

Pivotal Cloud Foundry on VMware vSphere using Dell EMC XC Series Hyper-Converged Appliances Deployment Guide

Dell EMC Engineering
May 2017

Revisions

Date	Description
May 2017	Initial release

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA. [5/5/2017]

Dell EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Table of contents

Revisions.....	2
Executive summary.....	4
1 Introduction.....	5
1.1 Audience.....	5
1.2 Infrastructure.....	5
1.3 Prerequisites.....	5
1.4 Assumptions.....	7
2 Deploying and configuring Operations Manager.....	8
2.1 Deploying Operations Manager to vSphere.....	8
2.2 Configuring Operations Manager Director for vSphere.....	14
3 Deploying and configuring Elastic Runtime for vSphere.....	27
3.1 Adding Elastic Runtime to Ops Manager.....	27
3.1.1 Viewing all the VMs for Ops Manager Director or Elastic Runtime.....	45
4 Creating new orgs, spaces, and user accounts.....	46
4.1 Obtaining credentials.....	46
4.2 cf CLI for orgs, spaces, and user accounts.....	47
5 Obtaining and pushing apps to PCF.....	51
5.1 Hello World.....	52
5.1.1 Pushing Hello World.....	53
5.1.2 Confirm Hello World is working.....	55
5.2 Spring Music.....	56
5.2.1 Assemble Spring Music.....	57
5.2.2 Confirming Spring Music is working.....	60
5.3 Apps Manager.....	61
A Options for settings proxies.....	63
A.1 Git for Windows proxy list.....	63
A.2 Adding proxy to manifest.yml.....	63
A.3 Adding proxy to gradle.properties file.....	64
B Technical support and resources.....	65
C Related resources.....	66
D Deployment checklist.....	67

Executive summary

The Dell EMC™ XC Series Hyper-converged Infrastructure (HCI) appliance powered by Nutanix™ delivers a highly resilient, converged compute and storage platform that brings benefits of scalable architecture to business-critical enterprise applications.

The XC Series platform is hypervisor agnostic and software installs quickly for deployment of multiple virtualized workloads. The XC Series Nutanix platform delivers storage through multiple protocols such as NFS, SMB, and iSCSI.

Pivotal Cloud Foundry (PCF) is a Cloud Native Solution that supplies developers with a ready-to-use cloud computing environment and application service, all hosted by virtualized servers on an on-premises private infrastructure or public cloud. PCF delivers a turnkey experience for scaling and updating applications with no downtime.

Combining Pivotal Cloud Foundry with Dell EMC XC Series Hyper-converged appliance with vSphere, enterprises can create a full-featured, tightly integrated cloud platform based on open technologies.

This document provides the instructions for deploying PCF onto Dell EMC XC Series appliances in a VMware vSphere environment.

1 Introduction

This guide details the necessary steps to deploy and configure Pivotal Cloud Foundry (PCF) in a VMware vSphere environment on a standard configuration using XC Series appliances. For more information, refer to the latest Pivotal guide located at <http://docs.pivotal.io/pivotalcf/>.

1.1 Audience

This document is intended for decision makers, managers, architects, cloud administrators, developers, and technical administrators of IT environments who want a solution guide that demonstrates how to deploy Pivotal Cloud Foundry (PCF) on a Dell EMC XC Series cluster in a VMware vSphere environment. This guide also goes into some details for creating orgs/spaces/users and pushing apps for multiple frameworks. You must be familiar with Dell EMC XC Series, Pivotal technologies, VMware vSphere technologies, and have a basic familiarity with storage, compute, and network technologies.

Business and end-user readers of this document must be familiar with general IT, cloud technologies, and have an understanding of the relationship between their business, IT, and the application development requirements that are part of multiple business units.

1.2 Infrastructure

The infrastructure for Pivotal Cloud Foundry (PCF) on VMware vSphere in a standard configuration using XC Series appliances is defined in the *Dell EMC XC Series Pivotal Cloud Foundry Reference Architecture* document. This guide assumes you have read that document prior to doing this deployment.

1.3 Prerequisites

There are several prerequisites that must be in place before starting the PCF install. Review the general requirements for installing PCF on vSphere under [vSphere Requirements](#). Below is additional information that will be helpful. We have also included a deployment checklist for information you will need throughout this deployment. Before you begin, fill out what you can of the [Checklist](#) at the end of document and complete the following list of prerequisites.

Note: This deployment assumes you have read and understood the *Dell EMC XC Series Pivotal Cloud Foundry Reference Architecture* document and that you have successfully deployed an XC Series cluster with vSphere.

Table 1 Prerequisites for setting up PCF

Prerequisite	Definition
Minimum of 36 IPs	Because we are using DHCP, an exclusion range was created for these IPs so that DHCP does not hand out addresses in this range. Checklist item #1.
Load balancer considerations	If you do not have a load balancer and will be using the included HAProxy, pick one IP address in the reserved range above. That IP will be for the HAProxy. Most of the rest of the

Prerequisite	Definition
	IPs are assigned automatically. Write this HAProxy/Load Balancer IP in the Checklist item #7.
NTP	Necessary for timesync.
Create two (2) wildcard DNS entries	These should be in the format of: <code>*.apps.YourDomain.YourTopLevelDomain</code> <code>*.system.YourDomain.YourTopLevelDomain</code> Both should point to your load balancer or the HAProxy IP.
Resolve ESXi port issues	If you have recently setup ESXi 6.0 U1, there are two bugs that must be resolved before you can import the OpsManager OVA. On Step 1 of Deploying an OVF template, we received an error message that said <i>The source OVF uses networks but the destination host does not have any networks configured</i> . Follow the Resolution steps for both of the following KBs, in this order, on your vCenter server. Then restart your vCenter server. <ul style="list-style-type: none"> • KB 2125229 – “You do not have permissions to view this object or this object does not exist” in vSphere Web Client. This happens when going to Administration in vSphere Web Client. • KB 2120255 – Unable to access new Administration and Licensing features in vSphere Web Client 6.0.
Set up an SMTP server (recommended)	Use an SMTP server for notifications. Write in the Checklist item #9.
Pivotal Network Account	Account to login and download products from Pivotal Network . Checklist item #15. Use your corporate security recommendations to manage your credentials.

In addition to being a common practice, Dell EMC recommends creating a VM for all of the tools required in this environment. You must join this VM to the same domain and it is where you will do most of your management of the XC cluster and Pivotal Cloud Foundry. We created a Windows VM with the apps below. There may also be versions of these or similar apps for other platforms, such as Linux. Table 2 shows a list of suggested apps to install and links to where you can download them.

Table 2 List of suggested apps to install

Tool	Definition
VMware vSphere WebClient	Web-based client that connects to vCenter to manage an ESXi environment. Comes with VMware vCenter.
cf CLI	Cloud Foundry command line interface.
Notepad++	Text editor that supports tabbed editing.
Git for Windows	Lightweight set of GIT tools for use inside Windows.

Tool	Definition
Putty	Versatile tool for connecting to other machines or services.
WinSCP	SFTP/FTP Windows Secure Copy tool.

1.4 Assumptions

- The reader has read and understood the *Dell EMC XC Series Pivotal Cloud Foundry Reference Architecture* document. See Dell EMC Tech Center at <http://en.community.dell.com/techcenter/storage/w/wiki/11457.advanced-materials>.
- The reader has working knowledge to deploy, manage, and update the Dell EMC XC Series cluster. For additional documentation, see the **Dell.com/XCseriesmanuals** page.
- The Dell EMC XC Series cluster has been deployed and updated to the latest firmware and drivers. For the latest drivers and firmware visit the Dell EMC XC Series product support page.

2 Deploying and configuring Operations Manager

This section describes how to deploy and configure Operations Manager and Operations Manager Director. Operations Manager for Pivotal Cloud Foundry (PCF) provides a graphical interface to manage the deployment and upgrade of PCF components like Elastic Runtime, additional services and partner products.

2.1 Deploying Operations Manager to vSphere

For more information, go to the Pivotal page for [Deploying Operations Manager to vSphere](https://network.pivotal.io/products/ops-manager#/releases/4584).

Secure | <https://network.pivotal.io/products/ops-manager#/releases/4584>

Pivotal Network

Pivotal Cloud Foundry Operations Manager

[Get email updates](#)

[PRODUCT OVERVIEW](#)

Releases: 1.9.6

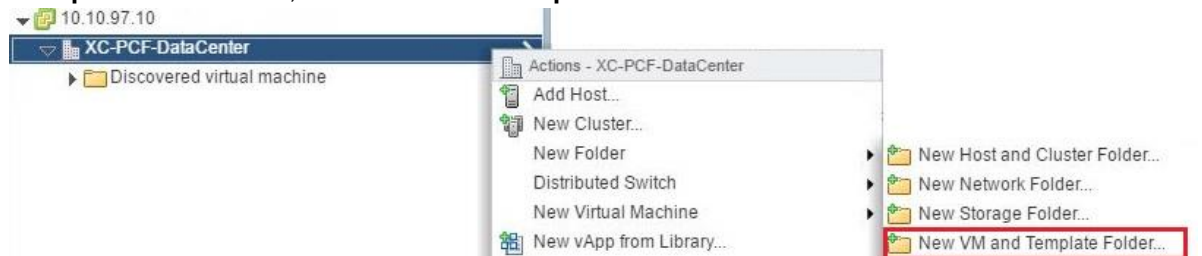
Release Download Files		
	Pivotal Cloud Foundry Ops Manager YAML for Azure - 1.9.6	366 Bytes 1.9.6
	Pivotal Cloud Foundry Ops Manager YAML for GCP - 1.9.6	128 Bytes 1.9.6
	Pivotal Cloud Foundry Ops Manager for Azure - 1.9.6	4.15 KB 1.9.6
	Pivotal Cloud Foundry Ops Manager for GCP - 1.9.6	3.78 KB 1.9.6
	Pivotal Cloud Foundry Ops Manager for AWS - 1.9.6	3.3 KB 1.9.6
	Pivotal Cloud Foundry Ops Manager YAML for AWS - 1.9.6	267 Bytes 1.9.6
	Pivotal Cloud Foundry BOSH Assets - 1.9.6	2.29 GB 1.9.6
	Pivotal Cloud Foundry Ops Manager for OpenStack - 1.9.6	4.39 GB 1.9.6
	Pivotal Cloud Foundry Ops Manager for vSphere - 1.9.6	2.52 GB 1.9.6

1. Navigate to the [Pivotal Cloud Foundry Ops Manager for vSphere](https://network.pivotal.io/products/ops-manager#/releases/4584) page to download the latest version or use the drop-down list to select a previous version. You must have a Pivotal account and must log in before you can download. Use your corporate security recommendations to manage your credentials for checklist item #15 at the end of this document.

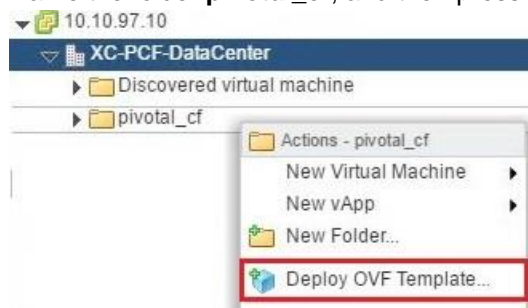
2. Select the latest Ops Manager release. Version 1.9.6 was used for this guide.



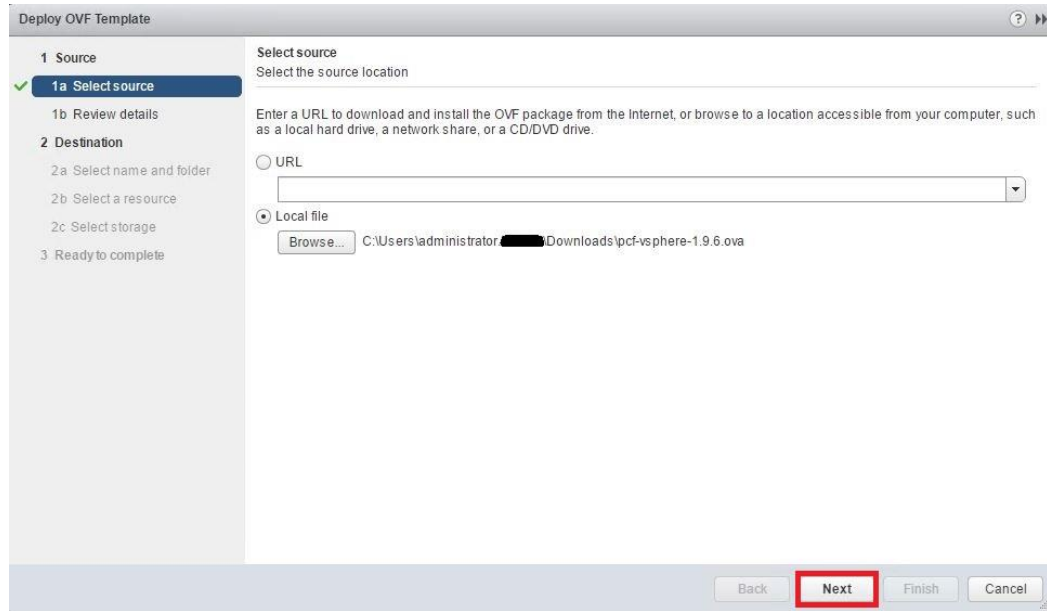
3. In **vSphere Web Client**, select **VMs and Templates**.



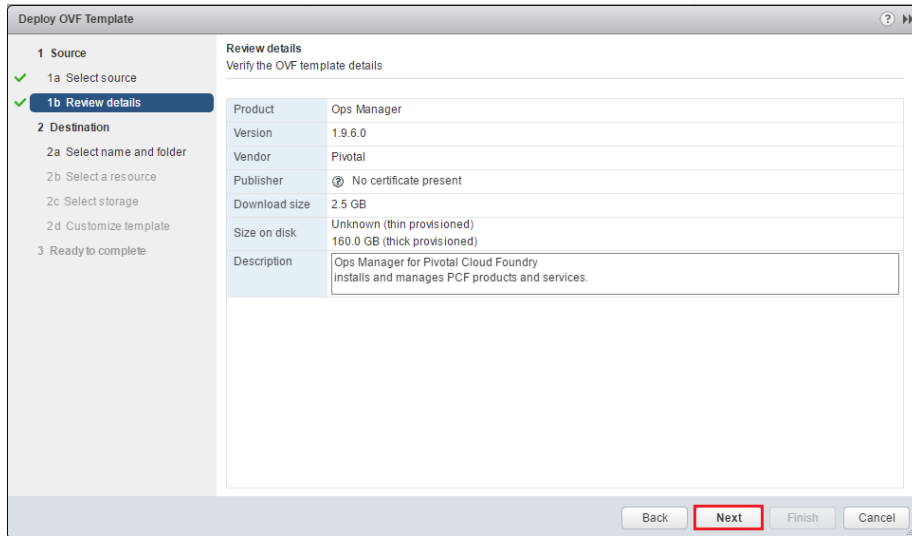
4. Write down the name of your DataCenter in the Checklist, item #12. Then right click your datacenter, and then select **New Folder > New VM and Template Folder**.
5. Name the folder **pivotal_cf**, and then press **OK**.



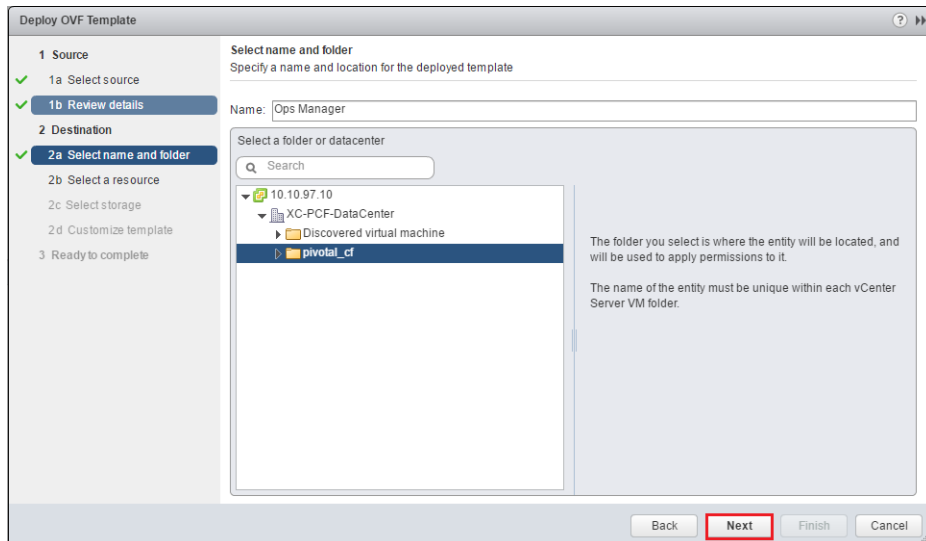
6. Right-click the new `pivotal_cf` folder and select **Deploy OVF Template**.



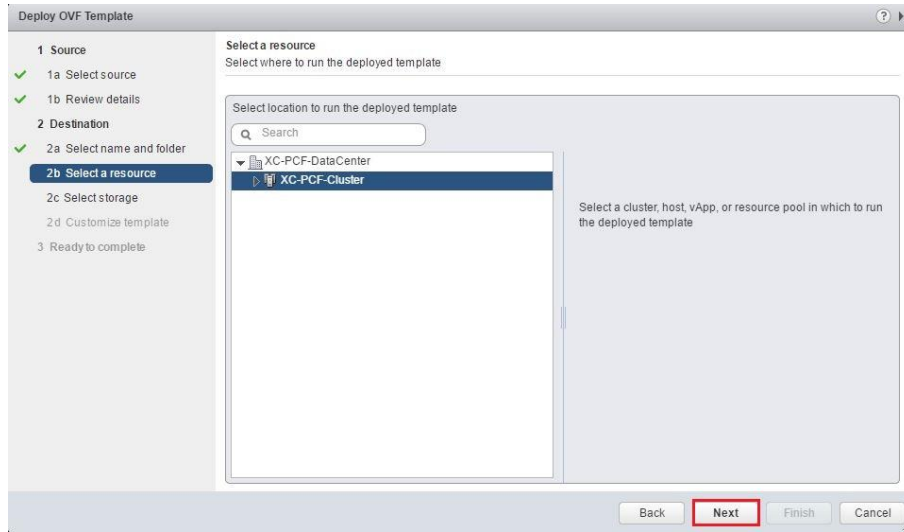
7. In the **Select source** screen, browse to and select the Pivotal Cloud Foundry Ops Manager for vSphere .ova file that you downloaded and click **Next**.



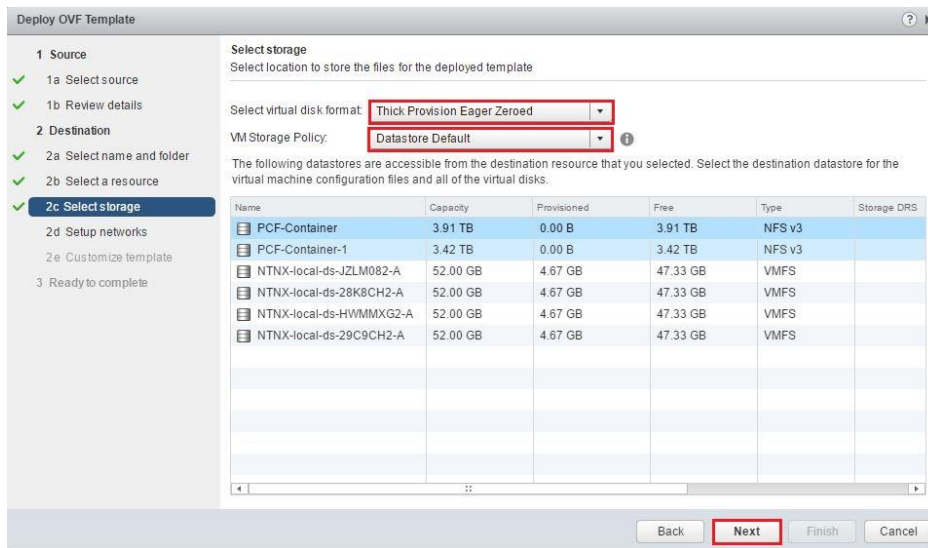
8. In the **Review details** screen, review the details page and click **Next**.



9. In the **Select name and folder** screen, name the VM and select the `pivotal_cf` folder you created earlier and then click **Next**.



10. In the **Select a resource** screen, select your XC cluster. Write down this cluster name in the Checklist, item #11. Then click **Next**.



11. In the **Select storage** screen, **select a virtual disk format**, **VM Storage Policy**, and highlight the datastore you want to use, which should have a minimum of 2 TB available. Write down the name of this datastore in the Checklist, item #13.
12. Click **Next**.

Note: For more information about formats, go to [Provisioning a Virtual Disk](#).

Deploy OVF Template

1 Source

- 1a Select source
- 1b Review details

2 Destination

- 2a Select name and folder
- 2b Select a resource
- 2c Select storage
- 2d Setup networks**
- 2e Customize template

3 Ready to complete

Setup networks
Configure the networks the deployed template should use

Source	Destination	Configuration
Network 1	VM Network	

IP protocol: IPv4 IP allocation: Static - Manual

Source: Network 1 - Description
Logical network used by this appliance.

Destination: VM Network - Protocol settings
No configuration needed for this network.

Back Next Finish Cancel

13. In the **Setup networks** screen, select a network. Write down the name of this network in the checklist, item #14. Click **Next**.

Deploy OVF Template

1 Source

- 1a Select source
- 1b Review details

2 Destination

- 2a Select name and folder
- 2b Select a resource
- 2c Select storage
- 2d Setup networks**
- 2e Customize template**

3 Ready to complete

Customize template
Customize the deployment properties of this software solution

All properties have valid values Show next... Collapse all...

▼ Uncategorized 7 settings

IP Address The IP address for the Ops Manager. Leave blank if DHCP is desired.
10.10.97.50

Netmask The netmask for the Ops Manager's network. Leave blank if DHCP is desired.
255.255.255.128

Default Gateway The default gateway address for the Ops Manager's network. Leave blank if DHCP is desired.
10.10.97.126

DNS The domain name servers for the Ops Manager (comma separated). Leave blank if DHCP is desired.
10.10.97.1,10.10.82.190,10.10.82.191

NTP Servers Comma-delimited list of NTP servers
10.10.97.1

Admin Password This password is used to SSH into the Ops Manager. The username is 'ubuntu'.
Enter password:
Confirm password:

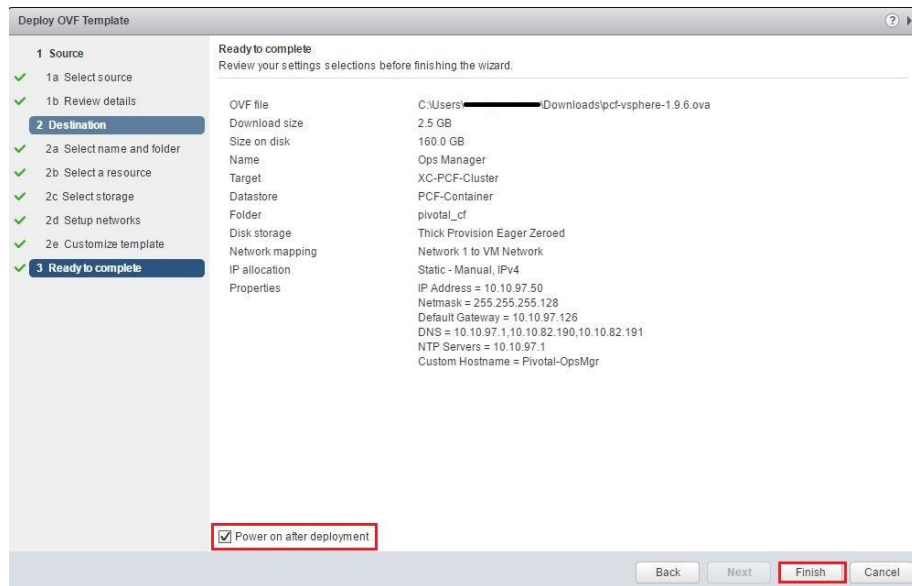
Custom Hostname This will be set as the hostname on the VM. Default: 'pivotal-ops-manager'.
Pivotal-OpsMgr

Back Next Finish Cancel

14. In the **Customize Template** screen, do the following:
- Type your network information.
 - Create an admin password.
 - Set a hostname for this VM. This IP Address for Ops Manager should be one you pick in the reserved range.
 - Write the IP Address in the Checklist item #6.
 - Netmask = Checklist item #3.
 - Gateway = Checklist item #4.

- iv. DNS = Checklist item #5.
- v. NTP = Checklist item #8.
- vi. Admin password = Checklist #17.
- vii. The SSH username is always Ubuntu and is entered for you on the Checklist item #17.

15. Click **Next**.



16. In the **Ready to complete** screen, review information. Select the **Power on after deployment** check box.

17. Click **Finish**.

This deploys the Ops Manager VM to the `pivotal_cf` folder you created under your cluster.

2.2 Configuring Operations Manager Director for vSphere

For more information, go to [Configuring Operations Manager Director for vSphere](#). Any field with a red asterisk (*) is mandatory. For more information about configuration options, see the online [Pivotal Documentation](#). The following steps cover the mandatory options and what Dell EMC set for a successful deployment.

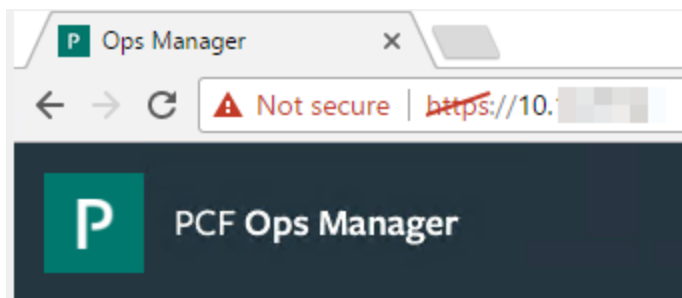
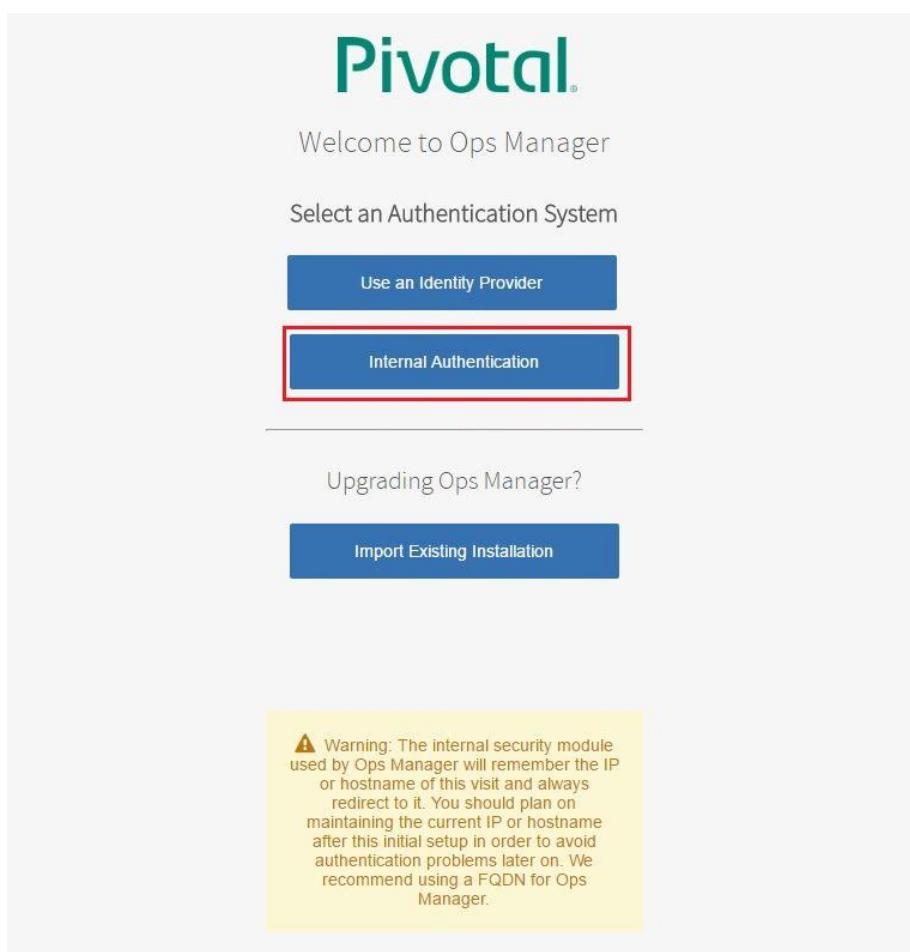


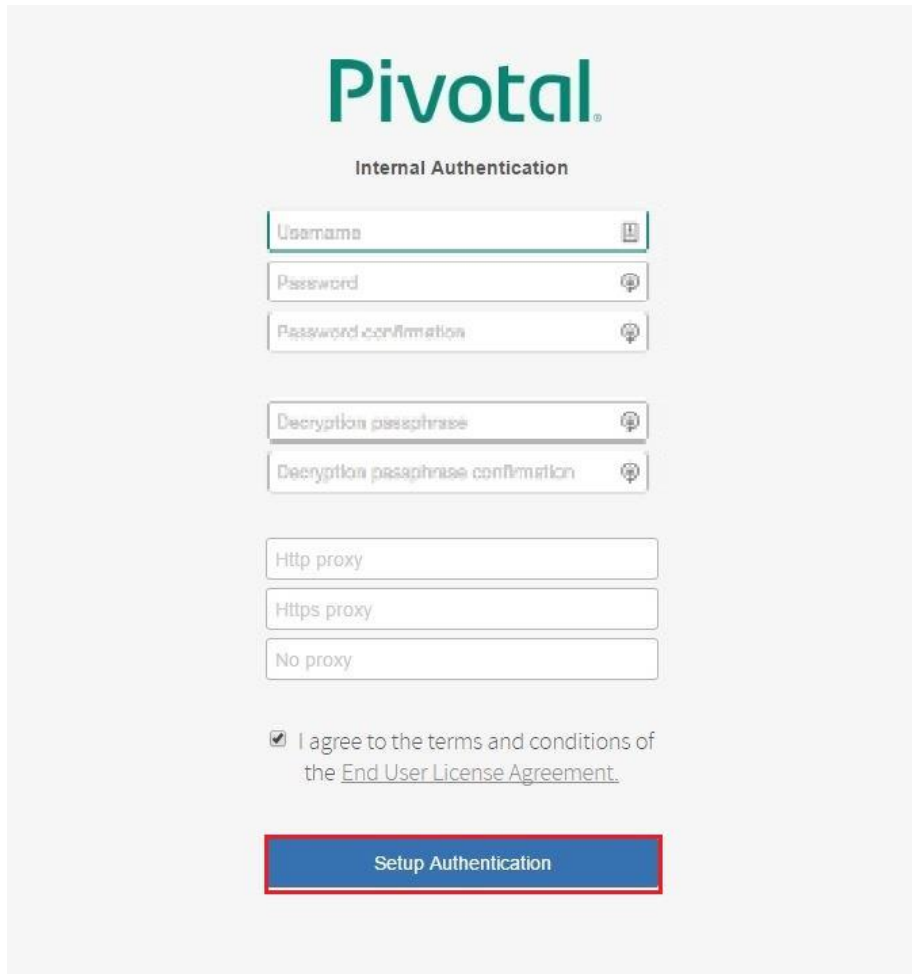
Figure 1 In a browser, navigate to the domain name or IP of your new Ops manager.

1. In a browser, navigate to the fully qualified domain name or IP of your new Ops Manager. For the IP address, see step 13 or 14 in the prior section, or Checklist item #6.



2. The first time you start Ops Manager, you must select one of the following. You can find more information from the provided Pivotal links.
 - [Use an Identity Provider](#), such as an external server that maintains your user database.
 - [Internal Authentication](#), PCF maintains your user database. We use this option for this guide.

Important: The internal security module used by Ops Manager remembers the IP or hostname of this visit and always redirects to it. If you select this option, you must maintain this current IP or hostname to avoid authentication issues in the future. An FQDN is recommended by Pivotal.

The image shows a web form titled "Pivotal Internal Authentication". 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 proxy-related fields: "Http proxy", "Https proxy", and "No proxy". A checkbox is present with the text "I agree to the terms and conditions of the [End User License Agreement](#)". At the bottom of the form is a blue button with the text "Setup Authentication".

Pivotal

Internal Authentication

Username

Password

Password confirmation

Decryption passphrase

Decryption passphrase confirmation

Http proxy

Https proxy

No proxy

☒ I agree to the terms and conditions of the [End User License Agreement](#).

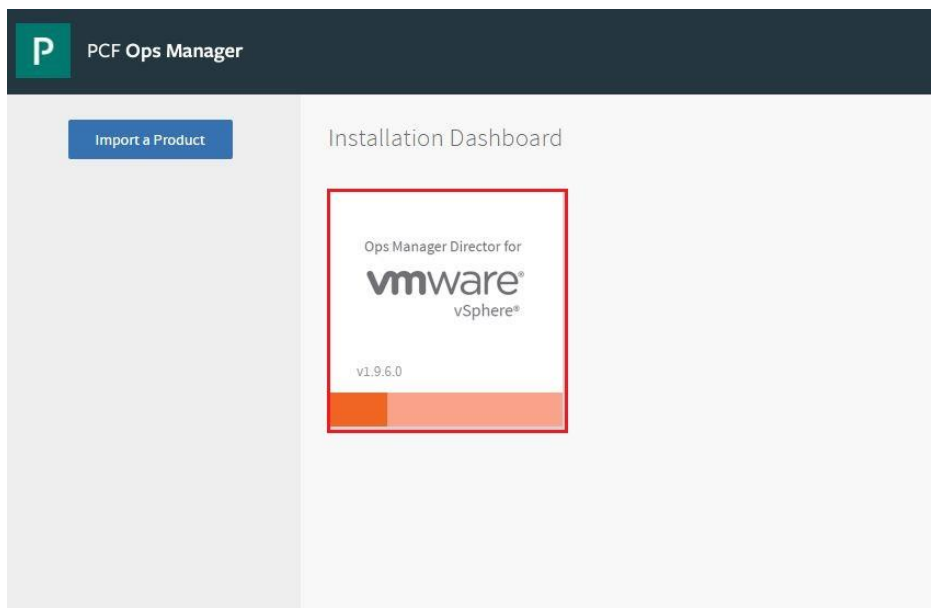
Setup Authentication

3. In the **Internal Authentication** dialog box, complete the following steps:
 - a. Enter a **Username**, **Password**, and **Password Confirmation**. Write this into the Checklist item #18. Use your corporate security recommendations for handling credentials.
 - b. Enter a Decryption passphrase and the Decryption passphrase confirmation. Write this into the Checklist item #21. Use your corporate security recommendations for handling credentials.
 - c. If you are using an Http or Https proxy, follow the [PCF Director Proxy Settings](#) instructions. We left them blank.
 - d. Read the terms and conditions and select the select box to accept.
 - e. Click **Setup Authentication**.

Note: This passphrase encrypts the Ops Manager datastore and is not recoverable.



4. In the **Pivotal log in** dialog box, log in to Ops Manager with the admin credentials you created in the previous step (Checklist item #18). Use the same format you entered previously. It does not have to be in email format.



5. In the **Installation Dashboard** screen, click the **Ops Manager Director** tile.

6. On the **Settings** tab, in the left pane, click **vCenter Config** and configure the following:
 - a. **vCenter Host**: The hostname, or IP, of the vCenter that manages vSphere. Checklist item #10
 - b. **vCenter Username**: A vCenter username with create and delete privileges for virtual machines (VMs) and folders. Checklist item #16.
 - c. **vCenter Password**: The password for the vCenter used, which was specified above. Checklist item #16.
 - d. **Datacenter Name**: The name of the datacenter as it appears in vCenter. Checklist item #12.
 - e. **Virtual Disk Type**: The Virtual Disk Type to provision for all VMs. For guidance on the virtual disk type to select, see [Provisioning a Virtual Disk in vSphere](#).
 - f. **Ephemeral Datastore Names (comma delimited)**: The names of the datastores that store ephemeral VM disks deployed by Ops Manager. This was the same as the datastore we selected during the install of Ops Manager. Checklist item #13.
 - g. **Persistent Datastore Names (comma delimited)**: The names of the datastores that store persistent VM disks deployed by Ops Manager. This was also the same as the datastore we selected during the install of Ops Manager. Checklist item #13.
 - h. **VM Folder**: What you would like the vSphere datacenter folder to be named (default: pcf_vms). This is where Ops Manager places VMs.
 - i. **Template Folder**: What you would like the vSphere datacenter folder to be named (default: pcf_templates). This is where Ops Manager places VM Templates.
 - j. **Disk path Folder**: What you would like the vSphere datastore folder to be named (default: pcf_disk). This is where Ops Manager creates attached disk images. You must not nest this folder.
 - k. Click **Save**.

Settings updated

Installation Dashboard

Ops Manager Director

SettingsStatusCredentials

✓ vCenter Config

✓ Director Config

✓ Create Availability Zones

✓ Create Networks

○ Assign AZs and Networks

✓ Security

✓ Resource Config

Director Config

NTP Servers (comma delimited)*
10.10.97.1
One or more NTP server addresses for consistent and valid time stamps used

Metrics IP Address

☐ Enable VM Resurrect 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 both deploy retries
This will attempt to re-deploy a failed deployment up to 5 times.

☐ Keep Unreachable Director VMs

☐ HM Pager Duty Plugin
Service Key*

HTTP Proxy

☐ HM Email Plugin
Host*

Port*

Domain*

From*

The screenshot shows a configuration form with two main sections: Blobstore Location and Database Location. The Blobstore section has radio buttons for 'Internal' (selected) and 'S3 Compatible Blobstore'. Below are input fields for 'S3 Endpoint*', 'Bucket Name*', 'Access Key*', 'Secret Key*', and 'Region*'. There are also radio buttons for 'V2 Signature' (selected) and 'V4 Signature'. The Database section has radio buttons for 'Internal' (selected) and 'External MySQL Database'. Below are input fields for 'Host*', 'Port*', 'Username*', 'Password*', and 'Database*'. At the bottom are input fields for 'Max Threads' and 'Director Hostname', followed by a blue 'Save' button.

Blobstore Location

☒ Internal

☐ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

☒ V2 Signature

☐ V4 Signature

Region*

Database Location

☒ Internal

☐ External MySQL Database

Host*

Port*

Username*

Password*

Database*

Max Threads

Director Hostname

Save

7. Click **Director Config** and do the following:
 - a. In the **NTP Servers (comma delimited)** field, type your NTP server addresses. We set up our Domain Controller as an NTP server and typed that IP here. Checklist item #8.
 - b. Leave all other options cleared and set to defaults.
 - c. Click **Save**.

Successfully verified availability zone settings

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 Availability Zones

Availability Zones
Clusters and resource pools to which you will deploy Pivotal products

➤ XC-PCF-Zone1

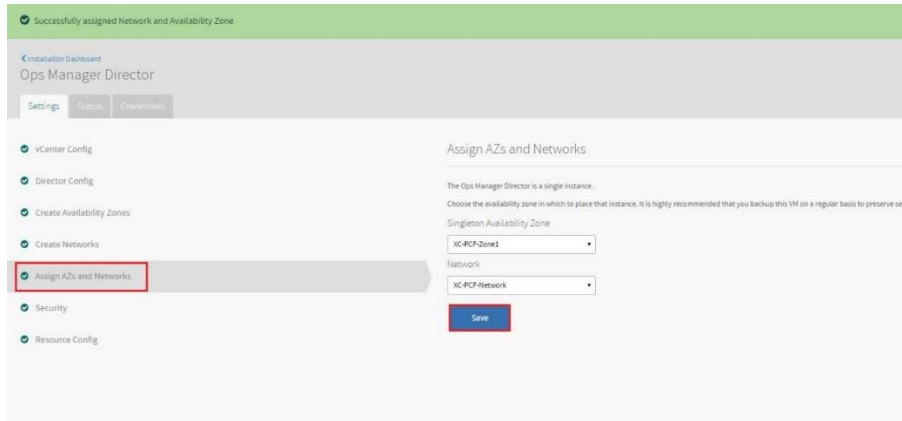
Name*

Cluster*

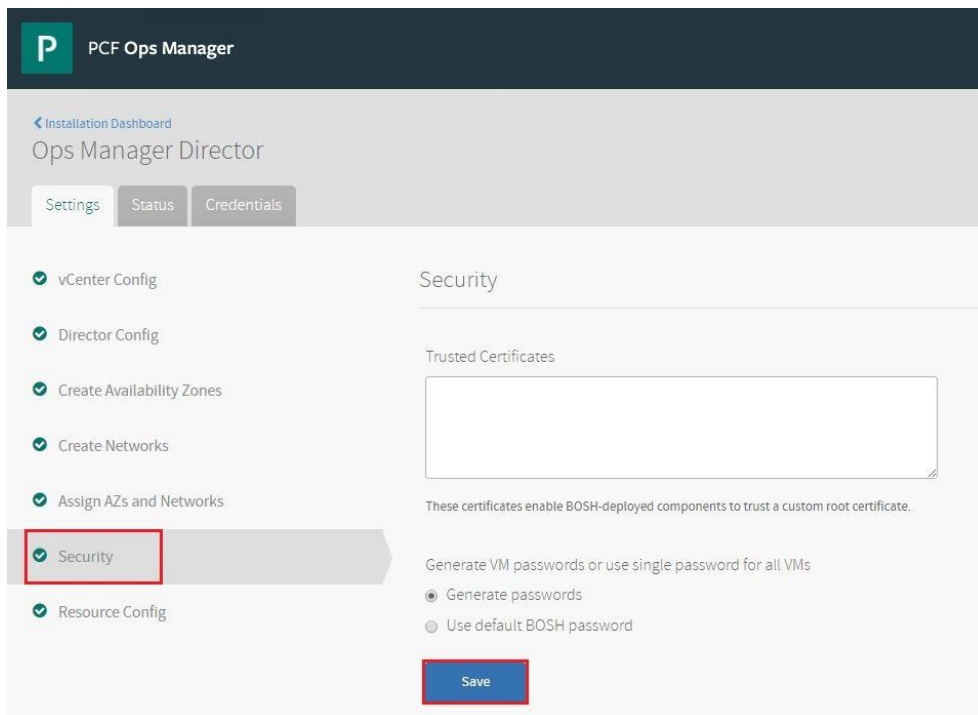
Resource Pool
 The name of the resource pool to limit resources that Ops Manager deployed VMs will use

8. In the left pane, click **Create Availability Zones**.
 - a. Click **Add**.
9. In the **Create Availability Zones** form do the following:
 - a. Type a unique **Name** for the Availability Zone.
 - b. Type the name of your existing vCenter **Cluster** to use as an Availability Zone. Checklist item #11.
 - c. Click **Save**.

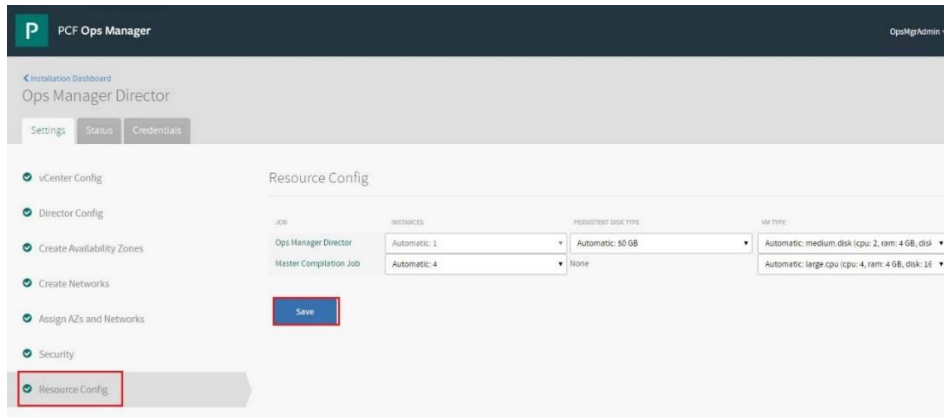
10. In the left pane, click **Create Networks**.
11. In the **Create Networks** form, do the following:
 - a. To enable ICMP on your networks, select **Enable ICMP checks**. Ops Manager uses ICMP checks to confirm that components within your network are reachable.
 - b. Use the following steps to create one or more Ops Manager networks:
 - i. Click **Add Network**.
 - ii. Type a unique **Name** for the network.
 - c. To create one or more subnets for the network, click **Add Subnet**.
 - i. Type the full path and **vSphere Network Name** as it displays in vCenter. Checklist item #14.
 - ii. For **CIDR**, type the valid CIDR notation of this block of IPs in which to deploy VMs. For example, 10.x.x.0/25. Checklist item #1.
 - iii. For **Reserved IP Ranges**, type any IP addresses from the **CIDR** that you want to blacklist from the deployment. Ops Manager will not deploy VMs to any address in this range. Checklist item #2.
 - iv. Type your **DNS** and **Gateway** IP addresses. Checklist items #4 & 5.
 - v. Select which **Availability Zones** to use with the network.
 - d. Click **Save**.



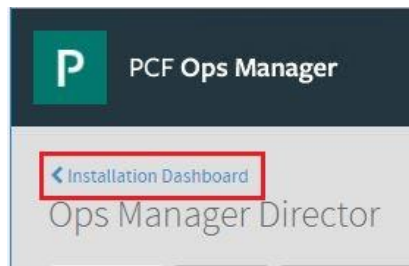
12. On the left, click **Assign AZs and Networks**.
 - a. Use the drop-down menu to select a **Singleton Availability Zone**. The Ops Manager Director installs in this Availability Zone.
 - b. Use the drop-down menu to select a **Network** for your Ops Manager Director.
 - c. Click **Save**.



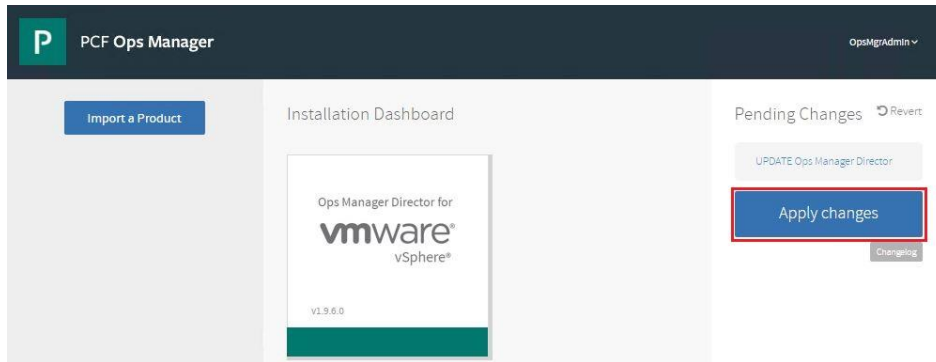
13. In the left pane, click **Security**.
 - a. Leave this at Default settings and click **Save**.



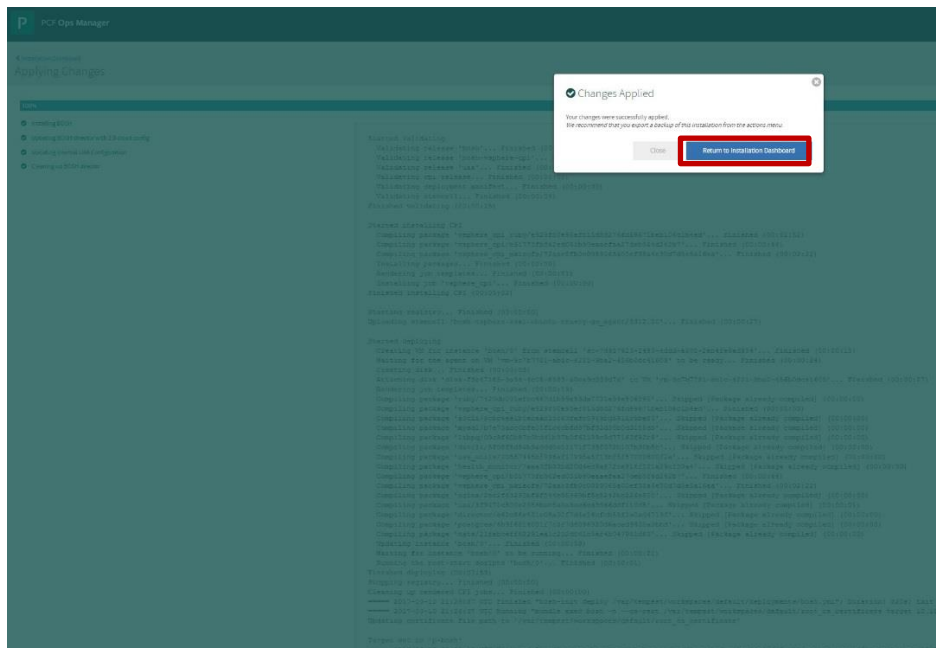
14. In the left pane, click **Resource Config**.
 - a. Leave this at default settings and click **Save**.



15. In the upper left area of the page, click **Installation Dashboard** to go back to the Dashboard.



16. On the right side of the page, click **Apply Changes**. This applies the changes made and deploy Ops Manager Director. When the deployment is complete, you should see the following screen telling you that changes were applied.



17. Click **Return to the Installation Dashboard**.

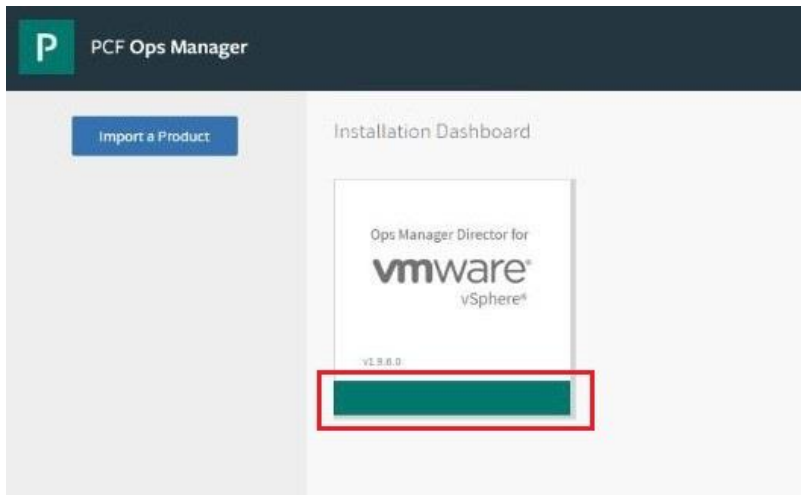


Figure 2 Green bar displays across the bottom of Ops Manager Director.

On the Installation Dashboard you can see the green bar across the bottom of Ops Manager Director tile indicating that it is fully deployed. If the deployment fails, you will continue to see the red bar across the bottom of the tile and you would be taken to the Change Log. There you can click on the Logs link at the end of the row for more information to begin troubleshooting. Troubleshooting it beyond the scope of this guide.

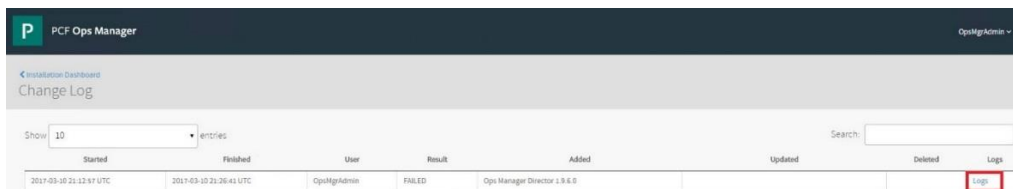


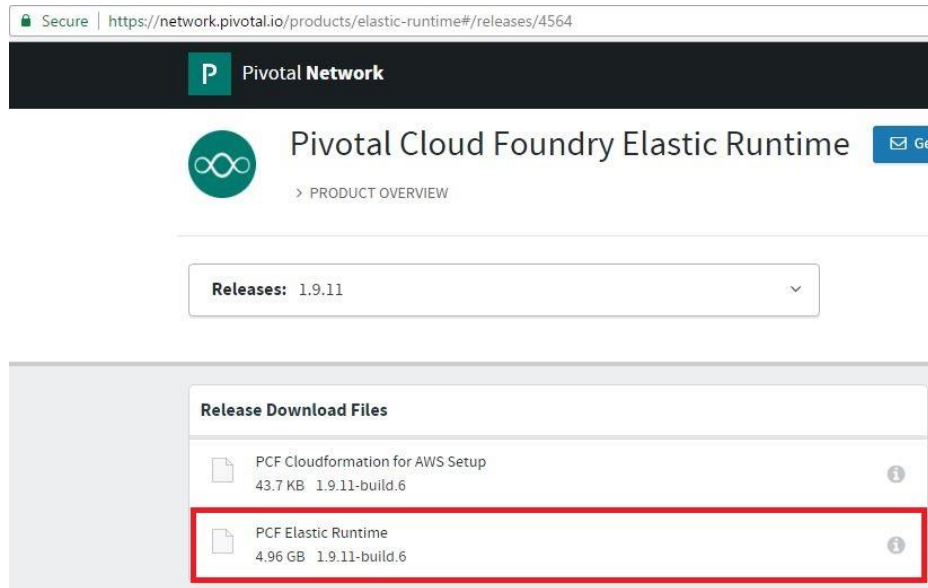
Figure 3 Get the log file if you want more information to help with troubleshooting.

3 Deploying and configuring Elastic Runtime for vSphere

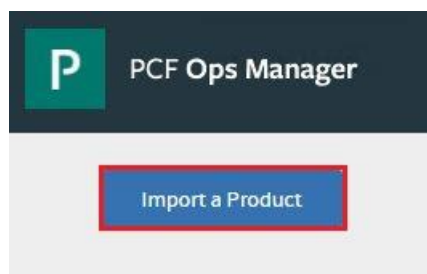
This section covers importing, configuring, and deploying Elastic Runtime for vSphere. For more information, go to the Pivotal page for [Configuring Elastic Runtime for vSphere](#).

3.1 Adding Elastic Runtime to Ops Manager

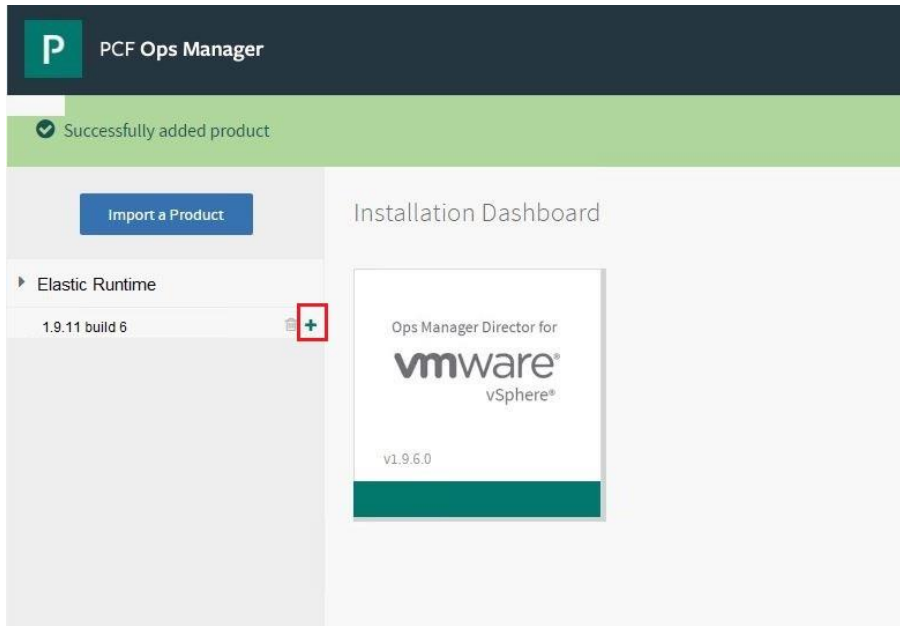
Pivotal Cloud Foundry Elastic Runtime is a complete, scalable runtime environment, extensible to most modern frameworks or languages running on Linux. Deployed applications enjoy built-in services and can automatically bind to new data services through a service broker or to an existing user-provided service.



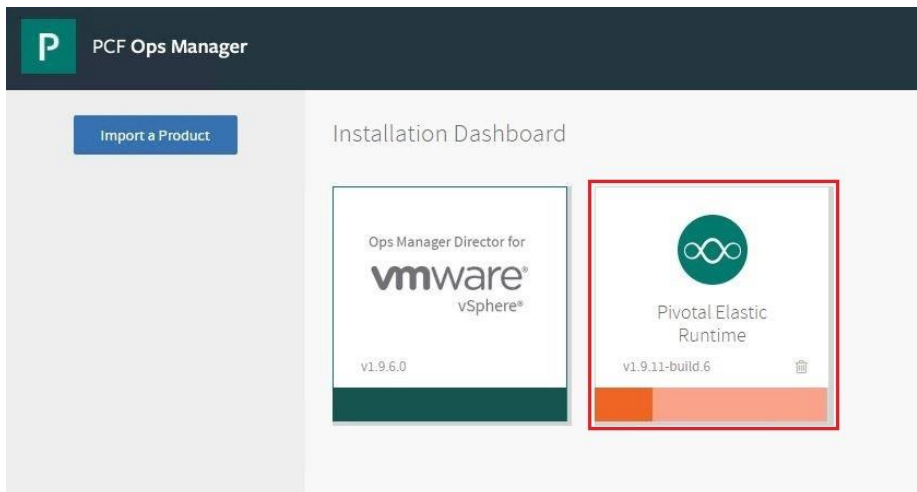
1. Navigate to the [Pivotal Cloud Foundry Elastic Runtime](#) download page. Download the latest version or use the drop-down menu to download a previous release. Version 1.9.11-Build 6 was used for this guide.



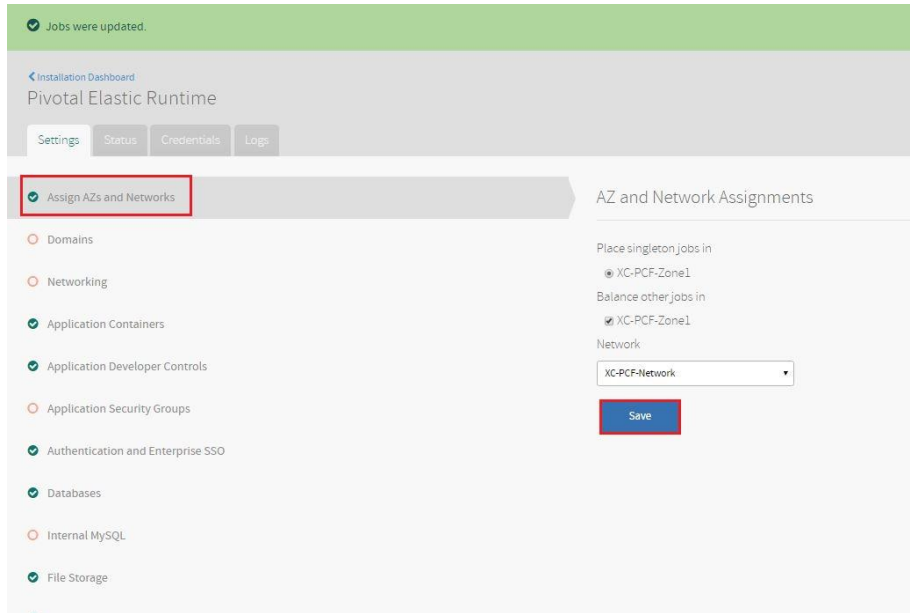
2. In Ops Manager, click **Import a Product** and select the **Elastic Runtime** file you downloaded. This may take a minute or two and then it should show up in the left column.



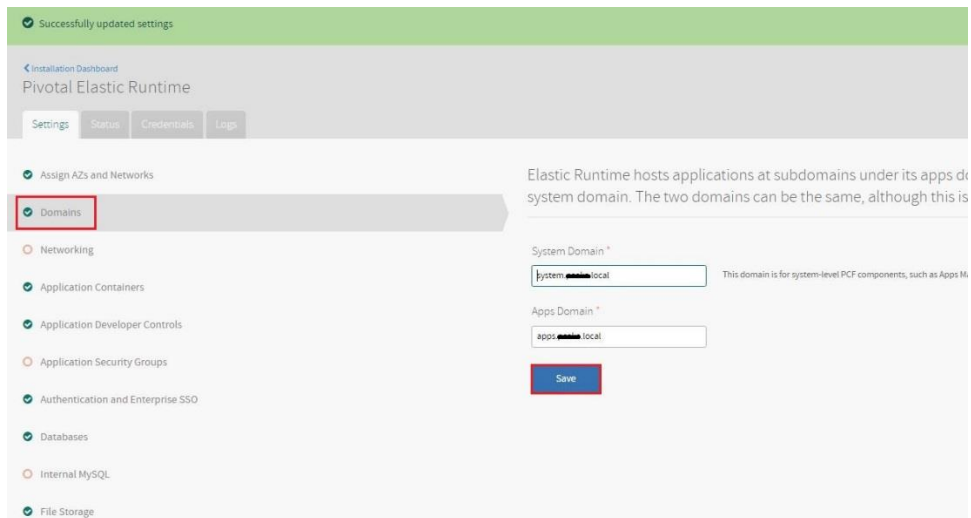
3. Then click the green + to add the Elastic Runtime tile.



4. Click the **Pivotal Elastic Runtime** tile to open the configuration.



5. The first section should already be selected but if not, on the **Settings** tab, click **Assign AZs and networks**.
 - a. The selections should already be set and you can click **Save**.



6. Click **Domains**.
 - a. The **System Domain** defines your target when you push apps to Elastic Runtime. Dell EMC and Pivotal recommend the domain format: `system.YourDomain.YourTopLevelDomain`. Replace the placeholders for your domain and top level domain.
 - b. The **Apps Domain** defines where Elastic Runtime should serve your apps. Dell EMC and Pivotal recommend the domain format: `apps.YourDomain.YourTopLevelDomain`. Replace the placeholders for your domain and top level domain.

- c. These are the domains you set a DNS wildcard entry for mentioned in the [Prerequisites](#).
- d. Click **Save**.

Assign AZs and Networks

Domains

Networking

Application Containers

Application Developer Controls

Application Security Groups

Authentication and Enterprise SSO

Databases

Internal MySQL

File Storage

System Logging

Custom Branding

Apps Manager

Email Notifications

Restore CDR Encryption Key

Smoke Tests

Advanced Features

Endpoints

Resource Config

Storeroom

Configure security and routing services for your platform. It is usually preferable to use your own load balancer instead of an HAProxy.

Router IP:

If you are not using HAProxy, enter static IP address(es) for the Router(s), which must be within the same CIDR block that you defined in the Ops Manager network configuration. If the name of your ELB or the Resource Config section, in the ELB Name column for Router.

SSL Proxy IPs:

HAProxy IPs:

TCP Router IPs:

Select one of the following points-of-ency options:

- ☐ Forward SSL to Elastic Runtime Router. Assumes an external load balancer is configured to forward encrypted traffic.
- ☐ Forward unencrypted traffic to Elastic Runtime Router. Assumes an external load balancer is configured to forward unencrypted traffic.
- ☒ Forward SSL to HAProxy. Use first option. Assumes an external load balancer is configured to forward encrypted traffic.

SSL Certificate and Private Key:

Change

☐ Disable HTTP traffic to HAProxy

HAProxy SSL Ciphers:

Request Max Buffer Size:

☒ Enable SSL certificate verification for this environment

☐ Enable insecure cookies on the Router

Request Max Buffer Size *

16384

☒ Disable SSL certificate verification for this environment

☐ Disable insecure cookies on the Router

☒ Enable Zipkin tracing headers on the router

Choose whether to enable route services. Route services enable you to proxy requests to your app over TLS to arbitrary URLs before hitting your app.

☒ Enable route services

☐ Disable route services

Loggregator Port

Applications Subnet (Only change this if you need to avoid address collision with a third-party service on the same subnet.) *

10.254.0.0/22

Applications Network Maximum Transmission Unit (MTU) (in bytes) *

1454

Router Timeout to Backends (in seconds) (min: 1) *

900

Load Balancer Unhealthy Threshold *

0

Load Balancer Healthy Threshold *

20

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 your app.

☒ Select this option if you prefer to enable TCP Routing at a later time

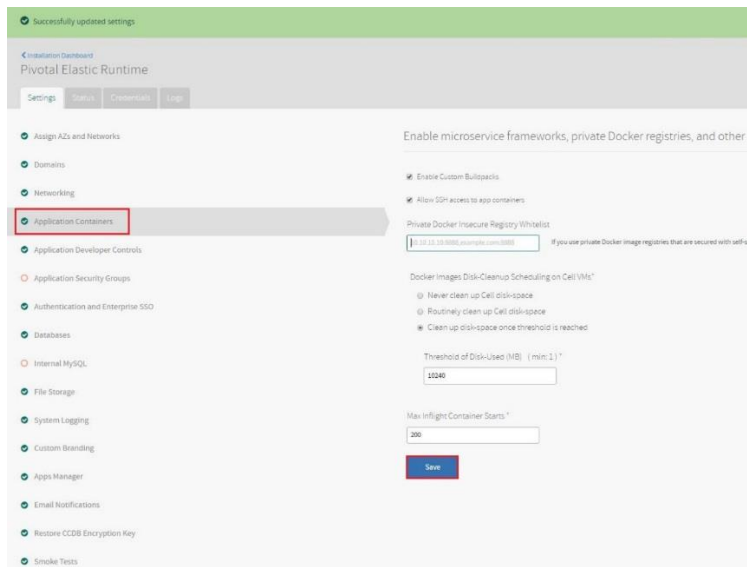
☐ Enable TCP Routing

HTTP Headers to Log

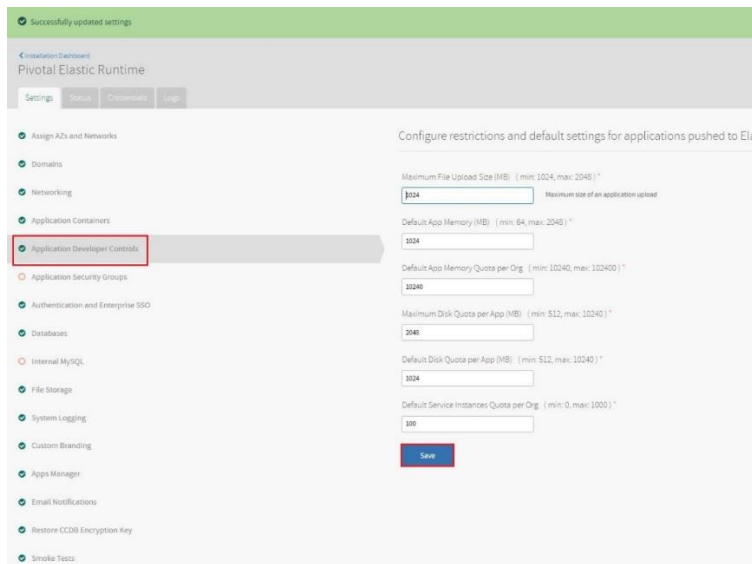
Save

7. Click **Networking**.

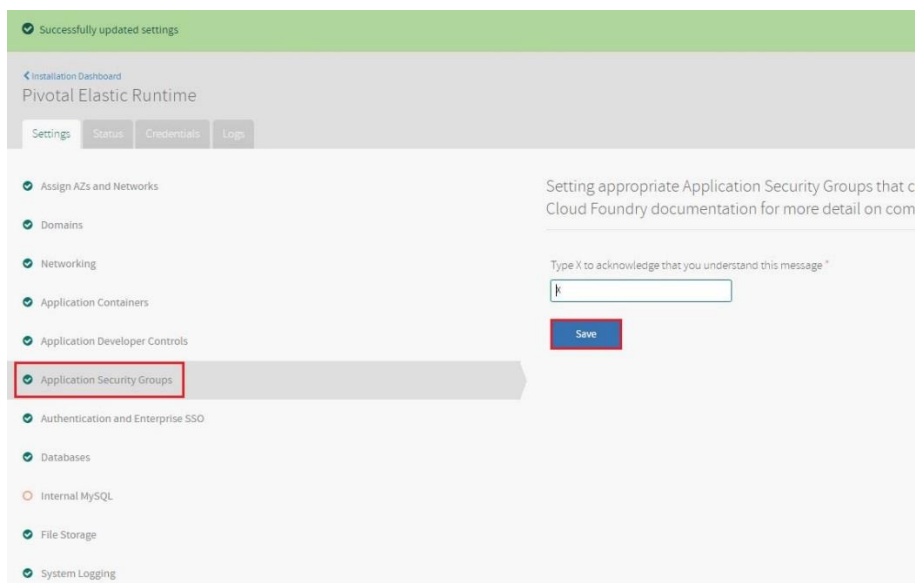
- a. Since we are going to be using the included HAProxy, We added our preselected IP from the reserved range into the HAProxy IPs field. Checklist item #7.
- b. Since we are using HAProxy, under point-of-entry, we selected **Forward SSL to HA Proxy**.
 - i. Click **Generate RSA Certificate**.
- c. Because we are not using SSL encryption, check **Disable SSL certificate verification for this environment**. This is not recommended for production environments.
- d. Leave the rest of the fields blank or set to defaults.
- e. Click **Save**.



8. Click **Application Containers**.
 - a. Leave the rest of the defaults set.
 - b. Click **Save**.

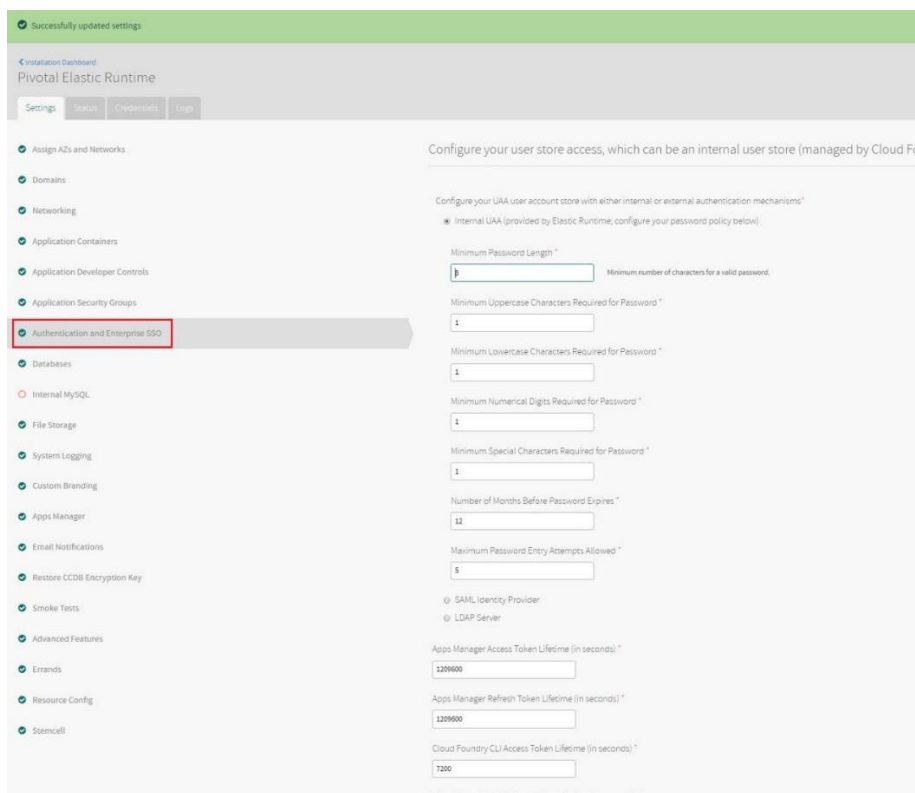


9. Click **Application Developer Controls**.
 - a. Leave the rest of the defaults set.
 - b. Click **Save**.



10. Click **Application Security Groups**.

- Read and understand the message and then follow the directions at the prompt.
- Click **Save**.



Stemcell 1209600

Cloud Foundry CLI Access Token Lifetime (in seconds) *

7200 Set the lifetime of the access token for the Cloud Foundry CLI.

Cloud Foundry CLI Refresh Token Lifetime (in seconds) *

1209600

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

11. Click **Authentication and Enterprise SSO**.

- Set the password policy to match your corporate password policy.
- Leave the rest of the defaults set.
- Click **Save**.

Successfully updated settings

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

Internal MySQL

File Storage

System Logging

Custom Branding

Apps Manager

Place the databases used by Elastic Runtime components like Cloud Controller and

Choose the location of your system databases*

Internal Databases - MySQL and Postgres (the Postgres DBs are not highly-available, but this selection is required)

* Internal Databases - MySQL (preferred for complete high-availability)

External Databases (preferred if, for example, you use AWS RDS)

Save

12. Click **Databases**.

- We selected **Internal Databases – MySQL (preferred for complete high-availability)**.
- Click **Save**.

✓ Successfully updated settings

Installation Dashboard
Pivotal Elastic Runtime

Settings Status Containers Logs

- Assign AZs and Networks
- Domains
- Networking
- Application Containers
- Application Developer Controls
- Application Security Groups
- Authentication and Enterprise SSO
- Databases
 - Internal MySQL**
- File Storage
- System Logging
- Custom Branding
- Apps Manager
- Email Notifications
- Restore CCDB Encryption Key
- Smoke Tests
- Advanced Features
- Errands
- Resource Config
- Stencel

Only configure this section if you selected Internal Databases - MySQL or Internal Da

A proxy tier routes MySQL connections from internal components to healthy cluster can be configured against port 1936.

The automated backups functionality works with any S3-compatible file store that c

MySQL Proxy IPs
 Enter the IP address(es) for the MySQL proxy instances configured on your external load balan

MySQL Service Hostname

Replication canary time period *

Replication canary read delay *

E-mail address (required) *

Automated Backups Configuration*

☒ Disable automated backups of MySQL
☐ Enable automated backups from MySQL to an S3 bucket or other S3-compatible file store
☐ Enable automated backups from MySQL to a remote host via SCP

Server Activity Logging*

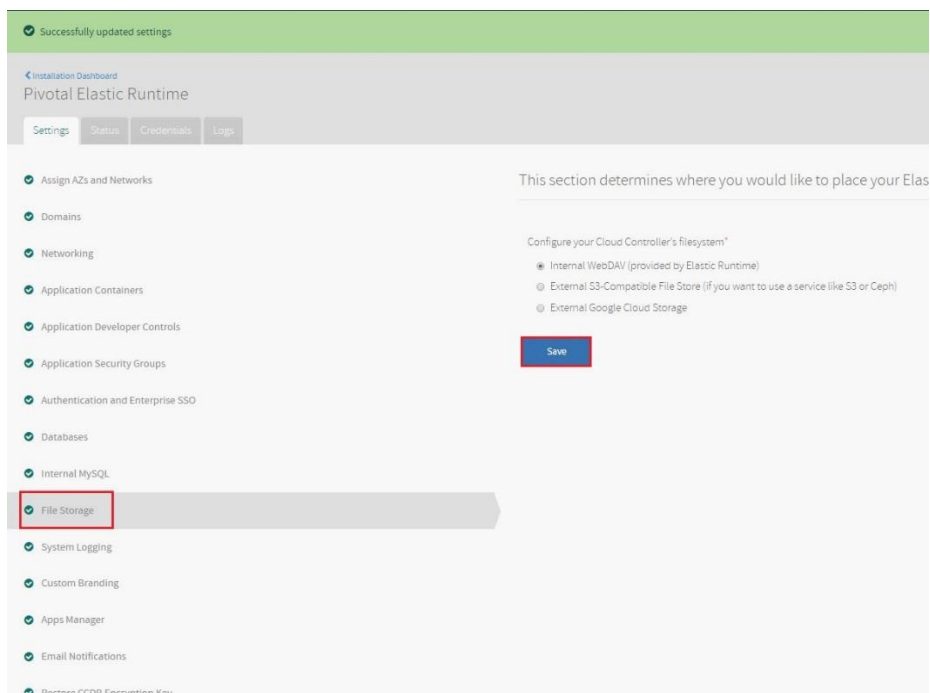
☐ Disable server activity logging
☒ Enable server activity logging

Event types *

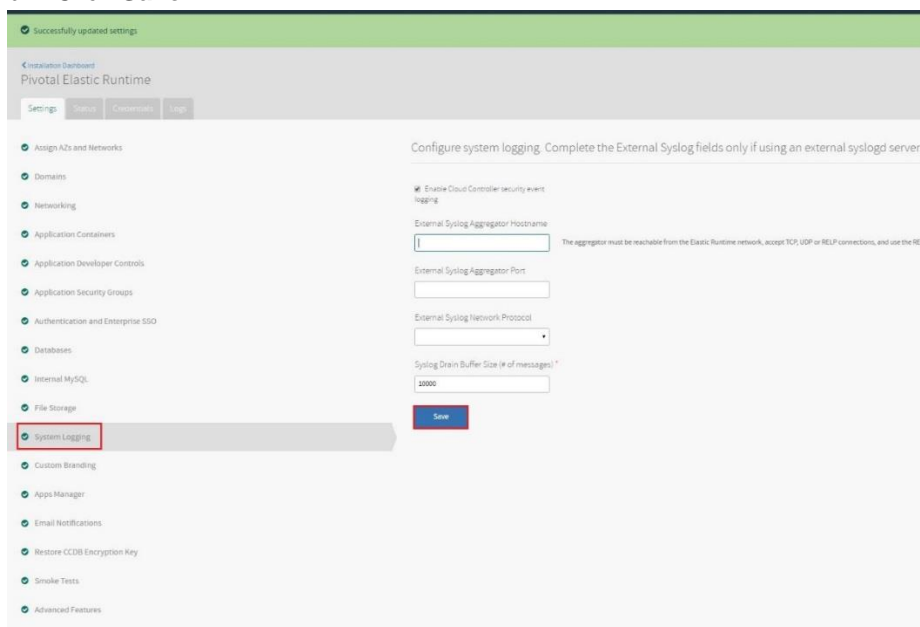
Save

13. Click **Internal MySQL**.

- Add an email address to which alerts can be sent.
- Select **Disabled automated backups of MySQL**, because this guide is based on a proof of concept install, so we are not doing backups.
- Leave all other defaults.
- Click **Save**.



14. Click **File Storage**.
 - a. Select **Internal WebDAV**.
 - b. Click **Save**.



15. Click **System Logging**.
 - a. This section is optional. Dell EMC recommends leaving defaults.
 - b. Click **Save**.

Successfully updated settings

← Installation Environment
Pivotal Elastic Runtime

Settings Status Configuration Logs

- Assign AZs and Networks
- Domains
- Networking
- Application Containers
- Application Developer Controls
- Application Security Groups
- Authentication and Enterprise SSO
- Databases
- Internal MySQL
- File Storage
- System Logging
- Custom Branding**
- Apps Manager
- Email Notifications
- Restore CDB Encryption Key
- Smoke Tests
- Advanced Features
- Errands
- Resource Config
- Storcraft

Customize colors, images, and text for Apps Manager and the Cloud Foundry login portal.

Company Name
Pivotal Defaults to 'Pivotal'

Accent Color
#500000

Main Logo (PNGs only)

Square Logo/Favicon (PNGs only)

Footer Text

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

16. Click **Custom Branding** (Optional).
 - a. Add a **Company Name**.
 - b. Set an **Accent Color**.
 - c. Leave everything else empty.
 - d. Click **Save**.

Successfully updated settings

< 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
- Internal MySQL
- File Storage
- System Logging
- Custom Branding
- Apps Manager**
- Email Notifications

Configure Apps Manager

☐ Display Marketplace Service Plan Prices

Supported currencies as json *
 Define the currency codes and associated symbols (defaults to ["usd": "\$", "eur": "€"])

Product Name

Marketplace Name

Customize Sidebar Links
 You may configure up to 30 links in the Apps Manager sidebar

- Marketplace
- Docs
- Tools

Save

17. Click **Apps Manager**.
 - a. Leave all the defaults.
 - b. Click **Save**.

Successfully updated settings

< 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
- Internal MySQL
- File Storage
- System Logging
- Custom Branding
- Apps Manager
- Email Notifications**
- Restore CCDB Encryption Key

Configure Simple Mail Transfer Protocol for the Notifications application to send email. If you do not need this service, leave this section blank and disable the Notifications application.

From Email
 The email address from which emails are sent.

Address of SMTP Server

Port of SMTP Server

SMTP Server Credentials

Username

Password

☐ SMTP Enable Automatic STARTTLS

SMTP Authentication Mechanism*

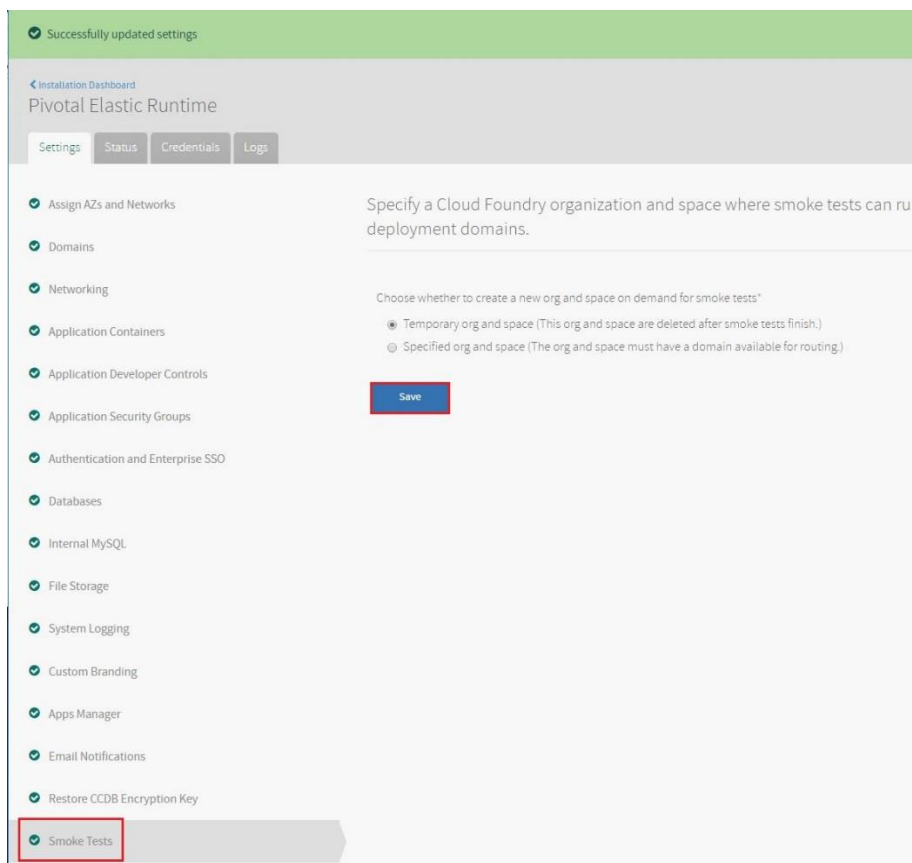
SMTP CRAMMD5 secret

Save

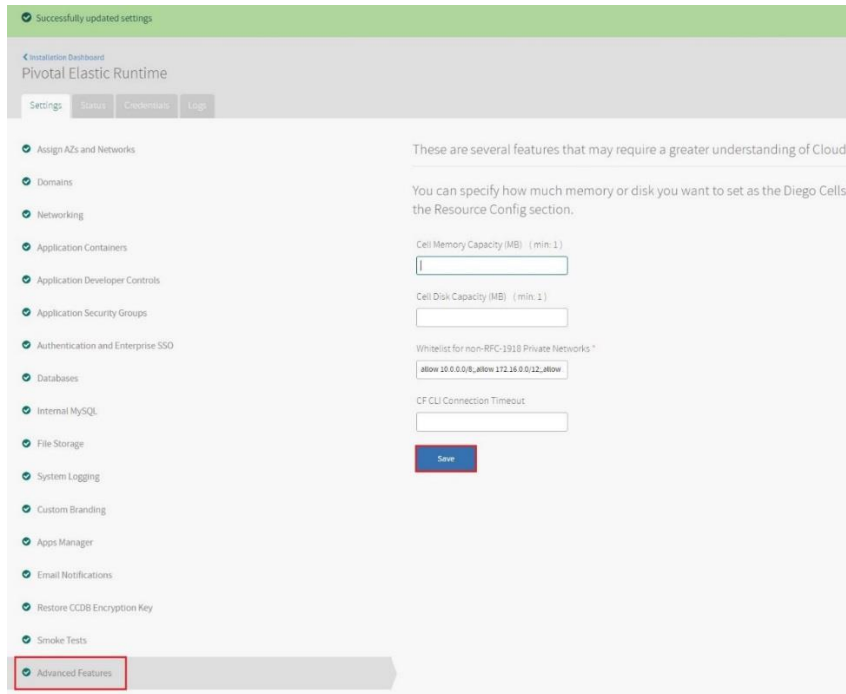
18. Click **Email Notifications**.

- a. Leave all of these blank or defaults. Leaving this section empty requires an Admin user to create all users accounts. Having an SMTP server available and completing this section facilitates user self-registration. SMTP server is Checklist item #9 if you have one.
- b. Click **Save**.

19. Click **Restore CCDB Encryption Key**.
 - a. Leave this blank. This is only necessary on subsequent deployments.
 - b. Click **Save**.

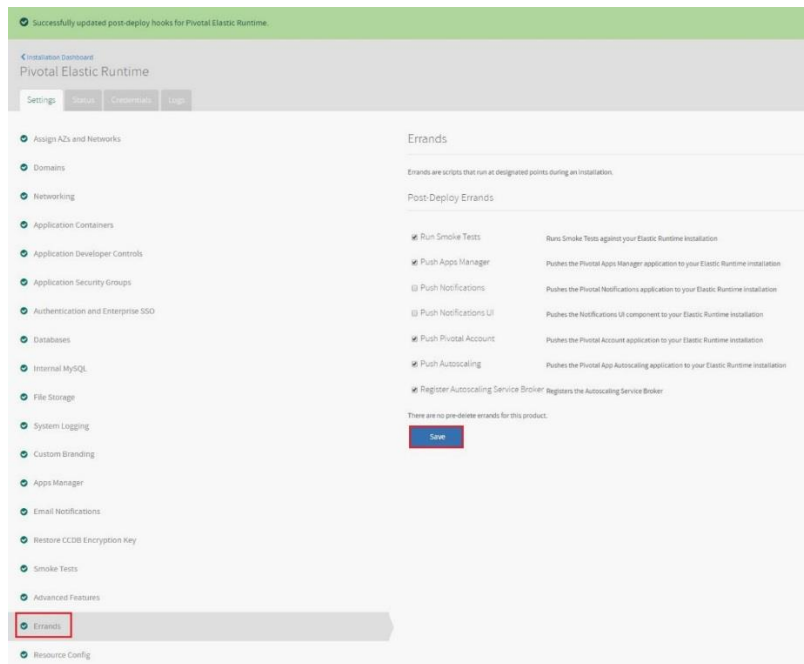


20. Click **Smoke Tests**.
 - a. Select **Temporary org and space**.
 - b. Click **Save**.



21. Click **Advanced Features**.

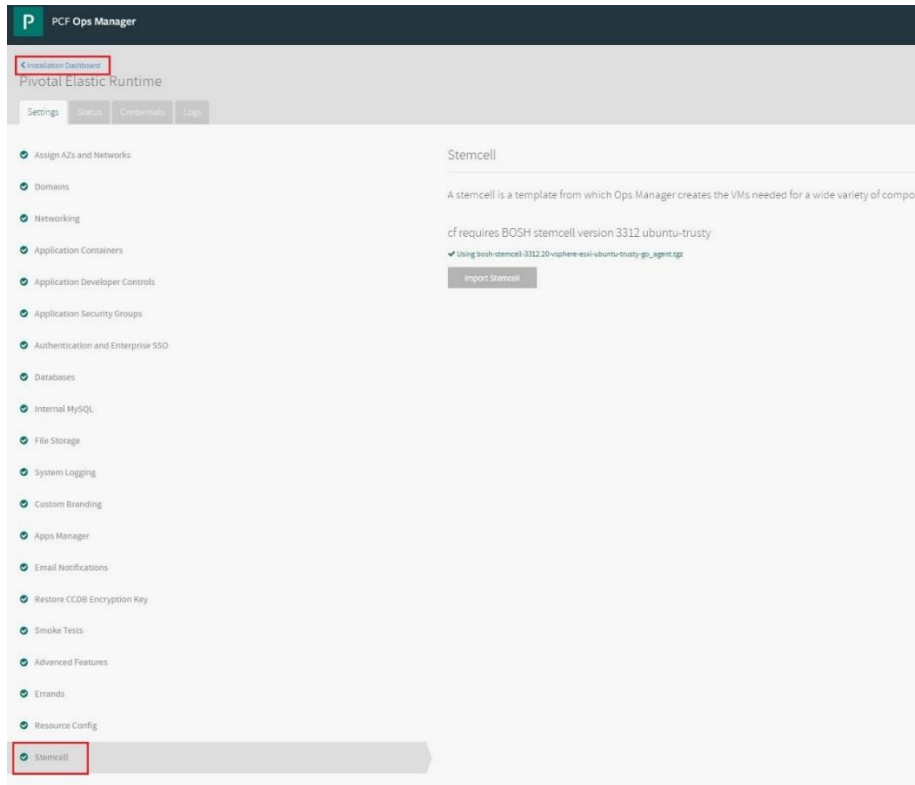
- Leave all defaults.
- Click **Save**.



22. Click **Errands**.

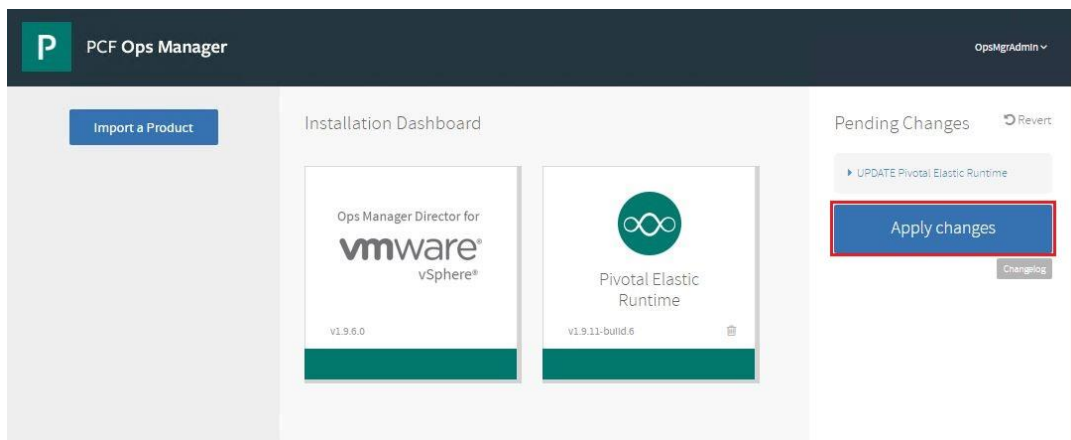
- Clear the **Push Notifications** and **Push Notifications UI** check boxes since we did not configure an SMTP server. If you configured an SMTP server, you can leave these checked.

- [illegible]

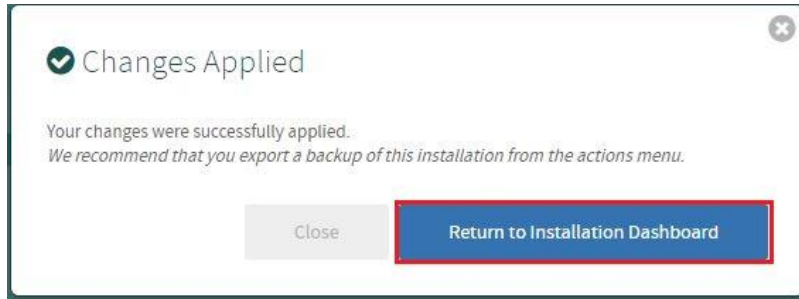


24. Click **Stemcell**.

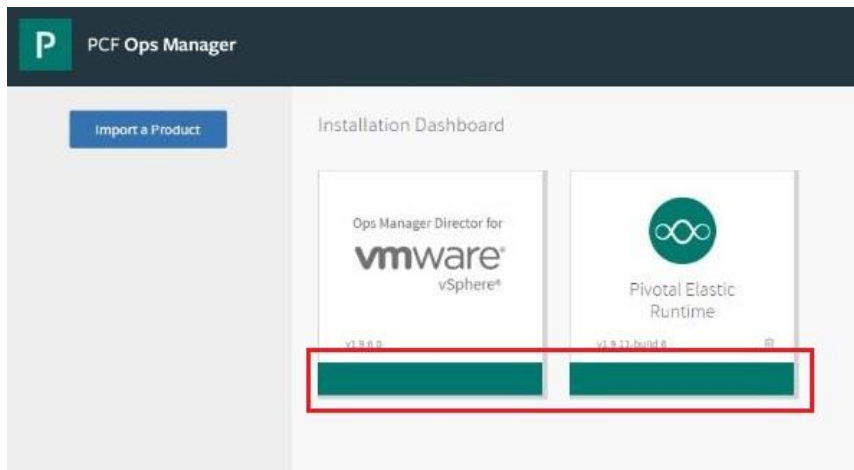
- Leave this page alone since it was already showing the latest stemcell version that came with Ops Manager.
- In the upper left area of the page, click **Installation Dashboard**.



25. On the right side of the page, click **Apply Changes**. This applies the changes and deploys Elastic Runtime.



26. When the deployment completes, you should see the following screen showing that changes have been applied. Click **Return to the Installation Dashboard**.

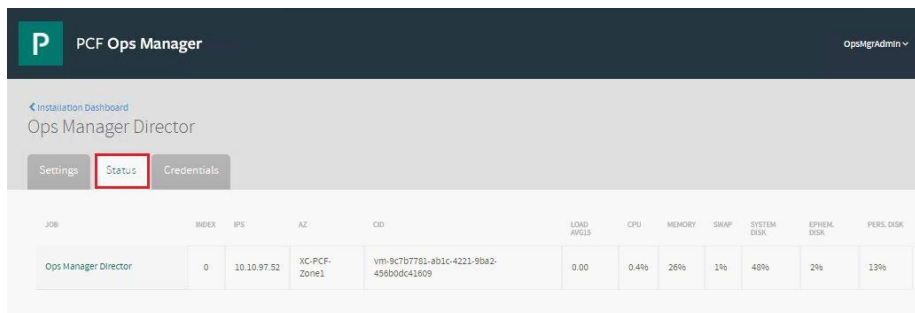


On the Installation Dashboard, you can now see the green bar across both the Ops Manager Director tile and Elastic Runtime tile indicating that they are both deployed correctly. If the deployment fails, you will continue to see the red bar across the bottom of the tile and you would be taken to the Change Log. There you can click on the Logs link at the end of the row for more information to begin troubleshooting. Troubleshooting it beyond the scope of this guide.

PCF Ops Manager									
OpsMgrAdmin									
Installation Dashboard									
Change Log									
Show: 10	entries								
Started	Finished	User	Result	Added	Updated	Deleted	Logs		
2017-03-13 19:36:53 UTC	2017-03-13 20:10:58 UTC	OpsMgrAdmin	SUCCEEDED	Pivotal Elastic Runtime 1.9.11-build.6			Logs		
2017-03-10 21:12:57 UTC	2017-03-10 21:26:43 UTC	OpsMgrAdmin	SUCCEEDED	Ops Manager Director 1.6.6.0			Logs		

Figure 4 Check the log file if you need to troubleshoot Ops Manager Director.

3.1.1 Viewing all the VMs for Ops Manager Director or Elastic Runtime



1. From the **Installation Dashboard**, click either **Ops Manager Director** tile or **Pivotal Elastic Runtime** tile. Then click on the **Status** tab. This displays all of the VMs for Ops Manager Director or Elastic Runtime, depending on which tile you selected.

The screenshot shows the PCF Ops Manager interface for 'Pivotal Elastic Runtime'. The 'Status' tab is highlighted with a red box. The table below lists various VMs and their resource usage.

JOB	INDEX	IPS	AZ	CID	LOAD AVG15	CPU	MEMORY	SWAP	SYSTEM DISK	EPHEM. DISK	PERM. DISK	LOGS
Consul	0	10.10.97.57	XC-PCF-Zone1	vm-52f588fc-d5a3-476d-908b-24bba2bb87e	0.00	0.2%	10%	0%	36%	3%	3%	⬆
NATS	0	10.10.97.58	XC-PCF-Zone1	vm-e04b884d-4911-409f-bb8b-b54c5ee4b6a	0.00	0.2%	9%	0%	36%	3%	N/A	⬆
etcd Server	0	10.10.97.59	XC-PCF-Zone1	vm-1b75895d-8bb8-4ac5-8dfe-573a36779c96	0.10	0.7%	16%	0%	36%	5%	31%	⬆
etcd Proxy	0	10.10.97.60	XC-PCF-Zone1	vm-d5e0d469-d974-4f48-862b-542c3fa1366c	0.00	0.0%	12%	0%	36%	3%	0%	⬆
File Storage	0	10.10.97.61	XC-PCF-Zone1	vm-d132ec11-2151-4997-9662-b00c26740145	0.00	0.9%	3%	0%	36%	6%	3%	⬆
MySQL Proxy	0	10.10.97.62	XC-PCF-Zone1	vm-2b4b53e2-d159-4e75-bb6c-60833d099f20	0.28	6.9%	11%	0%	36%	4%	N/A	⬆
MySQL Server	0	10.10.97.63	XC-PCF-Zone1	vm-f1bbd7ec-2c8d-4f8e-b376-d0b5d2ac0180	0.58	17.1%	11%	0%	36%	1%	5%	⬆
UAA	0	10.10.97.63	XC-PCF-Zone1	vm-e9ed950e-aac5f-4f6c7-e23d0963d5d2	0.00	2.2%	17%	0%	36%	3%	N/A	⬆
Cloud Controller	0	10.10.97.64	XC-PCF-Zone1	vm-3f69a20f-699d-43aa-0105-9969c8a5b2db	0.00	4.9%	19%	0%	36%	10%	0%	⬆
HAProxy	0	10.10.97.100	XC-PCF-Zone1	vm-ab7b3811-9dbd-4c7b-b0c4-45f72bd07630	0.00	0.0%	12%	0%	36%	2%	N/A	⬆
Router	0	10.10.97.97	XC-PCF-Zone1	vm-ef7a0a89-91a4-4e6e-8744-097042317d28	0.00	1.1%	11%	0%	36%	3%	N/A	⬆
MySQL Monitor	0	10.10.97.67	XC-PCF-Zone1	vm-a004053a-4719-4b06-902e-80ef777c5509	0.00	0.1%	8%	0%	36%	2%	N/A	⬆
Cloud Global	0	10.10.97.55	XC-PCF-Zone1	vm-0900b66c-b352-473d-4310-a996b0cc7f5f	0.00	0.3%	26%	0%	36%	8%	N/A	⬆
Cloud Controller Worker	0	10.10.97.56	XC-PCF-Zone1	vm-7912ab28-c6c4-f37f-0dbf-f886000d779	0.00	0.8%	24%	0%	36%	8%	N/A	⬆
Diego BBS	0	10.10.97.64	XC-PCF-Zone1	vm-aad37fac-9e00-4af1-93a9-e2f9a7ca972	0.01	0.3%	19%	0%	36%	9%	31%	⬆
Diego Brain	0	10.10.97.71	XC-PCF-Zone1	vm-0cc9e49c-102b-444c-875d-e263a009ba3e	0.00	0.9%	10%	0%	36%	7%	0%	⬆
Diego Cell	0	10.10.97.65	XC-PCF-Zone1	vm-74d9f558-a90b-4022-a881-900fcs119f5	0.15	1.8%	10%	0%	36%	11%	N/A	⬆
	1	10.10.97.69	XC-PCF-Zone1	vm-b1368599-201c-4452-b20a-de7a758d4f2a	0.16	2.4%	9%	0%	36%	10%	N/A	⬆
	2	10.10.97.68	XC-PCF-Zone1	vm-188aecc7-72ee-4596-b78c-b9ab4504e5eb	0.16	2.3%	9%	0%	36%	10%	N/A	⬆
Doppler Server	0	10.10.97.70	XC-PCF-Zone1	vm-8c18c3ff-ae5a-462a-bc6a-80336891ba0	0.00	1.3%	10%	0%	36%	3%	N/A	⬆
Loggregator Trafficcontroller	0	10.10.97.72	XC-PCF-Zone1	vm-74780997-d98d-481c-bd67-220cf05d490d	0.00	0.2%	11%	0%	36%	4%	N/A	⬆

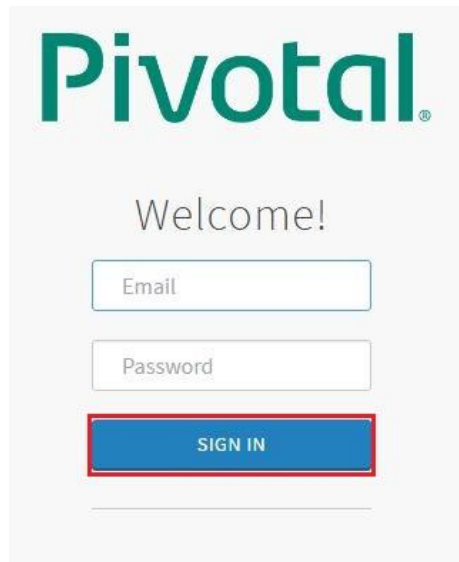
Figure 5 Page that displays when you select Pivotal Elastic Runtime Status.

4 Creating new orgs, spaces, and user accounts

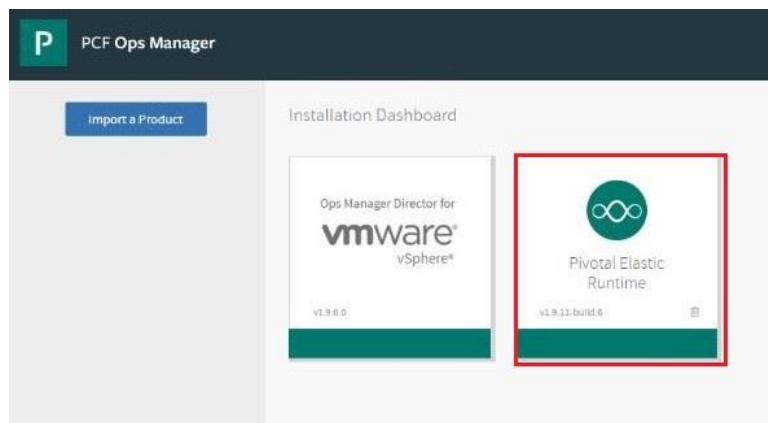
Next, we create new Orgs, Spaces, user accounts, and associate them together before you can push apps. Do this using your management VM. In addition, you can use the Apps Manager UI to create Orgs and Spaces, but *not* to create user accounts in Elastic Runtime v1.9.11. You can use the cf CLI to do both and we illustrate those steps in the following sections.

4.1 Obtaining credentials

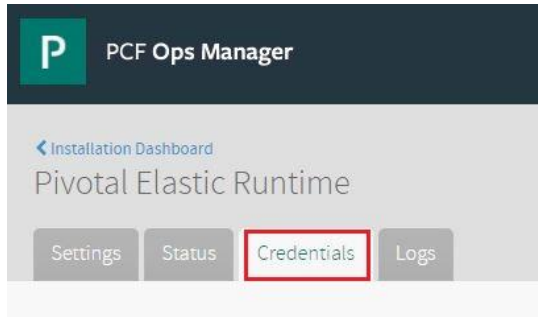
Before you can log in to the cf CLI, credentials are required. Many of the possibly needed sets of credentials are kept in Pivotal and are obtained from the Credentials tab in Ops Manager for each product.



1. Log in to Ops Manager with the credentials you created and used earlier in [Section 2.2](#), Step 3 (Checklist item #18).



2. Click on the **Elastic Runtime** tile.



3. Click the **Credentials** tab.



4. On the **Credentials** tab, find UAA in the left column and Admin Credentials in the right column. Click **Link to Credential**. This takes you to a page showing you the generated username and password. Write these credentials in the Checklist item #19.

Note: This page will not update if you log in to that user profile and change the password.

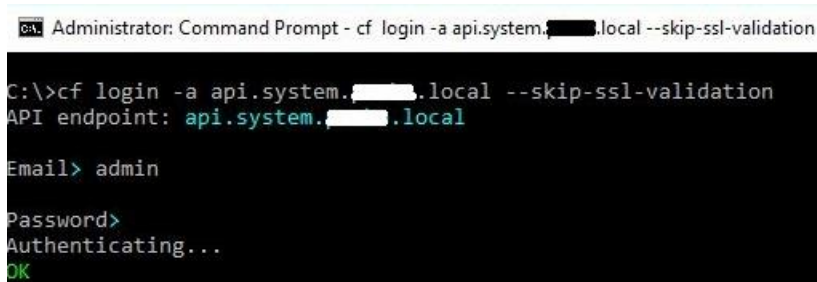
5. Use those credentials to log in to the cf CLI in the next section.

4.2 cf CLI for orgs, spaces, and user accounts

This is where we will create a new Org and a Space within that Org, a user account, and associate them together.

1. Open an elevated command prompt on your tools machine where you have the cf CLI installed.
2. At the command prompt, type:

```
cf login -a api.system.YourDomain.YourToplevelDomain --skip-ssl-validation
```



3. You are prompted for email and password. These are the credentials you obtained above in section 4.1 and do not need to be in email format. Checklist item #19.

```
Select an org (or press enter to skip):
1. PGStorage
2. system
3. TestOrg

Org>

API endpoint: https://api.system.____.local (API version: 2.65.0)
User: admin
No org or space targeted, use 'cf target -o ORG -s SPACE'

C:\>_
```

4. Next, you are asked for an Org. Because we want to create a new Org, press **Enter** to skip. This takes you back to a command prompt but you are now logged into the API system.

```
C:\>cf create-org OrgTest
Creating org OrgTest as admin...
OK

Assigning role OrgManager to user admin in org OrgTest ...
OK

TIP: Use 'cf target -o OrgTest' to target new org
```

5. To create a new Org, at the command prompt type the following and then press **Enter**:

```
cf create-org NewOrgName
```

```
C:\>cf create-space SpaceTest -o OrgTest
Creating space SpaceTest in org OrgTest as admin...
OK
Assigning role RoleSpaceManager to user admin in org OrgTest / space SpaceTest as admin...
OK
Assigning role RoleSpaceDeveloper to user admin in org OrgTest / space SpaceTest as admin...
OK

TIP: Use 'cf target -o "OrgTest" -s "SpaceTest"' to target new space
```

6. To create a new Space inside that Org, at the command prompt type the following and press **Enter**:

```
cf create-space NewSpaceName -o NewOrgName
```

```
C:\>cf target -o OrgTest -s SpaceTest
API endpoint: https://api.system.████.local
API version: 2.65.0
User: admin
Org: OrgTest
Space: SpaceTest
```

7. You must target that Org and Space to work inside of it. At the command prompt, type the following and press **Enter**:

```
cf target - NewOrgName -s NewSpaceName
```

```
C:\>cf create-user TestUser Password!
Creating user TestUser...
OK
TIP: Assign roles with 'cf set-org-role' and 'cf set-space-role'.
```

8. Time to create a new user in that Org and Space. Add these new credentials to the Checklist item #20. At the command prompt type the following and then press **Enter**:

```
cf create-user UserName Password
```

Note: Password must adhere to the password policy configured during Elastic Runtime configuration.

```
C:\>cf set-space-role --help
NAME:
  set-space-role - Assign a space role to a user

USAGE:
  cf set-space-role USERNAME ORG SPACE ROLE

ROLES:
  'SpaceManager' - Invite and manage users, and enable features for a given space
  'SpaceDeveloper' - Create and manage apps and services, and see logs and reports
  'SpaceAuditor' - View logs, reports, and settings on this space

SEE ALSO:
  space-users
```

9. After a user is created, that user must be given a role in this Org and Space. At the command prompt type the following and press **Enter**:

`cf set-space-role --help` to see the available roles.

For more information, go to [Orgs, Spaces, Roles, and Permissions](#).

```
C:\>cf set-space-role TestUser OrgTest SpaceTest SpaceDeveloper
Assigning role RoleSpaceDeveloper to user TestUser in org OrgTest / space SpaceTest as admin...
OK
```

10. At the command prompt, type the following and press **Enter**:

`cf set-space-role UserName OrgName SpaceName RoleName`

Now, you have a new Org, Space, and User account created. That user only has access to that Org and Space. Next, we can push an app to this Space as this User.

5 Obtaining and pushing apps to PCF

In our example app deployments, we used the Dotnet Core Hello World app and the Spring Music app from the [Cloud Foundry samples at Github](#) and then pushing them to our Pivotal Cloud Foundry deployment. We will verify they work by visiting the created webpages from another machine. Because we are using a private network behind a company proxy, there were a couple of additional configurations to get these to work. You may or may not need these same additional configurations.

- We are not able to publish public DNS records. This means that to check that our app is published and working, we have to use another machine in our environment that can resolve the web addresses created when the apps are pushed.
- Since we are behind a corporate proxy, there are some changes we have to make so that our management machine can access the internet and our intranet at the same time in the various tools.
 - Git for Windows uses its own proxy list instead of Internet Options proxies or environment variables. We had to set proxies directly in the Git for Windows tool.
 - While pushing an app, PCF will try to reach out to the internet to make sure it has the correct dependencies for that app. In our specific situation, this required us to set proxies in the `manifest.yml` file for each app we tried to push.
 - The Spring Music app has to be assembled first. This operation connects to the internet to download dependencies and assembles the app using the Gradlew command. We had to set our proxies in the `gradle.properties` file.
 - There are other possible ways to get around these, but this was a quick solution for this proof of concept.

Note: See Appendix for more information on these additional configurations.

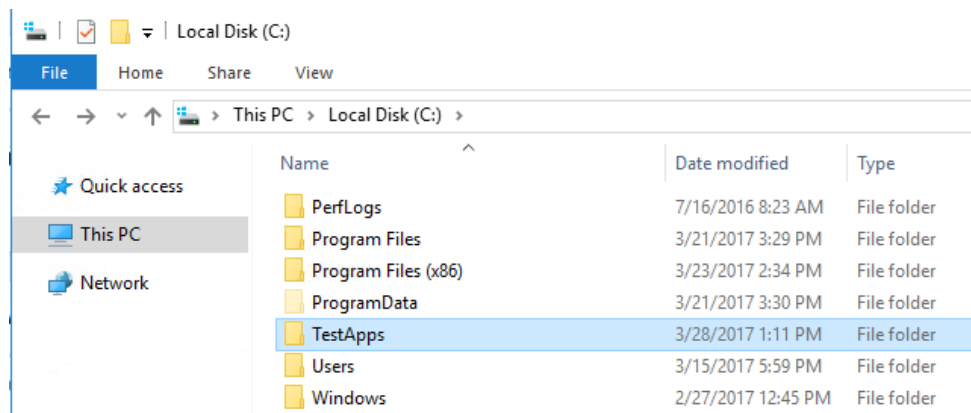


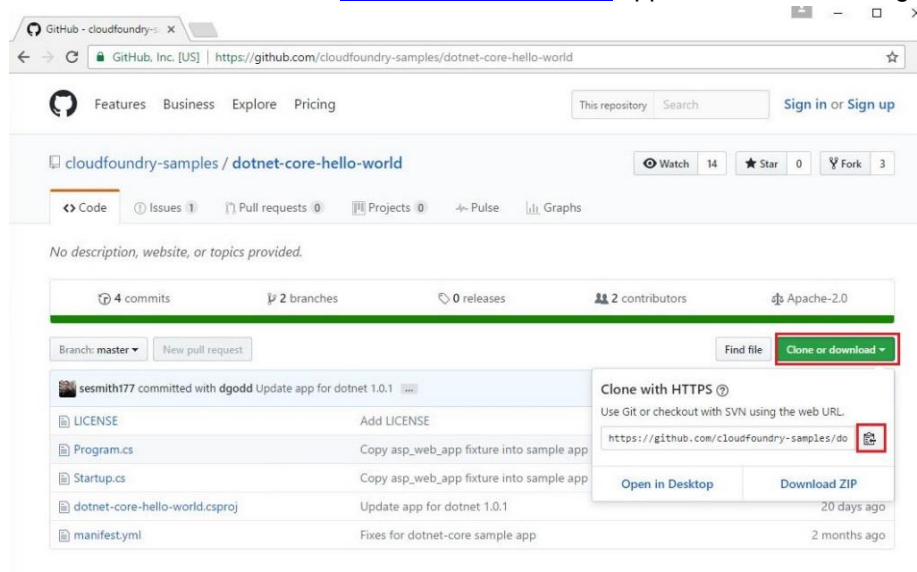
Figure 6 Create a folder where you can put your apps.

1. First, use your favorite File Explorer and create a new folder where you can put your apps from the web. We created a folder called TestApps.
2. [Cloud Foundry samples at Github](#) is where you will find several example applications. There are many more up level from that page as well.

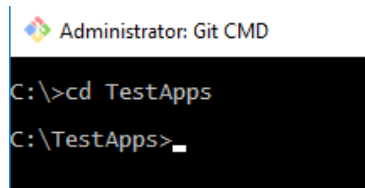
5.1 Hello World

Let's use Git for Windows to obtain the Hello World app.

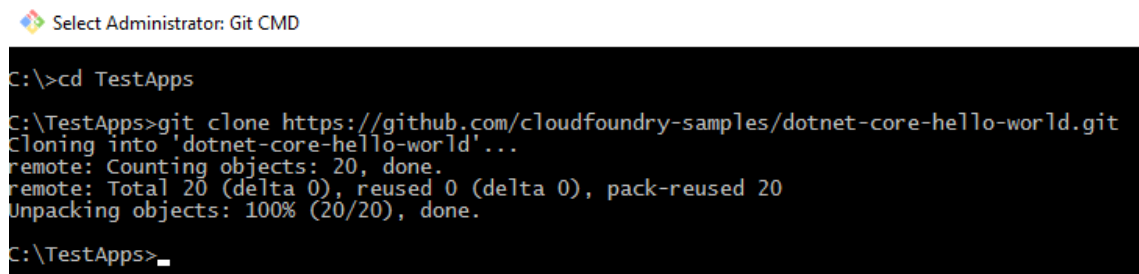
1. Here is the direct link to the [dotnet-core-hello-world](https://github.com/cloudfoundry-samples/dotnet-core-hello-world) app that we will be using.



2. On this page, click the green **Clone or download** button and then click on the **Copy to Clipboard** icon at the end of the address.

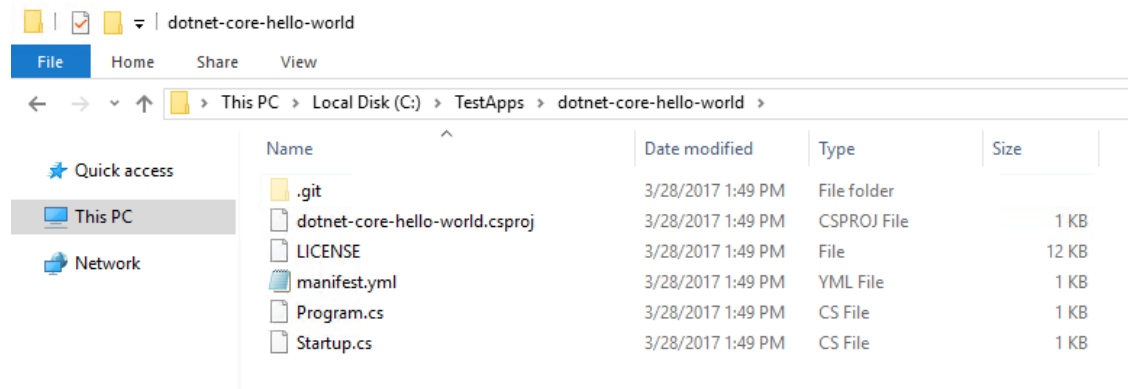


3. Open an elevated Git for Windows CMD. Change directory to the folder you created in step 1.



4. At the command prompt, type `git clone` and then CTRL + V to paste the URL that you copied to the clipboard. The result will be:

```
git clone https://github.com/cloudfoundry-samples/dotnet-core-hello-world.git
```



5. Press **Enter**. The Hello World app will be unpacked into its own folder inside your TestApps folder.

After the app is unpacked, you can make any changes to the `manifest.yml` file as needed such as how we had to add our proxies. That is discussed in more detail in the [Appendix](#).

5.1.1 Pushing Hello World

```
Administrator: Command Prompt

C:\>cf login -a api.system.████.local --skip-ssl-validation
API endpoint: api.system.████.local

Email> TestUser

Password>
Authenticating...
OK

Targeted org OrgTest

Targeted space SpaceTest

API endpoint: https://api.system.████.local (API version: 2.65.0)
User: TestUser
Org: OrgTest
Space: SpaceTest

C:\>_
```

1. Go back to the elevated CMD where we were typing cf commands if it is still open and you are still logged into the api.system.*YourDomain.YourTopLevelDomain*. If it is not still open, you must open a new elevated CMD and login with the following command again, using the new user we created. Use credentials in Checklist item #20.

```
cf login -a api.system.YourDomain.YourToplevelDomain --skip-ssl-validation
```

```
C:\>cd TestApps\dotnet-core-hello-world
C:\TestApps\dotnet-core-hello-world>_
```

2. Since this user only has access to this Org and Space, that is what is targeted. Change to the directory where your app has been unpacked.

```
C:\TestApps\dotnet-core-hello-world>cf buildpacks
Getting buildpacks...

buildpack      position  enabled  locked  filename
staticfile_buildpack  1         true    false   staticfile_buildpack-cached-v1.3.13.zip
java_buildpack_offline  2         true    false   java_buildpack-offline-v3.10.zip
ruby_buildpack    3         true    false   ruby_buildpack-cached-v1.6.28.zip
nodejs_buildpack  4         true    false   nodejs_buildpack-cached-v1.5.23.zip
go_buildpack      5         true    false   go_buildpack-cached-v1.7.16.zip
python_buildpack  6         true    false   python_buildpack-cached-v1.5.12.zip
php_buildpack     7         true    false   php_buildpack-cached-v4.3.22.zip
dotnet_core_buildpack  8         true    false   dotnet-core_buildpack-cached-v1.0.5.zip
binary_buildpack  9         true    false   binary_buildpack-cached-v1.0.5.zip
```

3. Buildpacks are updated frequently. At the command prompt, type `cf buildpacks` and press **Enter** to see the buildpacks currently installed and their versions.
4. The app we are going to push is a dotnet app and we can see that the version we have installed is an older version than what is currently available. Whether your deployment is with a newer version of Elastic Runtime, and you get newer buildpacks, this is a good exercise so that you get the latest buildpack. We want to reach out to Github and use the latest dotnet buildpack when we push this app. To do this, at the command prompt, type the following and press **Enter**:

```
cf push -b https://github.com/cloudfoundry/dotnet-core-buildpack.git
```

```

C:\TestApps\dotnet-core-hello-world>cf push -b https://github.com/cloudfoundry/dotnet-core-buildpack.git
Using manifest file C:\TestApps\dotnet-core-hello-world\manifest.yml

Updating app dotnet_core_hello_world in org OrgTest / space SpaceTest as TestUser...
OK

Uploading dotnet_core_hello_world...
Uploading app files from: C:\TestApps\dotnet-core-hello-world
Uploading 5.1K, 4 files
Done uploading
OK

Starting app dotnet_core_hello_world in org OrgTest / space SpaceTest as TestUser...
Creating container
Successfully created container
Downloading app package...
Downloaded app package (5.3K)
Staging...
-----> Buildpack version 1.0.13
ASP.NET Core buildpack version: 1.0.13
ASP.NET Core buildpack starting compile

```

5. You should see the app begin deployment.

```

Showing health and status for app dotnet_core_hello_world in org OrgTest / space SpaceTest as TestUser...
OK

requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: dotnet-core-hello-world-gaunt-schav.apps.██.local
last uploaded: Tue Mar 28 20:55:14 UTC 2017
stack: cflinuxfs2
buildpack: https://github.com/cloudfoundry/dotnet-core-buildpack.git

#0 state since cpu memory disk details
running 2017-03-28 03:58:29 PM 0.0% 912K of 1G 2.3M of 1.5G

```

6. After the app is pushed and started, you will see an OK for health and get a URL to access it. This will be the URL you use to access your newly published app. Write this URL in the Checklist item #22.

5.1.2 Confirm Hello World is working

Pivotal Cloud Foundry is installed and the first app has been pushed. Now to confirm that it is working, we will browse to the Hello World URL (Checklist item #22) given in the output of the cf push function. Do this from any other machine in the same environment. We have to use a machine that can resolve the URL.

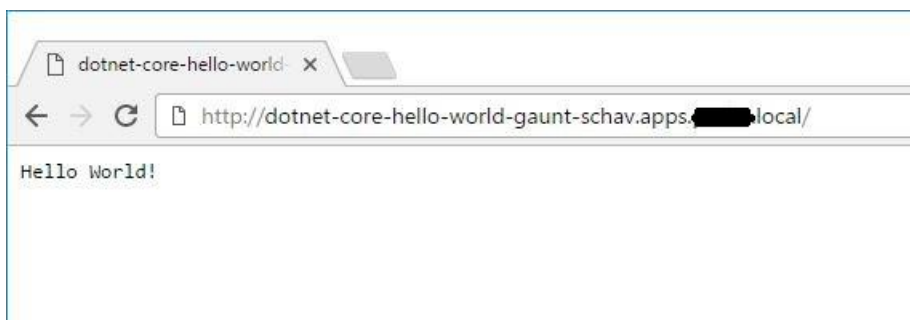
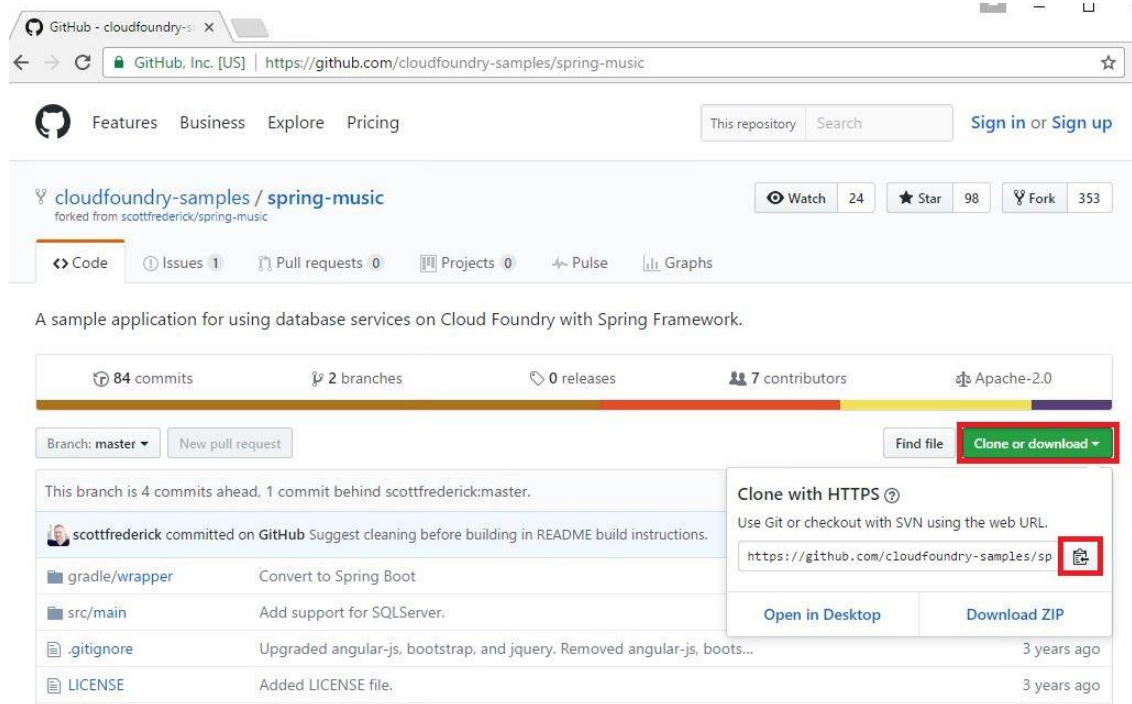


Figure 7 Browsing to the Hello World URL.

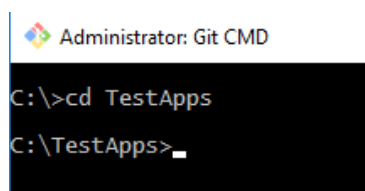
5.2 Spring Music

Let's use Git for Windows to obtain the Spring Music app.

1. Here is the direct link to the [Spring Music](https://github.com/cloudfoundry-samples/spring-music) app that we will be using.



2. On this page, click the green **Clone or download** button and then click the **Copy to Clipboard** icon at the end of the address.

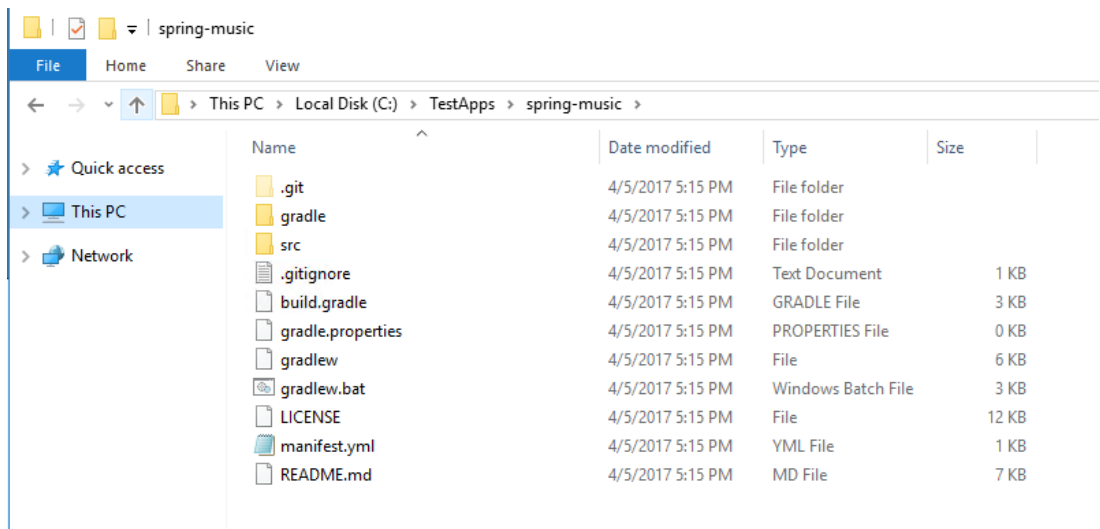


3. Open an elevated Git for Windows CMD. Change directory to the folder you created in Section 5, step 1.

```
C:\TestApps>git clone https://github.com/cloudfoundry-samples/spring-music.git
Cloning into 'spring-music'...
remote: Counting objects: 1045, done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 1045 (delta 0), reused 0 (delta 0), pack-reused 1042
Receiving objects: 100% (1045/1045), 697.19 KiB | 0 bytes/s, done.
Resolving deltas: 100% (366/366), done.
```

4. At the command prompt, type `git clone` and then `ctrl+v` to paste the URL that you copied to the clipboard. The result displays here:

```
git clone https://github.com/cloudfoundry-samples/spring-music.git
```

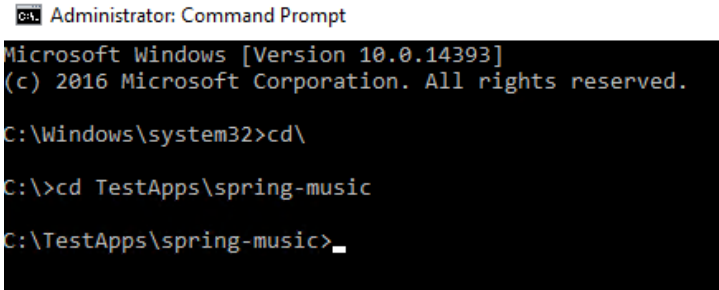


5. Press **Enter**. The Spring Music app will be unpacked into its own folder inside your TestApps folder.

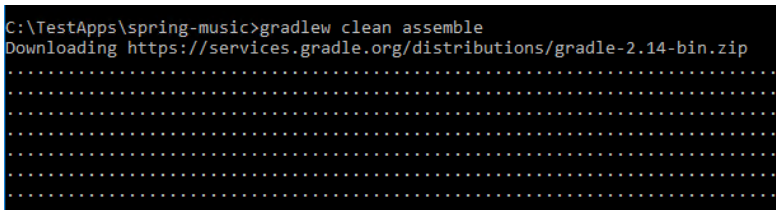
After the app is unpacked, you can make any changes to the `manifest.yml` file as needed such as how we had to add our proxies. That is discussed in more detail in the [Appendix](#).

5.2.1 Assemble Spring Music

Spring Music is a little different from Hello World in that it has to be assembled before it can be pushed. As mentioned above, this is where we had to set our proxies in the `gradlew.properties` file. More information about that can be found in the [Appendix](#).

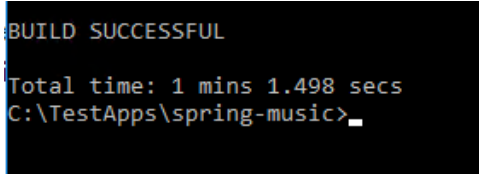


1. To assemble Spring Music, go back to the elevated CMD where we were typing cf commands if it is still open and you are still logged into the `api.system.YourDomain.YourTopLevelDomain`. If it is not still open, you must open a new elevated CMD. Change directory to your Spring Music folder.



2. At the command prompt, type the following command and press **Enter**. This starts assembling the app and you will see it downloading and unzipping packages.

Gradlew clean assemble



3. At the end of the assembly you will see BUILD SUCCESSFUL.

```
Administrator: Command Prompt

C:\>cf login -a api.system.████.local --skip-ssl-validation
API endpoint: api.system.████.local

Email> TestUser

Password>
Authenticating...
OK

Targeted org OrgTest

Targeted space SpaceTest

API endpoint: https://api.system.████.local (API version: 2.65.0)
User: TestUser
Org: OrgTest
Space: SpaceTest

C:\>_
```

4. Now, we need to make sure we are logged in with the cf CLI tools again using the new user we created. Use credentials in Checklist item #20 again. At the command prompt, type the following command and then press **Enter**.

```
cf login -a api.system.YourDomain.YourToplevelDomain --skip-ssl-validation
```

```
C:\>cd TestApps\spring-music

C:\TestApps\spring-music>_
```

5. Since this user only has access to this Org and Space, that is what is targeted. Change to the directory where your app has been unpacked.

```
C:\TestApps\spring-music>cf push
Using manifest file C:\TestApps\spring-music\manifest.yml

Creating app spring-music in org OrgTest / space SpaceTest as TestUser...
OK

Creating route spring-music-nontraveling-collins.apps.████.local...
OK

Binding spring-music-nontraveling-collins.apps.████.local to spring-music...
OK

Uploading spring-music...
Uploading app files from: C:\Users\ADMINI~1\████\AppData\Local\Temp\2\unzipped-app036859187
Uploading 38.3M, 233 files
Done uploading
OK
```

6. Since this app was assembled already, we should only have to push it. At the command prompt, type the following command: `cf push` and press **Enter** to see the deployment begin.

```
Showing health and status for app spring-music in org OrgTest / space SpaceTest as TestUser...
OK

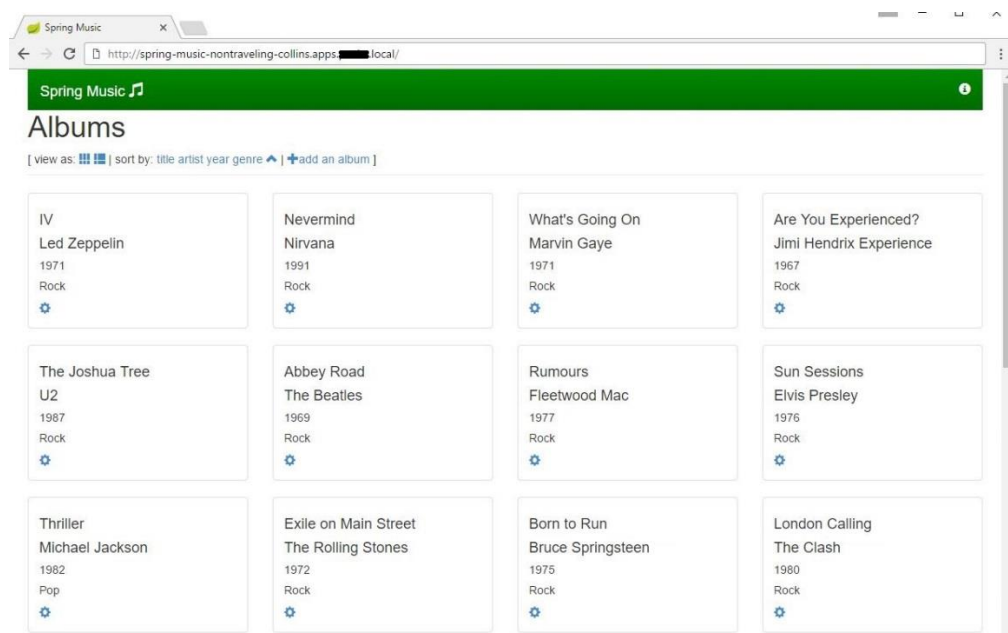
requested state: started
instances: 1/1
usage: 16 x 1 instances
urls: spring-music-nontraveling-collins.apps.█.local
last uploaded: Wed Apr 5 23:04:32 UTC 2017
stack: cflinuxfs2
buildpack: java-buildpack=v3.10-offline-https://github.com/cloudfoundry/java-buildpack.git#193
ke-jre=1.8.0_111 open-jdk-like-memory-calculator=2.0.2_RELEASE spring-auto-reconfiguration=1.1

state since cpu memory disk details
#0 running 2017-04-05 06:05:11 PM 0.0% 431.8M of 1G 166.5M of 1G
```

7. After the app is pushed and started, you will see an OK for health and get a URL to access it. This will be the URL you use to access your newly published app. Write this URL in the Checklist item #23.

5.2.2 Confirming Spring Music is working

Pivotal Cloud Foundry is installed and the second app has been pushed. Now to confirm that it is working, we will browse to the Spring Music URL (Checklist item #23) given in the output of the `cf push` function. Do this from any other machine in the same environment. We have to use a machine that can resolve the URL.



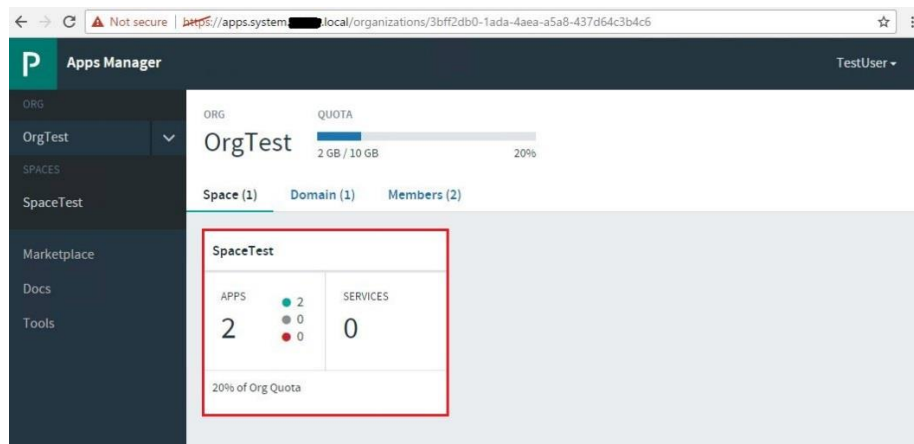
5.3 Apps Manager

The last thing we can do is take a look in Apps Manager to see our running apps in their Org and Space.

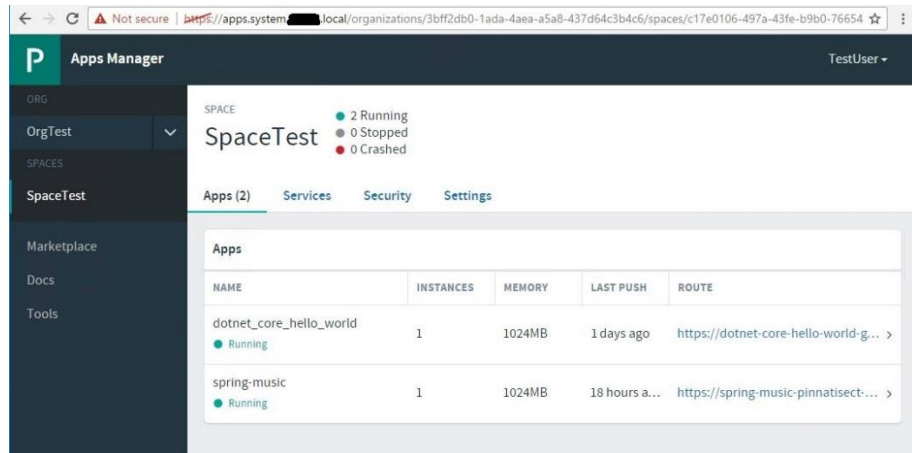


1. Open a webpage on your tools VM and browse to the following URL. On this page, you will log in with the credentials that you created in Section 4.2, Step 8 (Checklist item #20) and then click **Sign In**.

`https://login.system.YourDomain.YourTopLevelDomain/login`



2. After you are logged in, you see your new Org and the smaller box is your Space. Click on your Space where it shows two Apps.



3. On the Space page, we can see both of our apps (Hello World and Spring Music), that they are both running, and some additional information about them. You can click on one of them to drill down further.

This concludes our deployment of Pivotal Cloud Foundry on a Dell XC cluster including pushing two apps to confirm our deployment is working.

A Options for settings proxies

A.1 Git for Windows proxy list

If you use a proxy to access the Internet, Git for Windows uses its own list. It does not use the list under LAN Settings on the Connections tab in Internet Options. In addition, it does not use Windows environment variables. Proxies must be set in the Git for Windows CMD tool. Here are the commands and what they do.

Used to remove any previously set proxies:

- `git config --global --unset http.proxy`
- `git config --global --unset https.proxy`

Used to set your http and https proxies. Replace *FQDN:port* with the address and port of your proxies:

- `git config --global http.proxy FQDN:port`
- `git config --global https.proxy FQDN:port`
- **Example:** `git config --global http.proxy http://proxy.company.com:80`
- **Example:** `git config --global https.proxy http://proxy.company.com:80`

Used to verify the proxies are set. This should output the address and port you set above.

- `git config --global get http.proxy`
- `git config --global get https.proxy`

A.2 Adding proxy to manifest.yml

If you use a proxy to access the internet, you may need to add your proxy to the environment (env) section in the `Manifest.yml` file in each app before pushing the app. If the env section is not there, add it. In this example, the env section was already there and had the `CACHE_NUGET_PACKAGE` line. We added the `http_proxy` and `https_proxy` lines. Format should be similar to this.

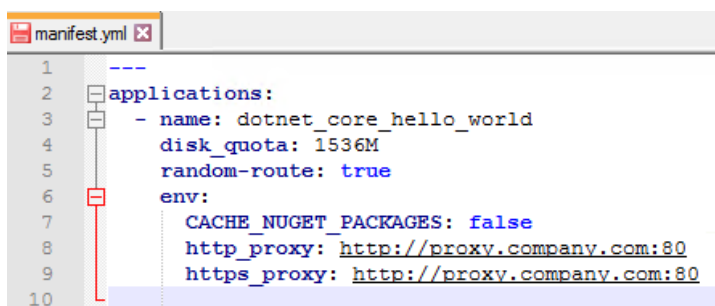
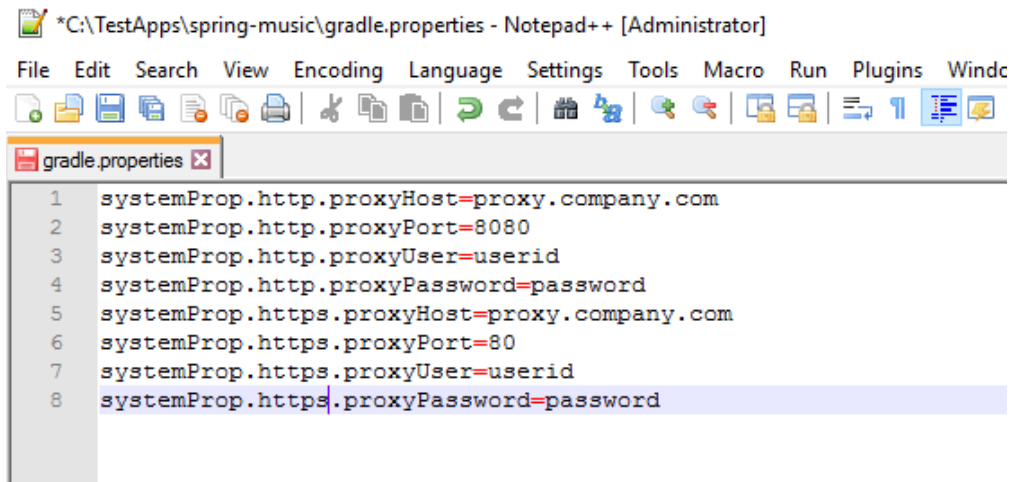


Figure 8 Adding the http_proxy.

A.3 Adding proxy to gradle.properties file

If you use a proxy to access the internet, and you have to assemble an app using the `gradlew` command, you may have to add your proxies to the `gradle.properties` file. This file should be located in the root of your app where the `gradlew` command is. Format should be similar to the following and you can remove any of these lines that you do not need. This shows both http and https settings for the proxy, port, and credentials if necessary. Notepad++ is used in the example to edit the `gradle.properties` file.



B Technical support and resources

- [Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.
- [Dell TechCenter](https://delltechcenter.com) is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware and services.
- [Advanced Materials](#) is the latest technical content and best practices for the Dell EMC XC Series appliances.

C Related resources

See the following referenced or recommended resources related to this document:

NOTE: The links below are open to customers although some may require registration for access.

- [Join Pivotal Network](#)
- [Pivotal Documents](#)
- [Pivotal Network](#)
- [vSphere Requirements](#)
- [KB 2125229](#)
- [KB 2120255](#)
- [cf CLI](#)
- [Notepad++](#)
- [Putty](#)
- [WinSCP](#)
- [Deploying Operations Manager to vSphere](#)
- [Pivotal Cloud Foundry Ops Manager for vSphere](#)
- [Provisioning a Virtual Disk](#)
- [Configuring Operations Manager Director for vSphere](#)
- [Use an Identity Provider](#)
- [Internal Authentication](#)
- [PCF Director Proxy Settings](#)
- [Provisioning a Virtual Disk in vSphere](#)
- [Configuring Elastic Runtime for vSphere](#)
- [Pivotal Cloud Foundry Elastic Runtime](#)
- [Orgs, Spaces, Roles, and Permissions](#)
- [Cloud Foundry samples at Github](#)
- [dotnet-core-hello-world](#)
- [Spring Music](#)

D Deployment checklist

Here is a checklist of information that you might want to keep handy before, during, and after your deployment. Fill out this checklist prior to starting the deployment process.

Table 3 Deployment checklist

Item #	Description	Enter your info here	
1	Minimum range of 36 IPs. If using DHCP, make an exclusion in your scope. Also write the CIDR format of this range. Example might be 10.x.x.x-10.x.x.y, and CIDR 10.x.x.0/25.		
2	List of any IPs in the above range that should not be used by PCF.		
3	Subnet Mask for above range.		
4	Gateway IP		
5	DNS server IPs		
6	IP, in above range, that you want to use for Ops Manager.		
7	IP, in above range, for the included HAProxy or your own load balancer IP, if you have one.		
8	NTP Server IP		
9	SMTP server IP, if you have one.		
10	vCenter host server IP		
11	Cluster name as it appears in vCenter.		
12	Datacenter name as it appears in vCenter.		
13	Datastore/Container name as it appears in vCenter.		
14	vSphere Network Name		
		Username	Password
15	Pivotal Network credentials*		
16	vCenter credentials*		
17	SSH for Ops Manager credentials*	Ubuntu	
18	Pivotal Ops Manager credentials*		

Item #	Description	Enter your info here	
19	UAA Admin credentials*		
20	New Org & Space credentials*		
21	Pivotal Ops Manager Decryption Passphrase* .		
22	Hello World URL		
23	Spring Music URL		

*Use your corporate security practices to manage your credentials.