.37.190:8041 |
| Cloudformation | http://100.82.37.190:8000/v1 |
| Orchestration | http://100.82.37.190:8004/v1/0bb18d4751c9490098e9bd434de5541a |

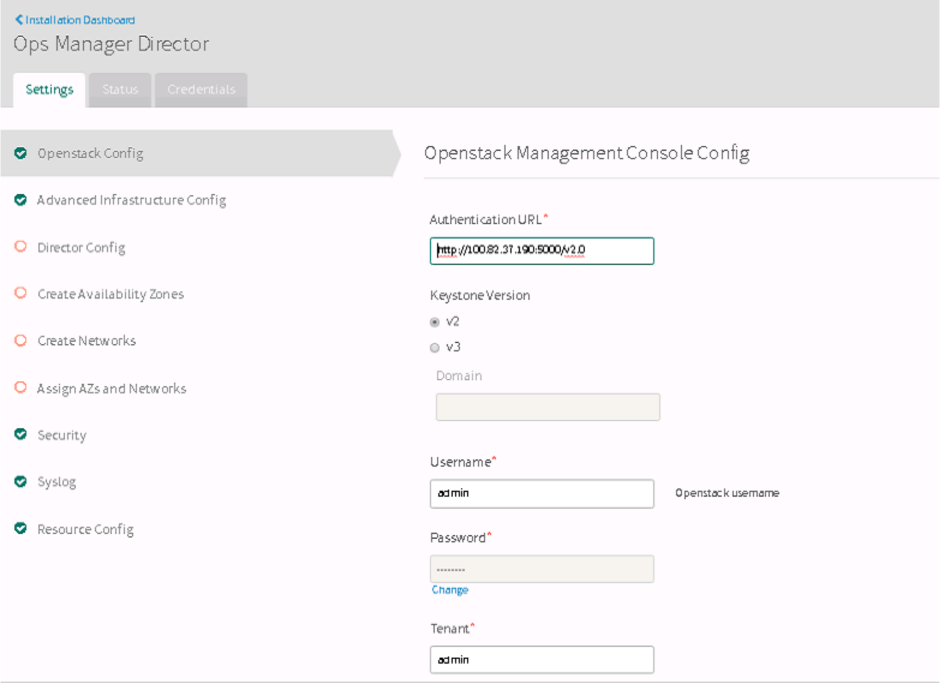
Displaying 13 items

**Figure 15: Access and Security Screen**

2. Select the **API Access** tab.
3. Record the **Service Endpoint** for the Identity service.

   **Note:** You will use this Service Endpoint as the authentication URL for Ops Manager in step *6* on page 24.

4. In the PCF Ops Manager Installation Dashboard, click on the **Ops Manager Director tile**.
5. Select **OpenStack Config**. See *Figure 16: OpenStack Management Console Config Page* on page 24.



Openstack Management Console Config

Authentication URL*: http://100.82.37.190:5000/v2.0

Keystone Version: ● v2 ○ v3

Domain:

Username*: admin — Openstack username

Password*: ••••••••

Tenant*: admin

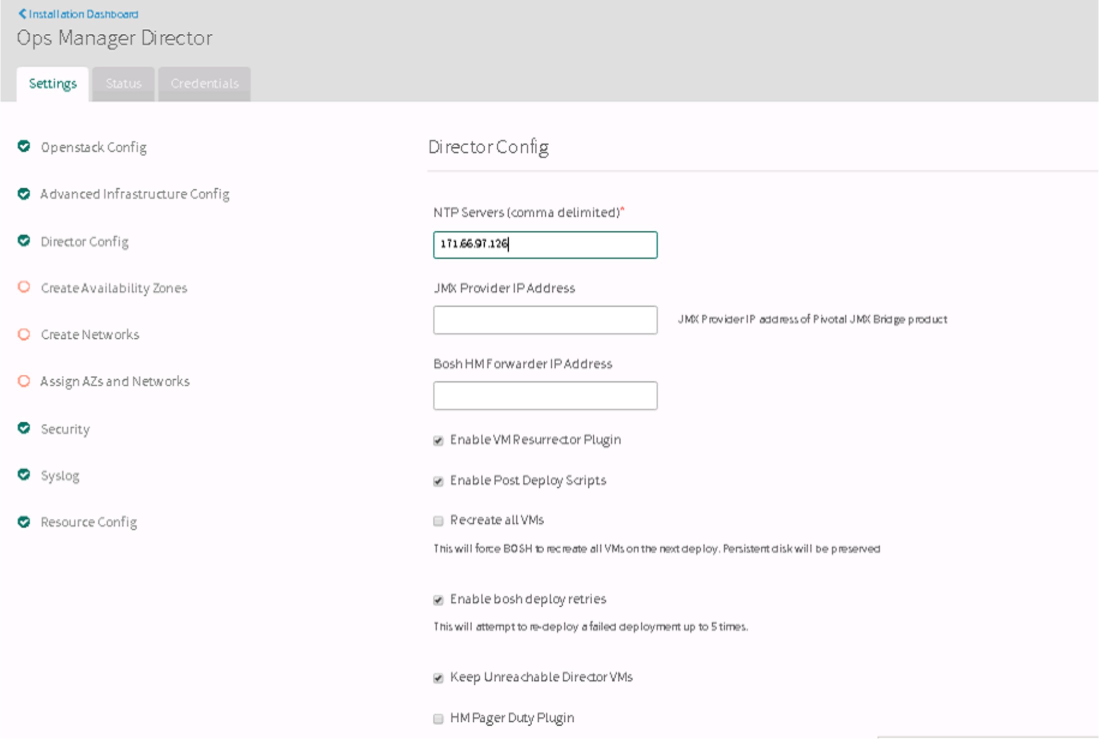
**Figure 16: OpenStack Management Console Config Page**

6. Complete the OpenStack Management Console Config page with the information below:
    - **Authentication URL** — Enter the *Service Endpoint for the Identity service* that you recorded in step *3* on page 23.
    - **Keystone Version** — Choose a *Keystone version*.
    - **Username** — Enter your *OpenStack Horizon username*.
    - **Password** — Enter your *OpenStack Horizon password*.
    - **Tenant** — Enter your *OpenStack tenant/project name*.
    - **Region** — Enter *regionOne*
    - **Ignore Server Availability Zone** — *Do not select*.
    - **Security Group Name** — Enter *pcf*. You created this Security Group in *Configure Security* on page 16.
    - **Key Pair Name** — Enter *pcf*. You created this key pair in *Create a Key Pair* on page 15.
    - **SSH Private Key** — Perform these steps:
        - In a text editor, open the *pcf.pem* **key pair file** that you downloaded in *Create a Key Pair* on page 15.
        - Copy and paste the contents of the key pair file into the field.
    - **API SSL Certificate** — *Leave this blank*, since OpenStack has not configured API SSL termination.
    - **Disable DHCP** — *Do not select*.
7. Click on **Save**.

## Complete the Director Config Page

To complete the Director Configuration Page:

1. In Ops Manager, select **Director Config**.See *Figure 17: Director Config Page* on page 25



Director Config

NTP Servers (comma delimited)*

171.66.97.126

JMX Provider IP Address

JMX Provider IP address of Pivotal JMX Bridge product

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

☐ HM Pager Duty Plugin

**Figure 17: Director Config Page**

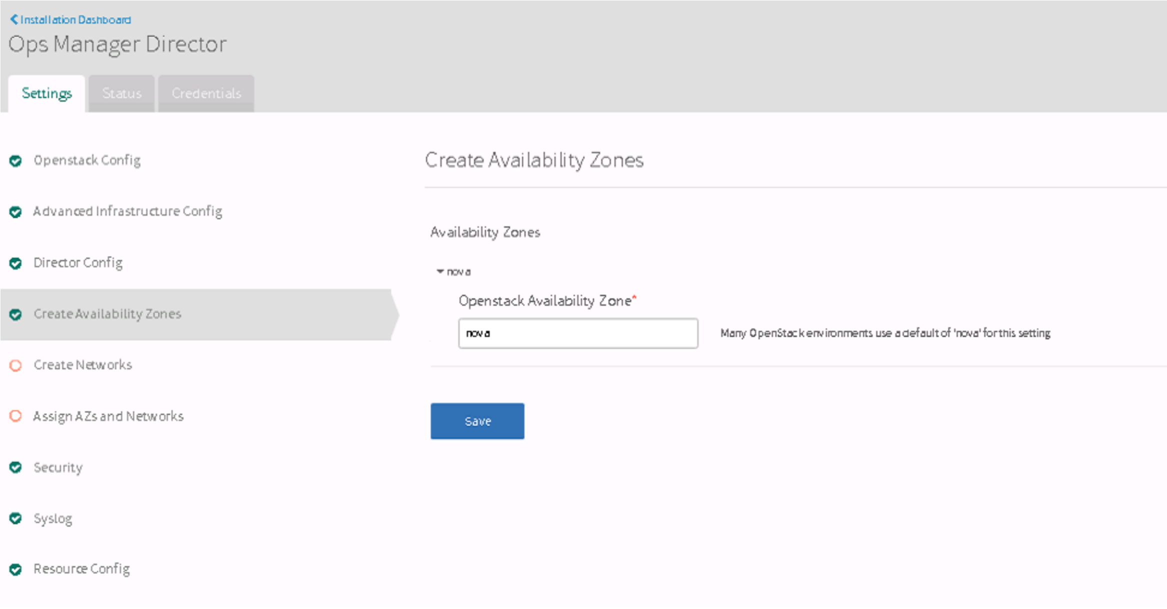
2. Complete the Director Config page with the information below:
   - **NTP Servers (comma delimited)** — Enter *one or more NTP servers*.
   - **JMX Provider IP Address** — *Leave this blank*.
   - **Bosh HM Forwarder IP Address** — *Leave this blank*.
   - **Enable VM Resurrector Plugin** — *Select* to enable the Ops Manager Resurrector functionality, and to increase Elastic Runtime availability.
   - **Enable Post Deploy Scripts** — *Select* to run a post-deployment script that allows the job to execute additional commands against a deployment.
   - **Recreate all VMs** — *Select* to force BOSH to recreate all VMs on the next deploy.

     **Note:** This process does not destroy any persistent disk data.
   - **Enable bosh deploy retries** — *Select* if you want Ops Manager to retry failed BOSH operations up to five times.
   - **Keep Unreachable Director VMs** — *Select* if you want to preserve Ops Manager Director VMs after a failed deployment, for troubleshooting purposes.
   - **Pager Duty Plugin** — *Do not select*.
   - **HM Email Plugin** — *Do not select*.
   - **Blobstore Location** — Select *Internal*.
   - **Database Location** — Select *Internal*.
   - **Director Workers** — Sets the number of workers available to execute Director tasks. This field defaults to *5*.
   - **Max Threads** — *Leave this blank*.
   - **Director Hostname** — *Leave this blank*.
3. Click on **Save**.

## Complete the Create Availability Zones Page

To complete the *Create Availability Zones* Page:

1. In Ops Manager, select **Create Availability Zones**. See *Figure 18: Availability Zones Page* on page 26.



‹ Installation Dashboard

Ops Manager Director

Settings | Status | Credentials

- ✓ Openstack Config
- ✓ Advanced Infrastructure Config
- ✓ Director Config
- ✓ Create Availability Zones
- ○ Create Networks
- ○ Assign AZs and Networks
- ✓ Security
- ✓ Syslog
- ✓ Resource Config

Create Availability Zones

Availability Zones

▾ nova

Openstack Availability Zone*: nova

Many OpenStack environments use a default of 'nova' for this setting

Save

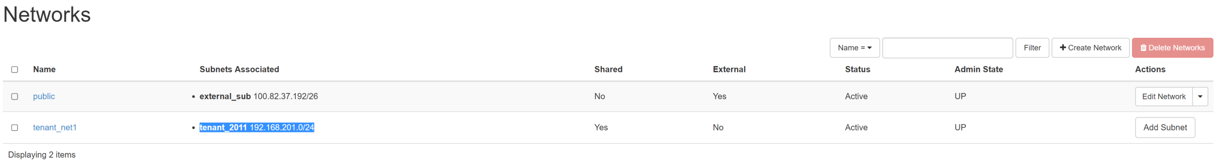
**Figure 18: Availability Zones Page**

2. Enter the **name of the availability zone** that you selected in *Launch the Ops Manager VM* on page 18.
3. Click on **Save**.

## Complete the Networks Page

To complete the *Networks* page:

1. In the left-hand pane of your OpenStack dashboard, click on **Project > Network > Networks**. See *Figure 19: Networks Page* on page 26.



Networks

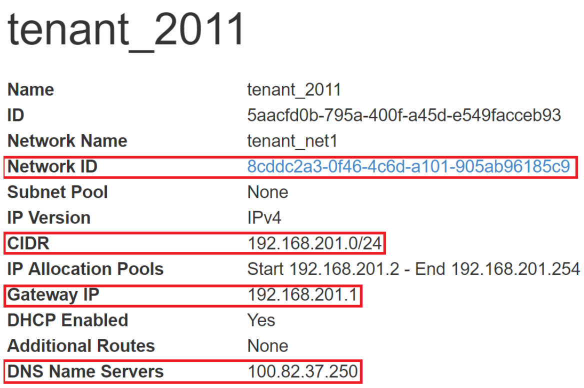
Name = ▾ | Filter | + Create Network | Delete Networks

| □ | Name | Subnets Associated | Shared | External | Status | Admin State | Actions |
|---|---|---|---|---|---|---|---|
| □ | public | • **external_sub** 100.82.37.192/26 | No | Yes | Active | UP | Edit Network ▾ |
| □ | tenant_net1 | • **tenant_2011** 192.168.201.0/24 | Yes | No | Active | UP | Add Subnet |

Displaying 2 items

**Figure 19: Networks Page**

2. Click on the **name** of the network that contains the private subnet where you deployed the Ops Manager VM. The OpenStack Network Detail page (see *Figure 20: Network Details Page* on page 27) displays your network settings.

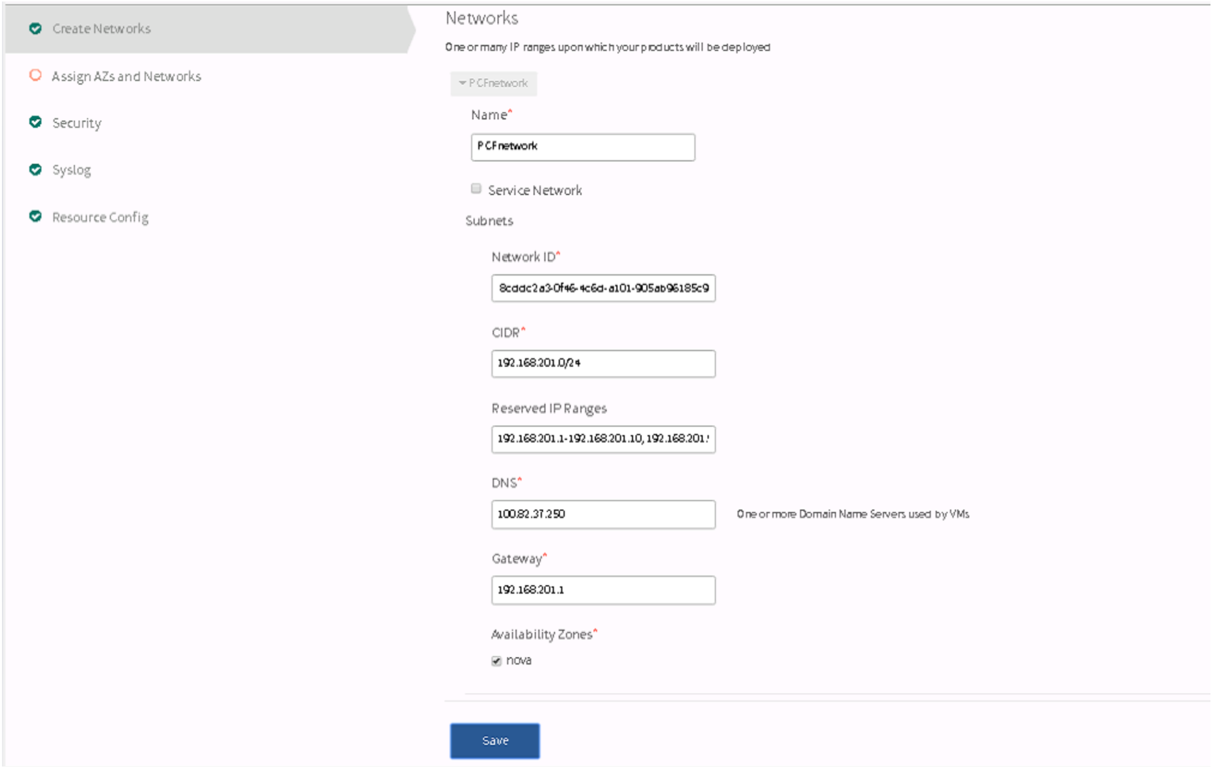


tenant_2011

| | |
|---|---|
| **Name** | tenant_2011 |
| **ID** | 5aacfd0b-795a-400f-a45d-e549facceb93 |
| **Network Name** | tenant_net1 |
| **Network ID** | 8cddc2a3-0f46-4c6d-a101-905ab96185c9 |
| **Subnet Pool** | None |
| **IP Version** | IPv4 |
| **CIDR** | 192.168.201.0/24 |
| **IP Allocation Pools** | Start 192.168.201.2 - End 192.168.201.254 |
| **Gateway IP** | 192.168.201.1 |
| **DHCP Enabled** | Yes |
| **Additional Routes** | None |
| **DNS Name Servers** | 100.82.37.250 |

**Figure 20: Network Details Page**

3. In Ops Manager, select **Create Networks**. See *Figure 21: Create Networks Page* on page 27.



Networks

One or many IP ranges upon which your products will be deployed

PCFnetwork

Name*: PCFnetwork

□ Service Network

Subnets

Network ID*: 8cddc2a3-0f46-4c6d-a101-905ab96185c9

CIDR*: 192.168.201.0/24

Reserved IP Ranges: 192.168.201.1-192.168.201.10, 192.168.201.!

DNS*: 100.82.37.250 One or more Domain Name Servers used by VMs

Gateway*: 192.168.201.1

Availability Zones*

☑ nova

**Figure 21: Create Networks Page**

4. Complete the **Networks** page with the following information:

- **Enable ICMP checks** — *Select* to enable ICMP on your networks. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
- **Add Network** — *Select* to add a network.
- **Name** — Enter a *unique name* for the network. For example, *PCFnetwork*.
- **Service Networks** — *Do not select*.
- **Add Subnet** — *Select* to create one or more subnets for the network.
- **Network ID** — Use the *ID* from the OpenStack page.
- **CIDR** — Use the *Network Address* from the OpenStack page.

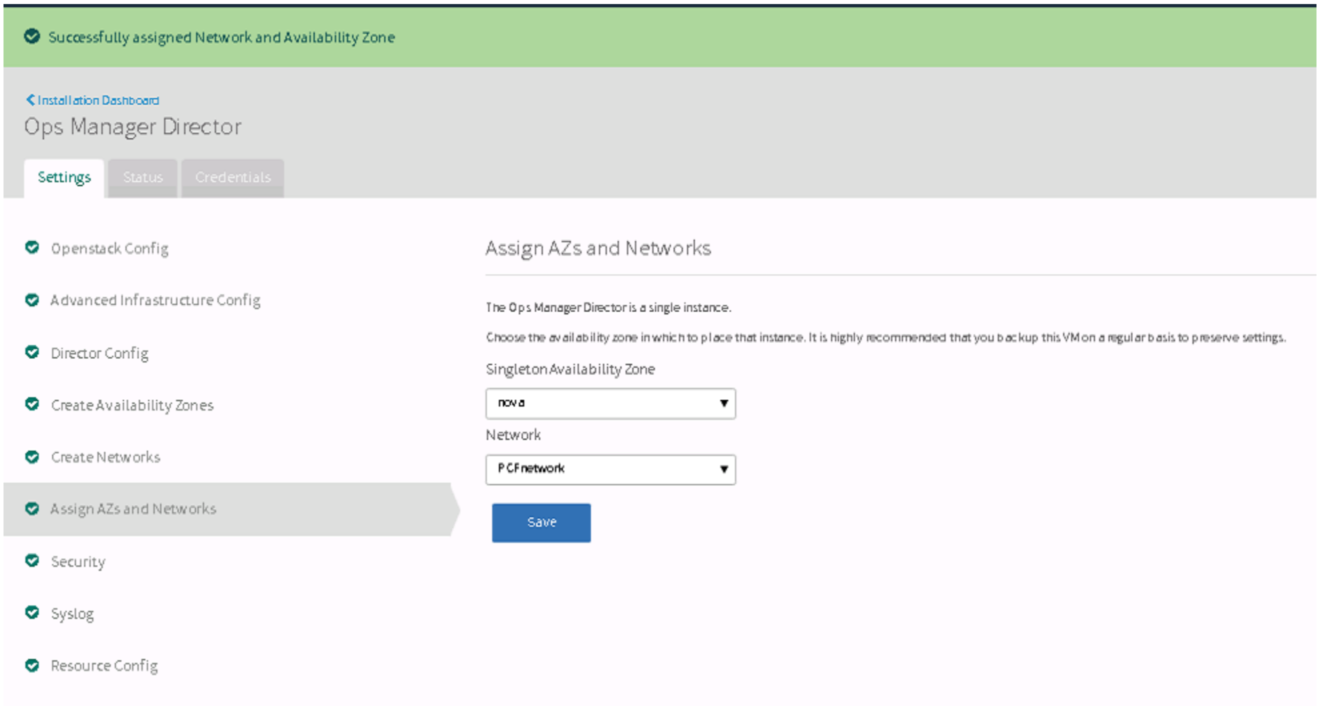
- **Reserved IP Ranges** — Use the first *50 IP addresses of the Network Address range*, and the *private IP address of the Ops Manager instance* that you recorded in *Associate a Floating IP Address* on page 19.
- **DNS** — Enter *one or more DNS servers*.
- **Gateway** — Use the *Gateway IP* from the OpenStack page.
- **Availability Zones** — Select which *Availability Zones* to use with the network.

5. Click on **Save**.

## Complete the Assign AZs and Networks Page

To complete the Assign AZs and Networks Page:

1. Select **Assign Availability Zones**. See *Figure 22: Assign Availability Zones* on page 28.



Successfully assigned Network and Availability Zone

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: PCFnetwork

**Figure 22: Assign Availability Zones**

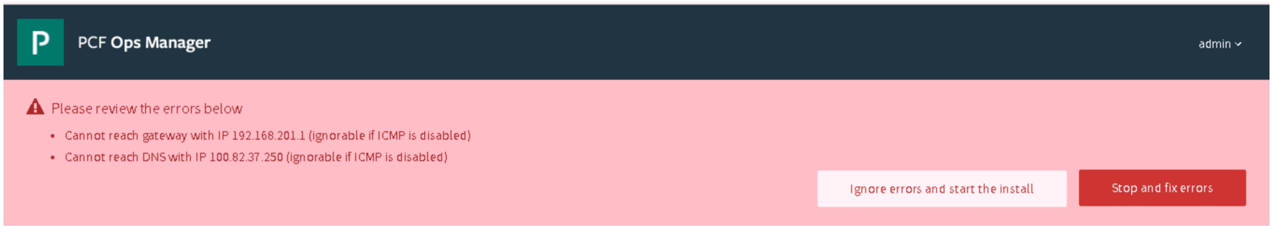
2. From the *Singleton Availability Zone* drop-down menu, select the **availability zone** that you created in *Complete the Create Availability Zones Page* on page 25. The Ops Manager Director installs in this Availability Zone.
3. Use the drop-down menu to select the **Network** that you created in *Complete the Networks Page* on page 26. Ops Manager Director installs in this network .
4. Click on **Save**.

## Complete the Ops Manager Director Installation

To complete the Ops Manager Director Installation:

1. Click on the **Installation Dashboard link** to return to the Installation Dashboard.
2. Click on **Apply Changes**.

   a) If an error message similar to *Figure 23: Ops Manager Install Error Message* on page 29 appears, click on **Ignore errors and start the install**.

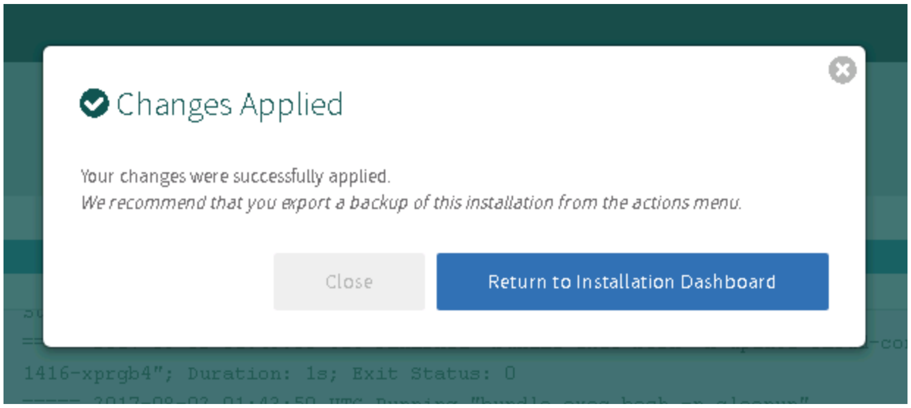


Please review the errors below

- Cannot reach gateway with IP 192.168.201.1 (ignorable if ICMP is disabled)
- Cannot reach DNS with IP 100.82.37.250 (ignorable if ICMP is disabled)

**Figure 23: Ops Manager Install Error Message**

When Ops Manager Director successfully installs a message similar to *Figure 24: Ops Manager Director Changes Applied Message* on page 29 displays:



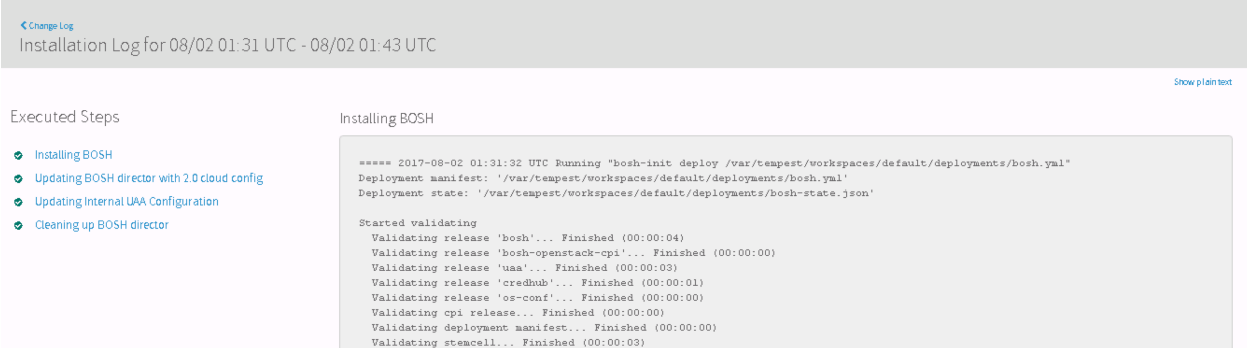
Changes Applied

Your changes were successfully applied.
*We recommend that you export a backup of this installation from the actions menu.*

```
1416-xprgb4"; Duration: 1s; Exit Status: 0
```

**Figure 24: Ops Manager Director Changes Applied Message**

3. On the *Installation Dashboard* you can select **ChangeLog** to observe the deployment steps. See *Figure 25: Ops Manager Director Change Log* on page 29.



Installation Log for 08/02 01:31 UTC - 08/02 01:43 UTC

Executed Steps

- Installing BOSH
- Updating BOSH director with 2.0 cloud config
- Updating Internal UAA Configuration
- Cleaning up BOSH director

Installing BOSH

```
===== 2017-08-02 01:31:32 UTC Running "bosh-init deploy /var/tempest/workspaces/default/deployments/bosh.yml"
Deployment manifest: '/var/tempest/workspaces/default/deployments/bosh.yml'
Deployment state: '/var/tempest/workspaces/default/deployments/bosh-state.json'

Started validating
  Validating release 'bosh'... Finished (00:00:04)
  Validating release 'bosh-openstack-cpi'... Finished (00:00:00)
  Validating release 'uaa'... Finished (00:00:03)
  Validating release 'credhub'... Finished (00:00:01)
  Validating release 'os-conf'... Finished (00:00:00)
  Validating cpi release... Finished (00:00:00)
  Validating deployment manifest... Finished (00:00:00)
  Validating stemcell... Finished (00:00:03)
```

**Figure 25: Ops Manager Director Change Log**

## Install and Configure Elastic Runtime

Perform the following procedures, in the order listed, to install and configure Elastic Runtime:

1. *Add Elastic Runtime to Ops Manager* on page 30
2. *Assign Availability Zones and Networks* on page 31
3. *Configure Elastic Runtime Domains* on page 32

4. *Configure Networking* on page 33
5. *Review Application Security Groups* on page 34
6. *Configure UAA* on page 35
7. *Configure Internal MySQL* on page 35
8. *Enable Traffic to OpenStack Private Subnet* on page 35
9. *Complete Elastic Runtime Installation* on page 36

For detailed information about these steps, see *https://docs.pivotal.io/pivotalcf/customizing/openstack-er-config.html*.

## Add Elastic Runtime to Ops Manager

To add Elastic Runtime to Pivotal Ops Manager:

1. Download the Pivotal Cloud Foundry Elastic Runtime tile, `cf-1.11.5-build.2.pivotal`, from *Pivotal Network*.
2. Log into your Ops Manager **Installation Dashboard**.
3. Click on **Import a Product** to add the downloaded file to Installation Dashboard. See *Figure 26: Elastic Runtime Import Product Screen* on page 30.

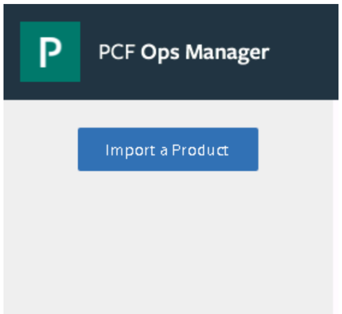


**Figure 26: Elastic Runtime Import Product Screen**

4. Select the **.pivotal file** that you downloaded from Pivotal Network, or received from your software distributor.
5. Click on **Open**.
   a) If the product is successfully added, it appears in your product list.
   b) If the product you selected is not the latest version, the most up-to-date version will appear on your product list.
6. Add the product tile to the Installation Dashboard by clicking the **green plus sign icon (+)**. See *Figure 27: Ops Manager Add Product Screen* on page 31.

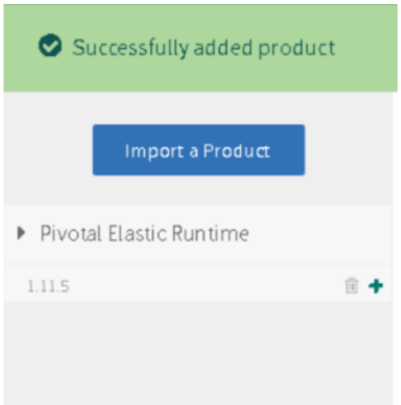


**Figure 27: Ops Manager Add Product Screen**

7. The product tile appears in the Installation Dashboard. See *Figure 28: Ops Manager Product Added Screen* on page 31.
   a) If the product requires configuration, the tile appears orange.
   b) If necessary, configure the product.

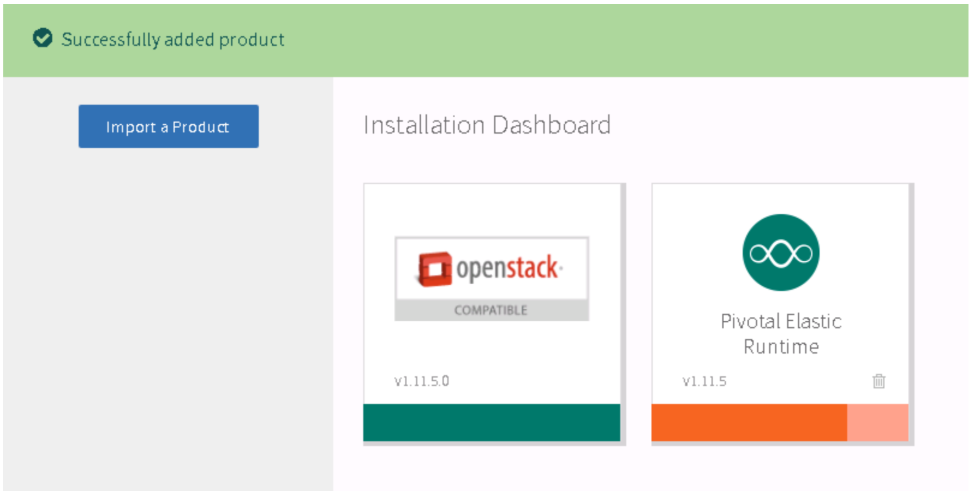
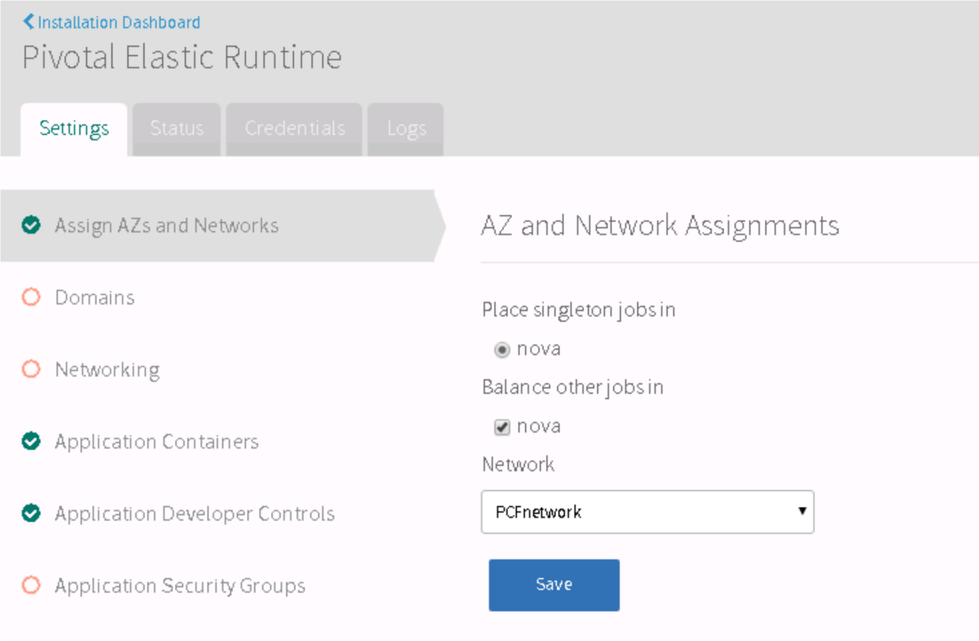


**Figure 28: Ops Manager Product Added Screen**

## Assign Availability Zones and Networks

To assign Availability Zones and Networks to Elastic Runtime:

1. In the Installation Dashboard, select **Elastic Runtime**.
2. Enter the Availability Zone and Network that you created in *Complete the Assign AZs and Networks Page* on page 28. See *Figure 29: Elastic Runtime AZ and Network Assignments Page* on page 32.



Place singleton jobs in

● nova

Balance other jobs in

☑ nova

Network

PCFnetwork ▾

**Figure 29: Elastic Runtime AZ and Network Assignments Page**

3. Click on **Save**.

## Configure Elastic Runtime Domains

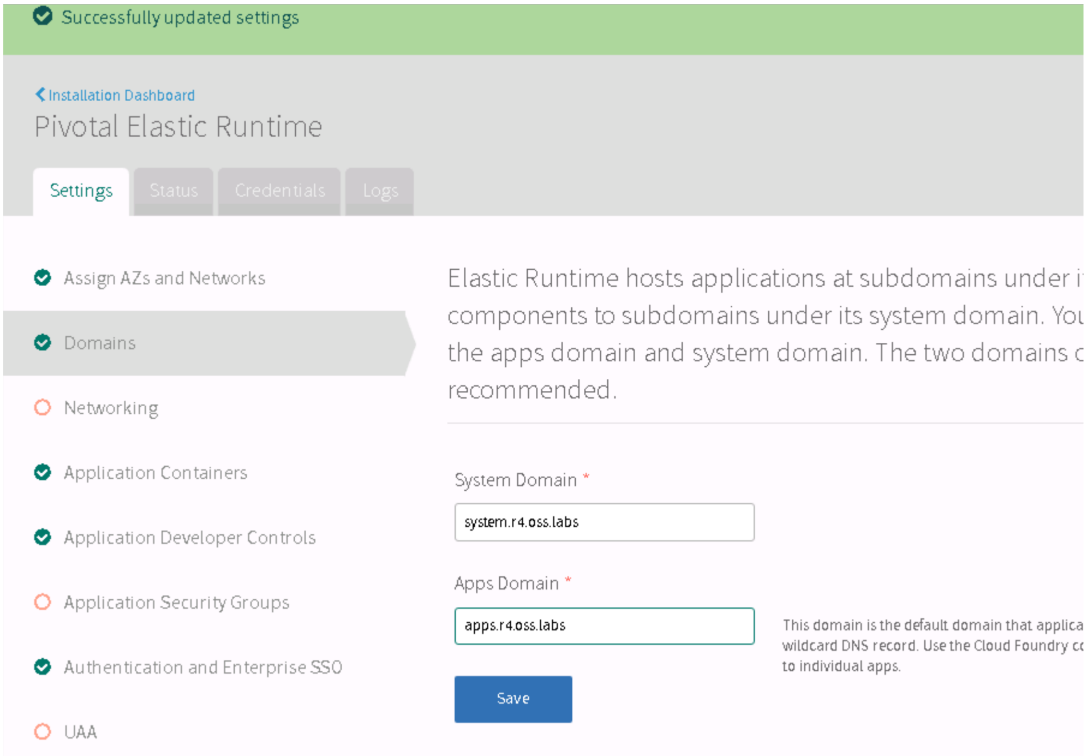
To configure Elastic Runtime domains:

1. Enter the system and application domains. See *Figure 30: Domains Page* on page 33.

   - The **Apps Domain** defines where Elastic Runtime should serve your applications.
   - The **System Domain** defines the domain for all other system components (UAA, etc.).

   For example, name your System Domain *system.r4.oss.labs* and your **Apps Domain** *apps.r4.oss.labs*.

   **Note:** Make sure you fulfill the prerequisite of creating the **.apps* and **.system* wildcard DNS records for HAProxy. For example, `*.r4.oss.labs`.



Successfully updated settings

Pivotal Elastic Runtime

Elastic Runtime hosts applications at subdomains under i components to subdomains under its system domain. You the apps domain and system domain. The two domains c recommended.

System Domain *

system.r4.oss.labs

Apps Domain *

apps.r4.oss.labs

This domain is the default domain that applica wildcard DNS record. Use the Cloud Foundry co to individual apps.

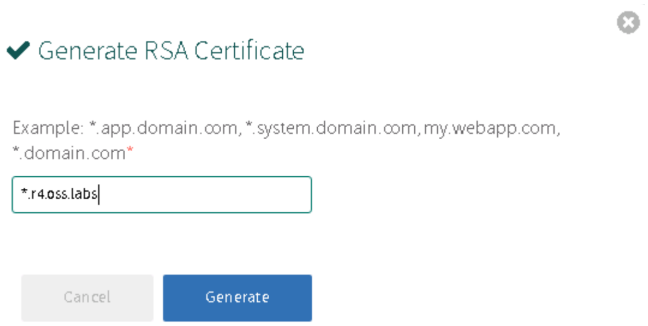
**Figure 30: Domains Page**

2. Click on **Save**.

## Configure Networking

To configure networking:

1. Select **Networking**.
2. Complete the Networks page with the following information:
   - **Router IPs** — *Leave this blank*, as you are not using your own load balancer.
   - **HAProxy IPs** — Use the *HAProxy* load balancer, but you can leave this blank and assign a floating IP to it later.
   - **SSH Proxy IPs** — *Leave this blank*.
   - **TCP Router IPs** — *Leave this blank*.
   - **Configure the point-of-entry to this environment** — Choose *Forward SSL to HAProxy*, and then click on **Generate RSA certificate** to generate SSL Certificate & Private key. See *Figure 31: Generate RSA Certificate* on page 34.



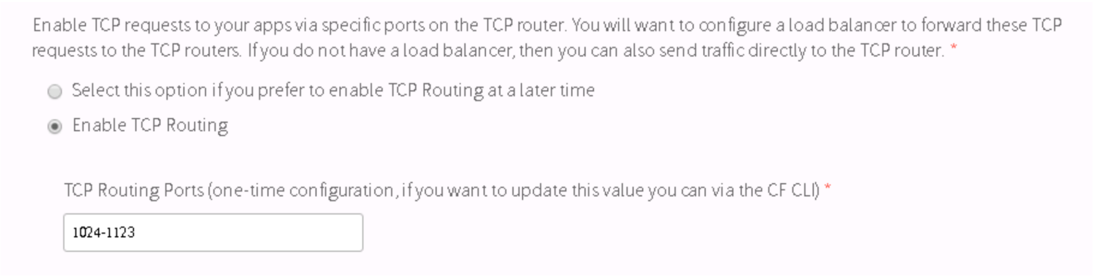
✔ Generate RSA Certificate

Example: *.app.domain.com, *.system.domain.com, my.webapp.com, *.domain.com*

*.r4.oss.labs

**Figure 31: Generate RSA Certificate**

3. Complete the Generate RSA Certificate page with the following information:
   - **Disable HTTP traffic to HAProxy** — *Do not select*. The HAProxy should allow both HTTP and HTTPS traffic.
   - **Disable SSL certificate verification for this environment** — *Select*, since you are not using SSL encryption, or you are using self-signed certificates.
   - **Disable insecure cookies on the Router** — *Select* to set the secure flag.
   - **Enable Zipkin tracing headers on the router** — *Leave selected* to enable Zipkin tracing headers (the default). *Deselect* to disable Zipkin tracing headers.
   - **Choose whether or not to enable route services** — Choose *Enable route services*, and leave the optional fields blank.
   - **Enable TCP Requests** — TCP Routing is disabled by default. See *Figure 32: Enable TCP Routing* on page 34. To enable it:
     1. Select *Enable TCP Routing*.
     2. In **TCP Routing Ports**, enter a *range of ports* to be allocated for TCP Routes.



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

**Figure 32: Enable TCP Routing**

## Review Application Security Groups

Setting appropriate Application Security Group is critical for a secure deployment.

To review Application Security Groups:

1. Select **Application Security Groups**.
2. Enter **X** in the text box to acknowledge that once the Elastic Runtime deployment completes, you will review and set the appropriate application security groups.
3. Select the **Enable** option for the network policy using `cf allow-access` to govern the communication.
4. Click on **Save**.

## Configure UAA

To configure User Account and Authentication (UAA):

1. Select **UAA**.
2. Complete the UAA page with the following information:
   - Under *Choose the location for your UAA database*, select **Internal MySQL**.
   - Click on **Generate RSA Certificate for SAML Service Provider Credentials**.
   - Leave the optional properties set to their *default values*.
3. Click on **Save**.

## Configure Internal MySQL

To configure Internal MySQL:

The MySQL service will send alerts when the cluster experiences a replication issue or a node is not allowed to auto-rejoin the cluster.

1. Select **Internal MySQL**.
2. Enter an **E-mail address**.
3. Leave the optional properties set to their *default values*.
4. Click on **Save**.

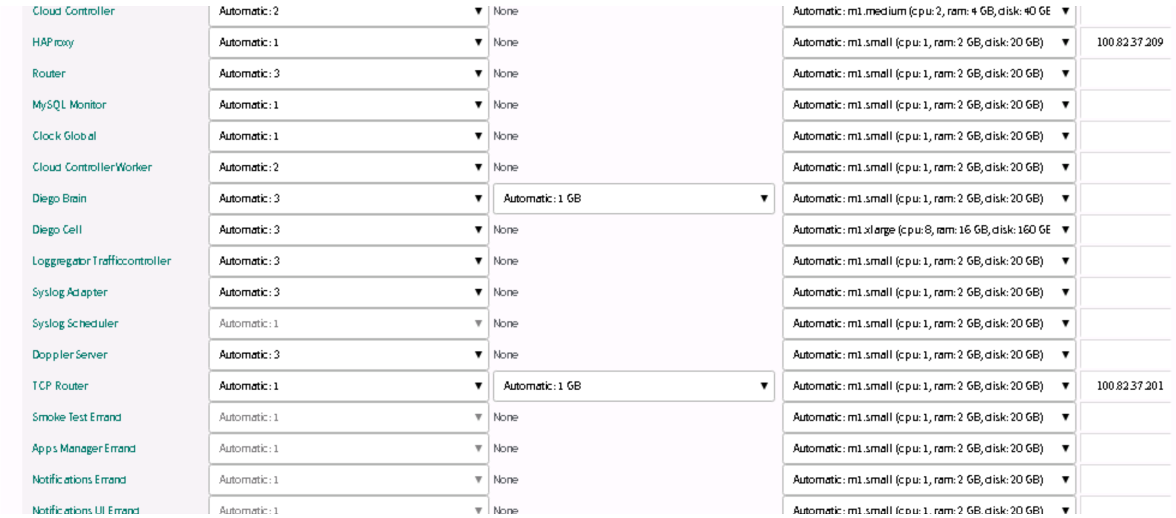
## Enable Traffic to OpenStack Private Subnet

You must enable traffic flow to the OpenStack private subnet. This provides HAProxy with a way of routing traffic into the private subnet, by providing public IP addresses as floating IP addresses.

To enable tyraffic to the OpenStack private subnet:

1. Enter one or more **IP addresses** in the *Floating IPs* column for each HAProxy. See *Figure 33: Floating IP Addresses* on page 35.

   **Note:** Use the Floating IP address you created for setting up the wildcard DNS entry in *Configure Elastic Runtime Domains* on page 32.

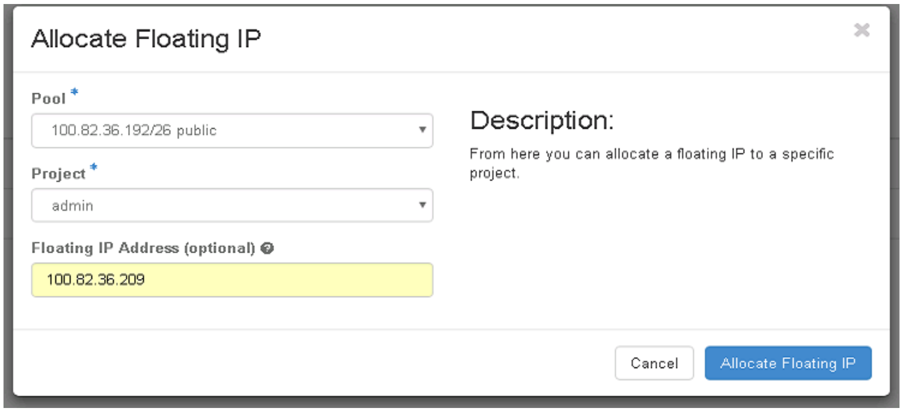


| | | | | |
|---|---|---|---|---|
| Cloud Controller | Automatic: 2 ▼ | None | Automatic: m1.medium (cpu: 2, ram: 4 GB, disk: 40 GE ▼ | |
| HAProxy | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | 100.82.37.209 |
| Router | Automatic: 3 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| MySQL Monitor | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Clock Global | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Cloud Controller Worker | Automatic: 2 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Diego Brain | Automatic: 3 ▼ | Automatic: 1 GB ▼ | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Diego Cell | Automatic: 3 ▼ | None | Automatic: m1.xlarge (cpu: 8, ram: 16 GB, disk: 160 GE ▼ | |
| Loggregator Trafficcontroller | Automatic: 3 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Syslog Adapter | Automatic: 3 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Syslog Scheduler | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Doppler Server | Automatic: 3 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| TCP Router | Automatic: 1 ▼ | Automatic: 1 GB ▼ | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | 100.82.37.201 |
| Smoke Test Errand | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Apps Manager Errand | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Notifications Errand | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |
| Notifications UI Errand | Automatic: 1 ▼ | None | Automatic: m1.small (cpu: 1, ram: 2 GB, disk: 20 GB) ▼ | |

**Figure 33: Floating IP Addresses**

2. Enter one or more **IP addresses** in the *Floating IPs* column for each TCP Router.
3. Log into Horizon.
4. Navigate to **Admin > Floating IPs**.

5. Click on **Allocate Floating IP** to enter your *HAProxy floating IP address* as shown in *Figure 34: Allocate Floating IP Address* on page 36.



Allocate Floating IP

Pool *
100.82.36.192/26 public

Project *
admin

Floating IP Address (optional)
100.82.36.209

Description:
From here you can allocate a floating IP to a specific project.

**Figure 34: Allocate Floating IP Address**

6. Repeat step *5* on page 36 to enter your *TCPRouter floating IP address*.
7. Click on **Save**.

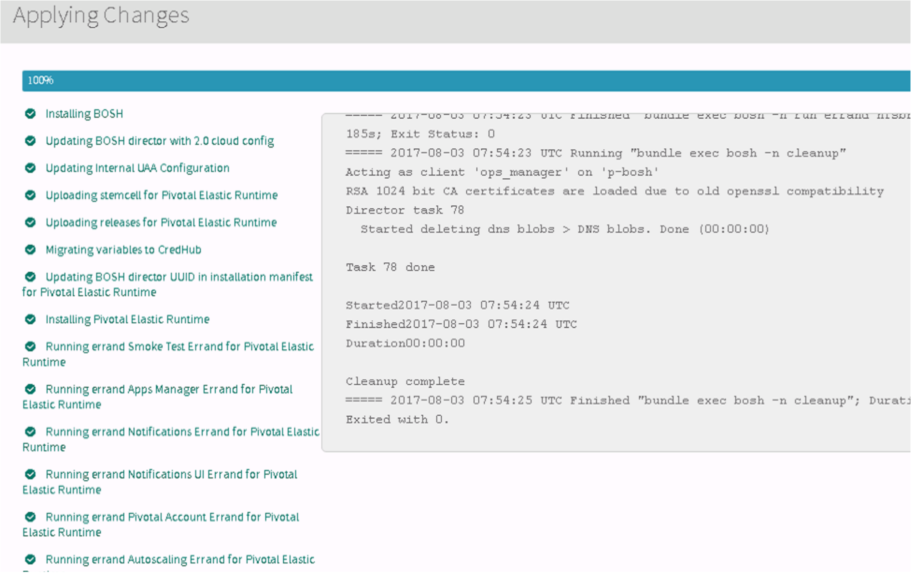
## Complete Elastic Runtime Installation

To complete the Elastic Runtime installation:

1. Click on the **Installation Dashboard** link to return to the Installation Dashboard.
2. Click on **Apply Changes**.

   a) If an ICMP error message displays, click on **Ignore errors and start the install**.

   When Elastic Runtime successfully installs a **Changes Applied** message displays.
3. On the *Installation Dashboard* you can select **ChangeLog** to observe the deployment steps. See *Figure 35: Elastic Runtime Change Log* on page 36.



Applying Changes

100%

✓ Installing BOSH
✓ Updating BOSH director with 2.0 cloud config
✓ Updating Internal UAA Configuration
✓ Uploading stemcell for Pivotal Elastic Runtime
✓ Uploading releases for Pivotal Elastic Runtime
✓ Migrating variables to CredHub
✓ Updating BOSH director UUID in installation manifest for Pivotal Elastic Runtime
✓ Installing Pivotal Elastic Runtime
✓ Running errand Smoke Test Errand for Pivotal Elastic Runtime
✓ Running errand Apps Manager Errand for Pivotal Elastic Runtime
✓ Running errand Notifications Errand for Pivotal Elastic Runtime
✓ Running errand Notifications UI Errand for Pivotal Elastic Runtime
✓ Running errand Pivotal Account Errand for Pivotal Elastic Runtime
✓ Running errand Autoscaling Errand for Pivotal Elastic

```
===== 2017-08-03 07:54:23 UTC Finished "bundle exec bosh -n run errand nfsbr
185s; Exit Status: 0
===== 2017-08-03 07:54:23 UTC Running "bundle exec bosh -n cleanup"
Acting as client 'ops_manager' on 'p-bosh'
RSA 1024 bit CA certificates are loaded due to old openssl compatibility
Director task 78
  Started deleting dns blobs > DNS blobs. Done (00:00:00)

Task 78 done

Started2017-08-03 07:54:24 UTC
Finished2017-08-03 07:54:24 UTC
Duration00:00:00

Cleanup complete
===== 2017-08-03 07:54:25 UTC Finished "bundle exec bosh -n cleanup"; Durati
Exited with 0.
```

**Figure 35: Elastic Runtime Change Log**

# Deploy JMX Bridge

Perform the following procedures, in the order listed, to deploy JMX Bridge:

1. *Add JMX Bridge to Ops Manager* on page 37
2. *Assign Availability Zones and Networks* on page 37
3. *Configure JMX Provider* on page 37
4. *Update Stemcell for JMX Provider* on page 38
5. *Apply JMX Bridge Changes* on page 39
6. *Find the JMX Provider IP Address* on page 39
7. *Configure the Metrics IP Address* on page 39
8. *Complete JMX Bridge Installation* on page 40

## Add JMX Bridge to Ops Manager

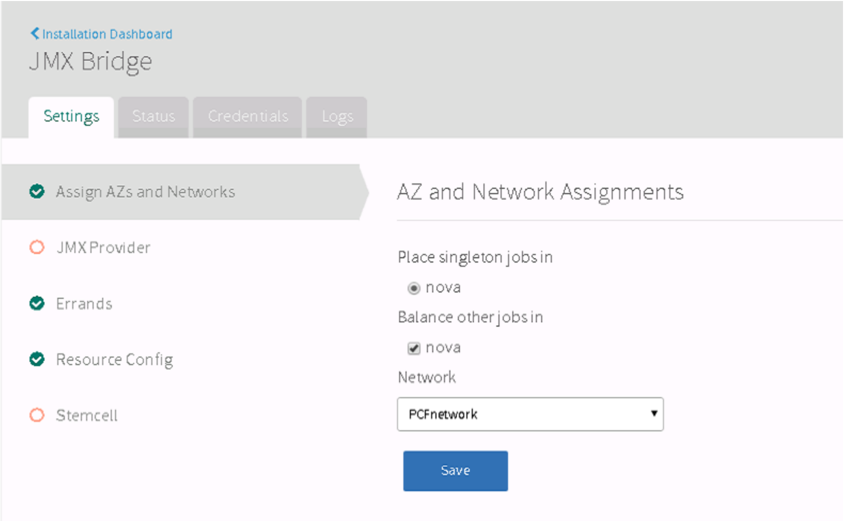
To add JMX Bridge to Ops Manager:

1. Download the JMX Bridge tile, `p-metrics-1.9.1.pivotal`, from *Pivotal Network*.
2. Log into your Ops Manager **Installation Dashboard**.
3. Click on **Import a Product** to add the downloaded file to Installation Dashboard.
4. Click on **Save**.

## Assign Availability Zones and Networks

To assign Availability Zones and Networks to JMX Bridge:

1. In the Installation Dashboard, select **JMX Bridge**.
2. Enter the Availability Zone and Network that you created in *Complete the Assign AZs and Networks Page* on page 28. See *Figure 36: JMX Bridge AZ and Network Assignments Page* on page 37.



AZ and Network Assignments

Place singleton jobs in

● nova

Balance other jobs in

☑ nova

Network

PCFnetwork

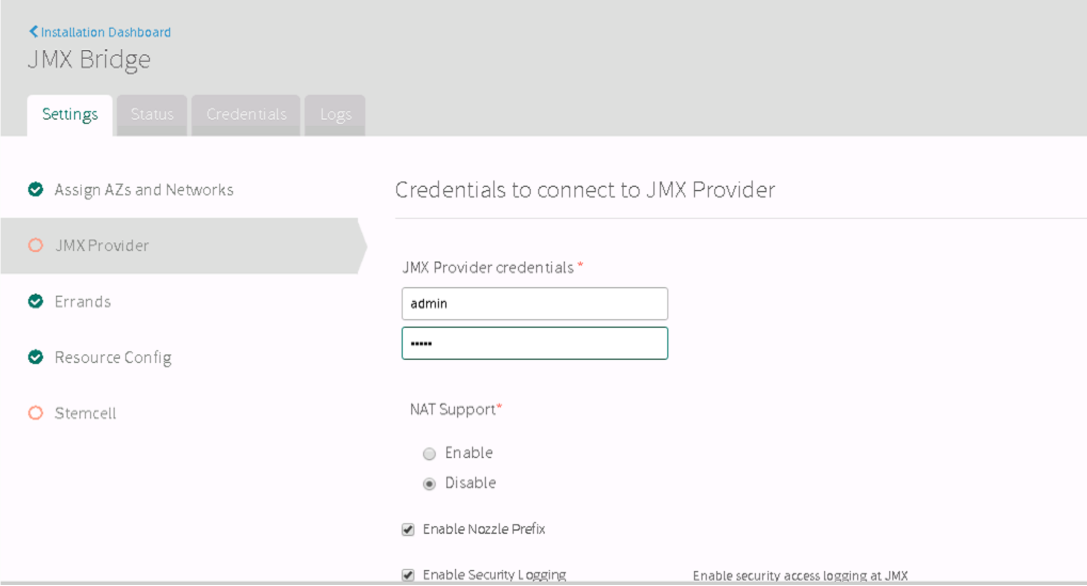
**Figure 36: JMX Bridge AZ and Network Assignments Page**

3. Click on **Save**.

## Configure JMX Provider

To configure JMX Provider:

1. Select **JMX Provider**. See *Figure 37: JMX Provider Page* on page 38.



Credentials to connect to JMX Provider

JMX Provider credentials *

admin

•••••

NAT Support*

○ Enable

● Disable

☑ Enable Nozzle Prefix

☑ Enable Security Logging Enable security access logging at JMX

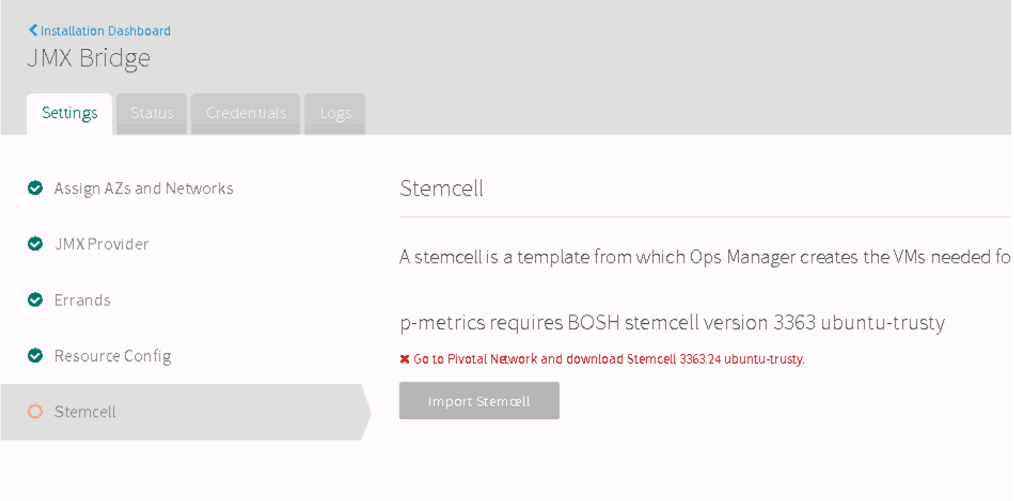
**Figure 37: JMX Provider Page**

2. Enter a new **username** and **password** into the JMX Provider credentials *username and password fields*.
3. Record these credentials. You will use them to connect JMX clients to the JMX Provider.

## Update Stemcell for JMX Provider

To update Stemcell for JMX Provider:

1. Select **Stemcell**. See *Figure 38: Stemcell Page* on page 38.



Stemcell

A stemcell is a template from which Ops Manager creates the VMs needed fo

p-metrics requires BOSH stemcell version 3363 ubuntu-trusty

✖ Go to Pivotal Network and download Stemcell 3363.24 ubuntu-trusty.

**Figure 38: Stemcell Page**

2. Download the Stemcell for OpenStack tile, `bosh-stemcell-3363.24-openstack-kvm-ubuntu-trusty-go_agent-raw.tgz`, from *Pivotal Network*.
3. Click on **Import a Product** to add the downloaded file to Installation Dashboard.
4. Click on **Save**.

## Apply JMX Bridge Changes

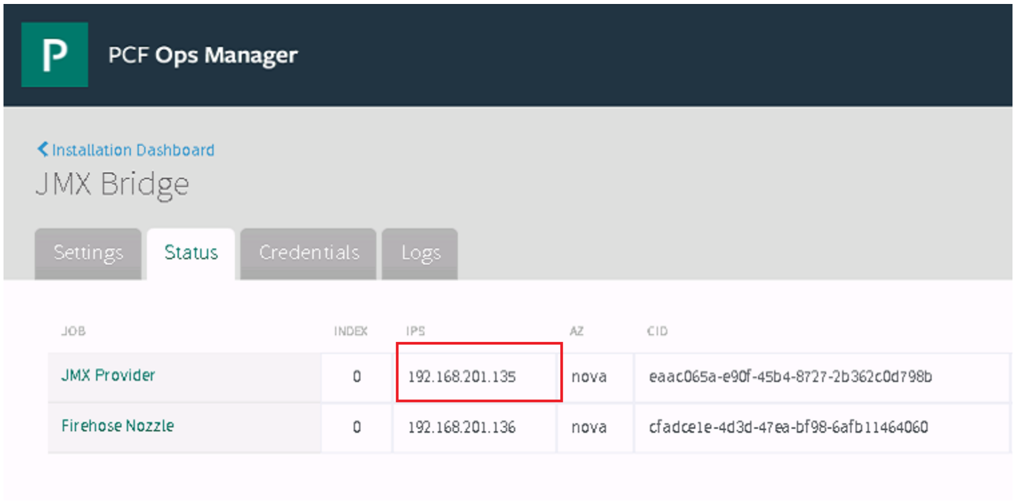
To apply the JMX Bridge changes:

1. Navigate to the PCF Ops Manager Installation Dashboard.
2. In the *Pending Changes* view, click on **Apply Changes** to install JMX Bridge.
   a) If an ICMP error message displays, click on **Ignore errors and start the install**.
   When Elastic Runtime successfully installs a **Changes Applied** message displays.
3. On the *Installation Dashboard* you can select **ChangeLog** to observe the deployment steps.

## Find the JMX Provider IP Address

To find the JMX Provider IP Address:

1. Click on **Return to Product Dashboard**.
2. Click on the **JMX Bridge tile**.
3. Select the **Status** tab. See *Figure 39: JMX Provider Status* on page 39.



| JOB | INDEX | IPS | AZ | CID |
|---|---|---|---|---|
| JMX Provider | 0 | 192.168.201.135 | nova | eaac065a-e90f-45b4-8727-2b362c0d798b |
| Firehose Nozzle | 0 | 192.168.201.136 | nova | cfadce1e-4d3d-47ea-bf98-6afb11464060 |

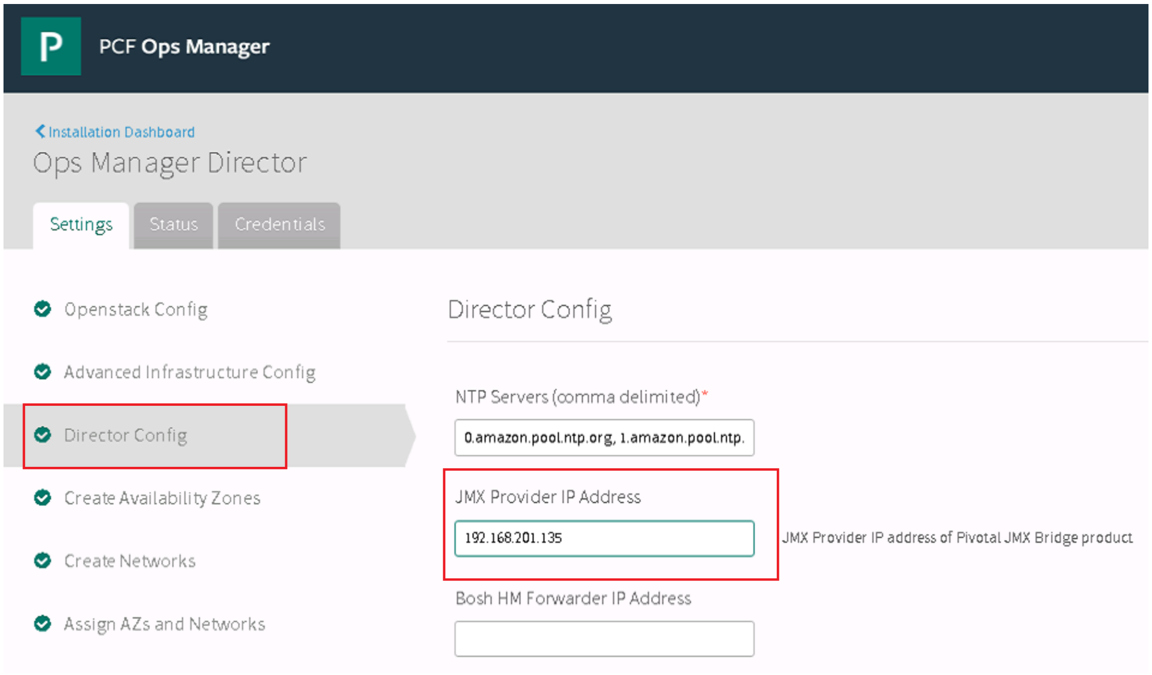
**Figure 39: JMX Provider Status**

4. Record the IP address of the **JMX Provider**.

## Configure the Metrics IP Address

To configure the Metrics IP Address

1. Click on **Return to Product Dashboard**.
2. Click on the **Ops Manager Director** tile.
3. Select the **Director Config** tab. See *Figure 40: Director Config Tab* on page 40.



NTP Servers (comma delimited)*: 0.amazon.pool.ntp.org, 1.amazon.pool.ntp.

JMX Provider IP Address: 192.168.201.135

JMX Provider IP address of Pivotal JMX Bridge product

Bosh HM Forwarder IP Address:

**Figure 40: Director Config Tab**

4. Enter the **IP address of the JMX Provider** into the *Metrics IP Address* field.
5. Click on **Save**.

## Complete JMX Bridge Installation

To complete the JMX Bridge installation:

1. Navigate to the PCF Ops Manager Installation Dashboard.
2. In the *Pending Changes* view, click on **Apply Changes** to install JMX Bridge.
   a) If an ICMP error message displays, click on **Ignore errors and start the install**.
   When Elastic Runtime successfully installs a **Changes Applied** message displays.
3. On the *Installation Dashboard* you can select **ChangeLog** to observe the deployment steps.

# Chapter 4

# Deploy a Sample Application

**Topics:**

- *Gather Credentials and API Endpoint Information*
- *Prepare to Deploy*
- *Deploy a Sample Application*

Now that Pivotal Cloud Foundry is installed, you can deploy a sample application using the procedures in this chapter.

## Gather Credentials and API Endpoint Information

Before you can push your application to Pivotal Cloud Foundry you need to know your username and password for your Pivotal Cloud Foundry instance.

To retrieve your Pivotal Cloud Foundry credentials:

1. Using a web browser, navigate to the Pivotal Cloud Foundry Ops Manager.
2. Click on the **Pivotal Elastic Runtime tile** in the Ops Manager Installation dashboard.
3. Click on the **Credentials** tab.
4. Locate the **UAA admin credentials**, and note the *Password*.
5. Click on the **Domains** tab, and note the *System Domain*.
6. Navigate to **https://login.system.mydomain.com**, where *system.mydomain.com* is the Pivotal Cloud Foundry system domain name that was specified in the Elastic Runtime Cloud Controller configuration.
7. At the login prompt, enter the following credentials:
   - **Email** — *admin*
   - **Password** — the *UAA admin password* you retrieved in step *4* on page 42
8. Click on **SIGN IN**.
9. Click on **Pivotal Dev Console** to display the Pivotal Apps Manager screen.

## Prepare to Deploy

To prepare to deploy your application:

1. Configure the **Pivotal 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 **Pivotal Cloud Foundry CLI**:

   ```
   $ sudo yum install cf-cli
   ```

3. Set the **API Endpoint**:

   ```
   $ cf api https://api.system.r4.oss.labs --skip-ssl-validation
   ```

4. Create a **new space**, *MYAPPSPACE*, under the *system* organization:

   ```
   $ cf target -o "system"
   $ cf create-space MYAPPSPACE
   $ cf target -s "MYAPPSPACE"
   ```

5. **Log in** using the credentials gathered in step *4* on page 42:

   ```
   $ cf login
   ```

# Deploy a Sample Application

To Deploy a sample application from Github:

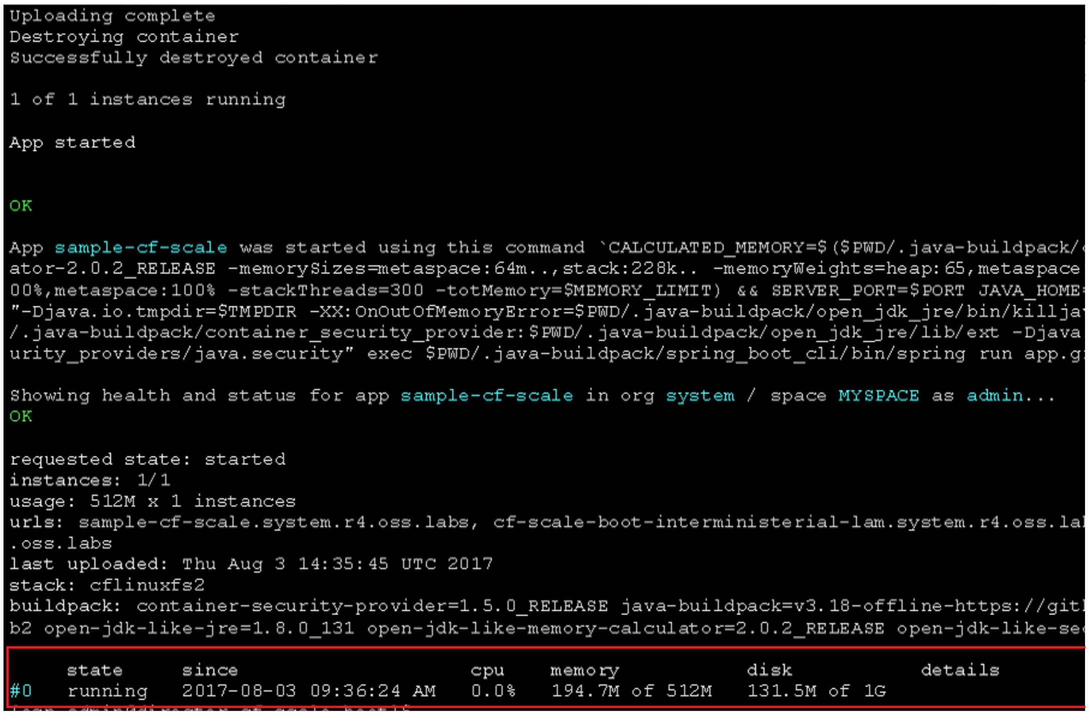
1. **Download** the `cf-scale-boot` sample application:

```
$ git clone https://github.com/cf-platform-eng/cf-scale-boot
```

2. **Push** the `cf-scale-boot` application to Pivotal Cloud Foundry:

```
$ cd sample-cf-scale
$ cf push sample-cf-scale
```

   a) When the application has been successfully pushed the output will display similarly to *Figure 41: Application Pushed Output* on page 43:



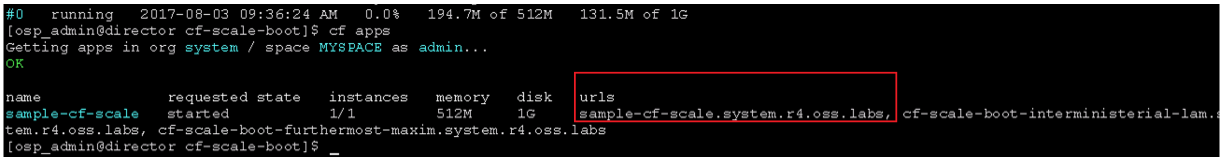
```
Uploading complete
Destroying container
Successfully destroyed container

1 of 1 instances running

App started


OK

App sample-cf-scale was started using this command `CALCULATED_MEMORY=$($PWD/.java-buildpack/
ator-2.0.2_RELEASE -memorySizes=metaspace:64m..,stack:228k.. -memoryWeights=heap:65,metaspace
00%,metaspace:100% -stackThreads=300 -totMemory=$MEMORY_LIMIT) && SERVER_PORT=$PORT JAVA_HOME
"-Djava.io.tmpdir=$TMPDIR -XX:OnOutOfMemoryError=$PWD/.java-buildpack/open_jdk_jre/bin/killja
/.java-buildpack/container_security_provider:$PWD/.java-buildpack/open_jdk_jre/lib/ext -Djava
urity_providers/java.security" exec $PWD/.java-buildpack/spring_boot_cli/bin/spring run app.g

Showing health and status for app sample-cf-scale in org system / space MYSPACE as admin...
OK

requested state: started
instances: 1/1
usage: 512M x 1 instances
urls: sample-cf-scale.system.r4.oss.labs, cf-scale-boot-interministerial-lam.system.r4.oss.la
.oss.labs
last uploaded: Thu Aug 3 14:35:45 UTC 2017
stack: cflinuxfs2
buildpack: container-security-provider=1.5.0_RELEASE java-buildpack=v3.18-offline-https://git
b2 open-jdk-like-jre=1.8.0_131 open-jdk-like-memory-calculator=2.0.2_RELEASE open-jdk-like-se

     state     since                    cpu    memory           disk           details
#0   running   2017-08-03 09:36:24 AM   0.0%   194.7M of 512M   131.5M of 1G
```

**Figure 41: Application Pushed Output**

3. **View** your application:

```
$ cf apps
```

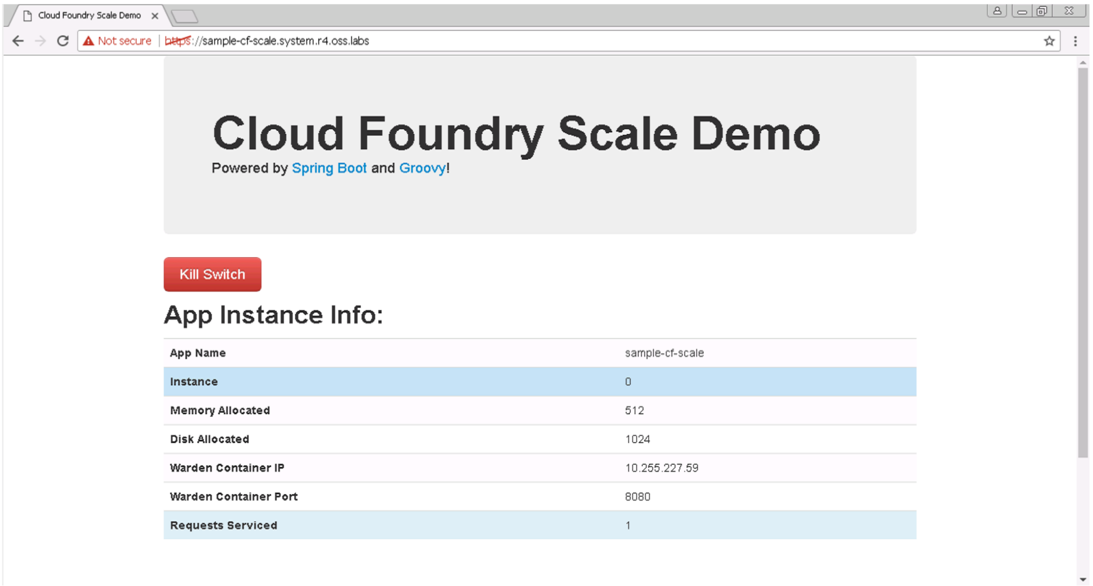
   a) The output displays the URL of your sample application, as in *Figure 42: Application URL Output* on page 43.



```
#0   running   2017-08-03 09:36:24 AM   0.0%   194.7M of 512M   131.5M of 1G
[osp_admin@director cf-scale-boot]$ cf apps
Getting apps in org system / space MYSPACE as admin...
OK

name              requested state   instances   memory   disk   urls
sample-cf-scale   started           1/1         512M     1G     sample-cf-scale.system.r4.oss.labs, cf-scale-boot-interministerial-lam.s
tem.r4.oss.labs, cf-scale-boot-furthermost-maxim.system.r4.oss.labs
[osp_admin@director cf-scale-boot]$ _
```

**Figure 42: Application URL Output**

4. **Open** a Web browser.
5. **Copy and paste** your application URL into the address field, then press **[ENTER]**.
   a) The `cf-scale-boot` application opens in your browser. See *Figure 43: Application Opened* on page 44.



# Cloud Foundry Scale Demo

Powered by Spring Boot and Groovy!

## App Instance Info:

| | |
|---|---|
| **App Name** | sample-cf-scale |
| **Instance** | 0 |
| **Memory Allocated** | 512 |
| **Disk Allocated** | 1024 |
| **Warden Container IP** | 10.255.227.59 |
| **Warden Container Port** | 8080 |
| **Requests Serviced** | 1 |

**Figure 43: Application Opened**

Your sample application is successfully deployed.

6. If you wish to **delete** your application, execute the following commands:

```
$ cd sample-cf-scale
$ cf delete sample-cf-scale
```

# Appendix A

## Getting Help

**Topics:**

- *Contacting Dell EMC*
- *References*

This appendix details contact and reference information for the Dell EMC Ready Bundle for Red Hat OpenStack Platform.

## Contacting Dell EMC

For customers in the United States, call 800-WWW-DELL (800-999-3355).

**Note:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell EMC product catalog.

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues:

1. Visit *dell.com/support*.
2. Click your country/region at the bottom of the page. For a full listing of country/region, click **All**.
3. Click **All Support** from the **Support** menu.
4. Select the appropriate service or support link based on your need.
5. Choose the method of contacting Dell EMC that is convenient for you.

## References

Additional information can be obtained at *http://www.dell.com/en-us/work/learn/openstack-cloud* or by e-mailing *openstack@dell.com*.

If you need additional services or implementation help, please contact your Dell EMC sales representative.

### To Learn More

For more information on the Dell EMC Ready Bundle for Red Hat OpenStack Platform visit *http://www.dell.com/learn/us/en/04/solutions/red-hat-openstack*.