



Cisco UCS Performance Manager Installation Guide

First Published: August 2016

Release 2.0.2

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014-2016 Cisco Systems, Inc. All rights reserved.

Contents

About this book.....	6
Chapter 1: Welcome to Cisco UCS Performance Manager.....	8
Introduction to Control Center.....	8
Packaging considerations.....	9
Deployment considerations.....	10
Part I: Creating a single-host deployment.....	11
Chapter 2: Creating a Control Center master host.....	12
Creating a virtual machine.....	12
Configuring the Control Center host mode.....	15
Edit a connection.....	16
Set system hostname.....	18
Adding a disk for backups to Hyper-V guest systems.....	19
Preparing a disk for backups.....	20
Deploying Cisco UCS Performance Manager.....	21
Chapter 3: Enabling access to browser interfaces.....	23
Creating public endpoints.....	23
Configuring name resolution for virtual hosts.....	32
Part II: Creating a multi-host deployment.....	34
Chapter 4: Creating a Control Center master host.....	35
Creating a virtual machine.....	35
Configuring the Control Center host mode.....	38
Edit a connection.....	39
Set system hostname.....	41
Adding a disk for backups to Hyper-V guest systems.....	42
Preparing a disk for backups.....	43
Deploying Cisco UCS Performance Manager.....	44
Chapter 5: Enabling access to browser interfaces.....	46
Creating public endpoints.....	46
Configuring name resolution for virtual hosts.....	55
Chapter 6: Creating Control Center agent hosts.....	57
Creating a virtual machine.....	57
Configuring the virtual machine mode.....	60

Edit a connection.....	61
Set system hostname.....	63
Optional: Editing the /etc/hosts file.....	64
Chapter 7: Enabling NTP on Microsoft Hyper-V guests.....	66
Configuring NTP for public time servers.....	66
Configuring an NTP master server.....	67
Configuring NTP clients.....	68
Chapter 8: Configuring the master host.....	70
Optional: Editing the /etc/hosts file.....	70
Adding agent hosts to the default resource pool.....	71
Identifying network device names.....	72
Adding a virtual IP address to the default pool.....	73
Moving the master host to a new pool.....	73
Changing IP assignments.....	75
Reducing master host resources.....	76
Restarting the master host.....	77
Chapter 9: Configuring a ZooKeeper cluster.....	79
Example multi-host ZooKeeper configuration.....	79
Configuring the master host.....	80
Configuring agent host A.....	81
Configuring agent host B.....	82
Starting a ZooKeeper cluster.....	83
Updating the agent host that is not in the ZooKeeper cluster.....	84
Part III: Performing upgrades.....	86
Chapter 10: Upgrading Cisco UCS Performance Manager on vSphere systems.....	87
Upgrading single-host deployments.....	88
Upgrading multi-host deployments.....	90
Chapter 11: Upgrading Cisco UCS Performance Manager on Hyper-V systems.....	100
Upgrading single-host deployments.....	101
Upgrading multi-host deployments.....	104
Appendix A: Managing Cisco UCS Performance Manager with Control Center.....	114
Starting Cisco UCS Performance Manager.....	114
Shutting down a Control Center master host.....	115
Removing migration software.....	115

Appendix B: Adding storage to a Control Center master host.....	118
Identifying block storage devices.....	118
Identifying new block storage devices.....	120
Preparing a device for data collection storage.....	120
Appendix C: Using the Appliance Administration menu.....	122
Configure Network and DNS.....	122
Configure IPv6 Network CIDR.....	125
Configure Timezone.....	126
Change Docker Hub Credentials.....	126
Change Root Password.....	126
Change ceuser Password.....	127
Update System.....	127
Change SSL settings.....	127
Root Shell.....	128
Reboot / Poweroff System.....	129
Appendix D: Networking and security.....	130
Networking requirements.....	130
Security considerations.....	131
Configuring the Docker virtual bridge.....	132
CIDR prefix lengths for commonly-used netmasks.....	133
Appendix E: Tuning considerations.....	134
Single-host deployment tuning options.....	134
Multi-host deployment tuning options.....	134
Appendix F: Using Zenoss Toolbox.....	136
Zenoss Toolbox tools.....	136
Downloading Zenoss Toolbox with internet access.....	136
Downloading Zenoss Toolbox without internet access.....	137
Installing Zenoss Toolbox.....	137
Running Zenoss Toolbox tools.....	138

About this book

Cisco UCS Performance Manager Installation Guide provides detailed instructions for installing and upgrading Cisco UCS Performance Manager Express and Cisco UCS Performance Manager.

- Cisco UCS Performance Manager Express provides monitoring for Cisco UCS Central, Cisco UCS Domains, Linux and Microsoft Windows servers, hypervisor servers, and Control Center.
- Cisco UCS Performance Manager provides monitoring for Cisco UCS Central, Cisco UCS Domains, Linux and Microsoft Windows servers, hypervisor servers, network devices, storage devices, and Control Center.

For convenience, this document uses "Cisco UCS Performance Manager" generically, and notes explicitly any differences between the two platforms.

Minimum system requirements

For deployments monitoring up to 500 servers, Cisco UCS Performance Manager requires one virtual machine with the following resources:

- 8 CPU cores
- 64GB RAM
- 600GB storage, supporting a minimum of 100 IOPS

Note If you plan to migrate data from a version 1.1.x system, the master host storage must support 400 IOPS.

For deployments monitoring more than 500 servers, Cisco UCS Performance Manager requires four virtual machines with the resources shown in the following table:

VM Count	Cores	Memory	Storage	IOPS
1	4	30GB	900GB	200
3	8	64GB	150GB	100

Note If you are uncertain whether your environment requires a single-host or a multi-host deployment, please use the Cisco UCS Performance Manager Deployment Calculator. The calculator is available at <https://zenoss.github.io/deployment-calculator/#/>.

Supported client and browser combinations

Note All browsers must have Adobe® Flash® Player 11 installed, or a more recent version.

Client OS	Supported Browsers
Windows 7 and 8.1	Internet Explorer 10 and above (compatibility mode is not supported)
	Firefox 30 and above
	Chrome 30 and above
Macintosh OS/X	Firefox 30 and above
	Chrome 30 and above
	Safari 7 and above
Linux/RHEL	Firefox 30 and above
	Chrome 30 and above

Related publications

Title	Description
<i>Cisco UCS Performance Manager Installation Guide</i>	Provides detailed information and procedures for installing and upgrading Cisco UCS Performance Manager.
<i>Cisco UCS Performance Manager Migration Guide</i>	Provides detailed information and procedures for migrating data from Cisco UCS Performance Manager version 1.1.x to version 2.0.x.
<i>Cisco UCS Performance Manager Getting Started Guide</i>	Provides instructions for configuring Cisco UCS Performance Manager to monitor your environment, after installation.
<i>Cisco UCS Performance Manager User Guide</i>	Provides specific instructions for using Cisco UCS Performance Manager in the UCS environment.
<i>Cisco UCS Performance Manager Administration Guide</i>	Provides an overview of Cisco UCS Performance Manager architecture and features, as well as procedures and examples to help use the system.
<i>Cisco UCS Performance Manager Release Notes</i>	Describes known issues, fixed issues, and late-breaking information not already provided in the published documentation set.

Documentation feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

Welcome to Cisco UCS Performance Manager

1

Cisco UCS Performance Manager provides visibility from a single console into UCS components for performance monitoring and capacity planning. It provides data center assurance of integrated infrastructures and ties application performance to physical and virtual infrastructure performance. This allows you to optimize resources and deliver better service levels to your customers.

This release features an additional component, Control Center, which is an open-source, application service orchestrator based on *Docker*. Control Center greatly simplifies the installation, deployment, and management of Cisco UCS Performance Manager.

This chapter provides a brief introduction to Control Center, and describes how it affects Cisco UCS Performance Manager deployments.

Introduction to Control Center

Control Center is a platform-as-a-service framework that can manage Cisco UCS Performance Manager and any other Docker application, from a simple web application to a multi-tiered stateful application stack. Control Center is based on a service-oriented architecture, which enables applications to run as a set of distributed services spanning hosts, datacenters, and geographic regions.

Control Center includes the following, key features:

- Intuitive HTML5 interface for deploying and managing Cisco UCS Performance Manager
- Integrated backup and restore, and incremental snapshot and rollback support
- Centralized logging, through Logstash and Elasticsearch
- Support for database services and other persistent services
- Encrypted communications among all services and containers

Docker fundamentals

Note This section is a summation of *the architecture description provided by Docker*, customized for Cisco UCS Performance Manager. For additional information, refer to the Docker site.

Docker provides convenient tools that make use of the *cgrouops feature of the Linux kernel* to develop, distribute, and run applications. Docker internals include images, registries, and containers.

Docker images

Docker images are read-only templates that are used to create Docker containers. Images are easy to build, and image updates are change layers, not wholesale replacements.

Docker registries

Docker registries hold images. The Cisco UCS Performance Manager appliance includes a private Docker registry that holds the images of the Cisco UCS Performance Manager application.

Docker containers

Docker containers have everything needed to run an instance of an application, and are created from images. The Cisco UCS Performance Manager application includes many different containers, and each container is used to run one or more instances of a specific service.

Control Center terms and concepts**application**

A collection of one or more software programs that have been converted into Docker containers. For example, Cisco UCS Performance Manager.

resource pool

A collection of one or more hypervisor guest systems, each with its own compute, network, and storage resources. The name of the default resource pool is `default`. All systems in a resource pool should be guests of the same hypervisor.

agent host (resource pool host)

A hypervisor guest system that runs application services scheduled for the resource pool to which it belongs. A system may be configured as agent and master, or just agent, or just master.

master host

The hypervisor guest system that runs the application services scheduler, the Docker registry, the distributed file system, ZooKeeper, and other internal services, including the server for the Control Center browser interface. A system may be configured as agent and master, or just agent, or just master. Only one system in a Control Center cluster may be the master.

ZooKeeper (*Apache ZooKeeper*)

The internal service Control Center relies on to distribute and manage application services. ZooKeeper maintains the definitions of each service and the list of services assigned to each host. The scheduler, which runs on the master host, determines the assignments and sends them to the ZooKeeper node that is serving as the leader. All Control Center agent hosts retrieve the assignments and service definitions and start containers for the services as required.

cluster

Control Center: One or more Control Center resource pools.

ZooKeeper: The group of hosts that are configured as ZooKeeper nodes.

Packaging considerations

Cisco UCS Performance Manager is distributed as a preconfigured appliance in the following, self-contained packages:

- A self-installing ISO package for Microsoft Hyper-V systems
- A VMware OVA package for vSphere systems

The appliance includes the run-time environment (CentOS 7.2) with Control Center installed, and Cisco UCS Performance Manager loaded into the local Docker registry. Most customers will only need to deploy a single guest system.

Note If you are uncertain whether your environment requires a single-host or a multi-host deployment, please use the Cisco UCS Performance Manager Deployment Calculator. The calculator is available at <https://zenoss.github.io/deployment-calculator/#/>.

Deployment considerations

The features of Control Center in this release affect deployments of Cisco UCS Performance Manager in the following ways.

- All Control Center hosts in a resource pool should have identical hardware resources.
- All Cisco UCS Performance Manager data is stored on the Control Center master host. Agent hosts access the data through the distributed file system, which is based on NFS.
- Using hypervisor commands alone to pause or stop Cisco UCS Performance Manager virtual machines is unsupported. Cisco UCS Performance Manager relies on timestamps and the system clock to keep services in sync, and pausing or stopping a virtual machine by using a hypervisor command disrupts the synchronization. Cisco recommends the following procedure for pausing or stopping Cisco UCS Performance Manager virtual machines:
 - 1 Log in to the Control Center browser interface.
 - 2 Stop Cisco UCS Performance Manager.
 - 3 Use a hypervisor feature to shut down the virtual machine, or log in to the virtual machine as root and enter a `shutdown` command.

Similarly, vSphere vMotion is not supported unless all of the virtual machines in your Cisco UCS Performance Manager deployment are paused or stopped.

- vSphere hosts that run Control Center guest systems must be configured to synchronize their clocks with public or private NTP servers. Control Center guest systems synchronize their clocks with their vSphere hosts through an hourly invocation of VMware Tools. For more information about configuring a vSphere host for NTP, refer to your VMware documentation.
- Multi-host deployments of Cisco UCS Performance Manager running on Hyper-V hosts must be configured to synchronize their clocks with public or private NTP servers. This guide includes instructions for configuring NTP on Control Center guest systems. Hyper-V hosts do not provide the equivalent of VMware Tools so that guest systems can synchronize with the host.
- Control Center includes backup and restore features for archiving and restoring Cisco UCS Performance Manager data. Hypervisor backups can be used instead of Control Center backups when Cisco UCS Performance Manager, Control Center, and the Control Center master host are shut down cleanly and completely.
- A single-host deployment has enough compute, memory, and storage resources to support up to 500 servers. However, multi-host deployments include important benefits beyond additional resources:
 - A multi-host deployment includes a ZooKeeper cluster, which enhances Control Center reliability.
 - A multi-host deployment can be configured for high availability.

This guide includes separate parts for creating single-host and multi-host deployments. After completing the instructions in either part, proceed to *Managing Cisco UCS Performance Manager with Control Center* on page 114 for information about starting Cisco UCS Performance Manager.

Part I: Creating a single-host deployment

The chapters in this part include all of the required and optional procedures for creating a single-host deployment of Cisco UCS Performance Manager. To create a multi-host deployment, either during a fresh install or after operating a single-host deployment for a while, see [Creating a multi-host deployment](#) on page 34.

A single-host deployment requires one static IPv4 address for the system you create with the Cisco UCS Performance Manager virtual appliance.

When all of the installation procedures are completed, proceed to [Managing Cisco UCS Performance Manager with Control Center](#) on page 114.

2

Creating a Control Center master host

This chapter describes how to install a Cisco UCS Performance Manager virtual appliance as a Control Center master host, using either VMware vSphere or Microsoft Hyper-V.

Note If you plan to migrate data from a version 1.1.x system, please ensure that the version 1.1.x system and the version 2.0.x system can use a common datastore or datastore cluster.

Creating a virtual machine

You may create a virtual machine for the Cisco UCS Performance Manager appliance with VMware vSphere or Microsoft Hyper-V. Choose one of the procedures in this section.

Creating a virtual machine with vSphere

To perform this task, you need:

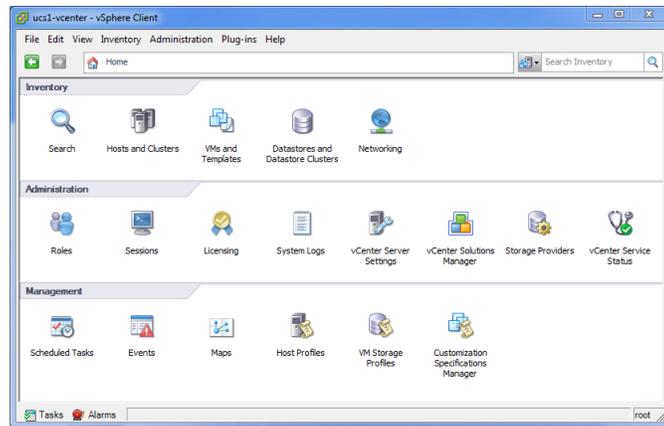
- A VMware vSphere client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

Use this procedure to install the Cisco UCS Performance Manager OVA package as a virtual machine managed by vSphere Server. The procedure includes steps to add a disk for backups.

The procedure is slightly different with different versions of VMware vSphere Client.

Note VMware vSphere Client 5.0.0 does not include a library that is needed to deploy compressed OVA files. You may uncompress the OVA package and then deploy it, or download and install *the missing library*. Cisco recommends installing the library.

- 1 Download the Cisco UCS Performance Manager OVA file from the *Cisco UCS Performance Manager* site to your workstation.
- 2 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home** view.

Figure 1: vSphere client Home view

- 3 From the **File** menu, select **Deploy OVF Template....**
- 4 In the **Source** panel, specify the path of the Cisco UCS Performance Manager package, and then click **Next >**.
- 5 In the **OVF Template Details** panel, click **Next >**.
- 6 In the **Name and Location** panel, provide a name and a location for the server.
 - a In the **Name** field, enter a new name or use the default.
 - b In the **Inventory Location** area, select a data center for the virtual machine.
 - c Click **Next >**.
- 7 In the **Host / Cluster** panel, select a host system, and then click **Next >**.
- 8 In the **Storage** panel, select a storage system with sufficient space for your UCS system, and then click **Next >**.
- 9 In the **Disk Format** panel, select **Thin Provision**, and then click **Next >**.
- 10 In the **Ready to Complete** panel, review the deployment settings, and then click **Finish**.
Please do not check the check box labeled **Power on after deployment**.
- 11 Navigate to the new virtual machine's **Getting Started** tab, and then click the **Edit virtual machine settings** link.
- 12 On the **Hardware** tab, click the **Add...** button.
- 13 In the **Add Hardware** dialog, select **Hard Disk**, and then click the **Next** button.
- 14 In the **Select a Disk** pane, click the **Create a new virtual disk** radio button, and then click the **Next** button.
- 15 In the **Create a Disk** pane, configure the virtual disk.
 - a In the **Capacity** area, set the disk size.
Cisco recommends 300GB.
 - b In the **Disk Provisioning** area, choose the option you prefer.
 - c In the **Location** area, choose the option you prefer.
 - d Click the **Next** button.
- 16 In the **Advanced Options** pane, configure the mode.
 - a In the **Mode** area, check the **Independent** check box.
 - b Click the **Persistent** radio button.
 - c Click the **Next** button.
- 17 In the **Ready to Complete** pane, confirm the virtual disk configuration, and then click the **Finish** button.
- 18 At the bottom of the **Virtual Machine Properties** dialog, click the **OK** button.
- 19 On the new virtual machine's **Getting Started** tab, click the **Power on virtual machine** link.

Creating a virtual machine with Hyper-V

To perform this task, you need:

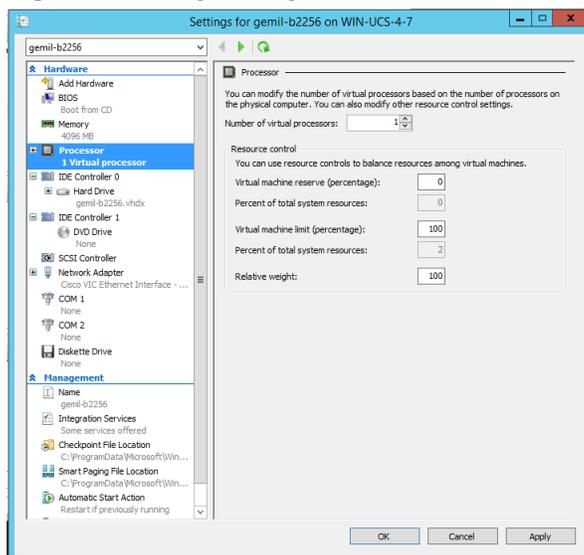
- A Microsoft Remote Desktop client

- Administrator privileges on a Microsoft Hyper-V server
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

Use this procedure to install the Cisco UCS Performance Manager appliance as a virtual machine managed by Microsoft Hyper-V.

- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Download the Cisco UCS Performance Manager ISO file from the [Cisco UCS Performance Manager](#) site to the Hyper-V host.
- 3 Start **Hyper-V Manager**.
- 4 In the left column, select a server to host the virtual machine.
- 5 From the **Action** menu, select **New > Virtual Machine....**
- 6 In the **New Virtual Machine Wizard** dialog, display the **Specify Name and Location** panel.
If the first panel displayed is the **Before You Begin** panel, click **Next**.
- 7 In the **Specify Name and Location** panel, provide a name for the virtual machine, and then click **Next**.
- 8 In the **Specify Generation** panel, select **Generation 1**, and then click **Next**.
- 9 In the **Assign Memory** panel, enter 65536 (64GB) in the **Startup memory** field, and then click **Next**.
- 10 In the **Configure Networking** panel, select **Cisco VIC Ethernet Interface - Virtual Switch**, and then click **Next**.
- 11 In the **Connect Virtual Hard Disk** panel, select **Create a virtual hard disk**, enter 300 in the **Size** field, and then click **Next**.
- 12 In the **Installation Options** panel, specify the Cisco UCS Performance Manager ISO package.
 - a Select **Install an operating system from a bootable CD/DVD-ROM**.
 - b Select **Image file (.iso)**, and then specify the location of the Cisco UCS Performance Manager ISO image file.
 - c Click **Next**.
- 13 In the **Summary** panel, review the virtual machine specification, and then click **Finish**.
Hyper-V Manager creates the new virtual machine, and then closes the **New Virtual Machine Wizard** dialog.
- 14 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Settings....**
- 15 In the **Hardware** area of the **Settings** dialog, select **Processor**.

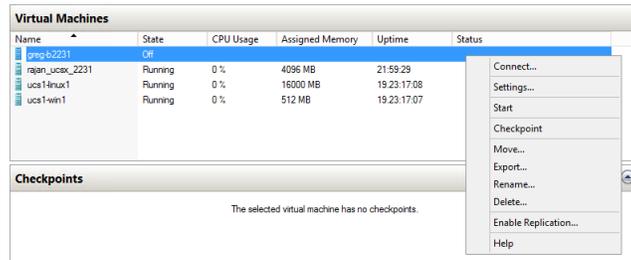
Figure 2: Settings dialog, Processor selected



- 16 In the **Processor** area, enter 8 in the **Number of virtual processors**, and then click **OK**.

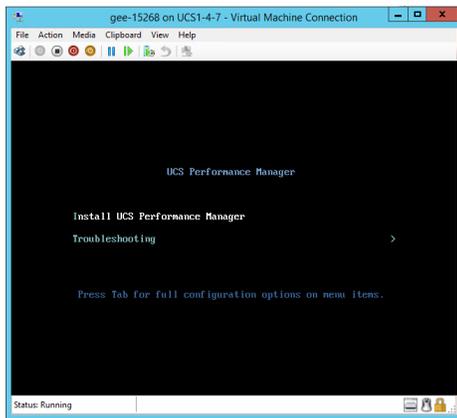
- 17 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Start**.

Figure 3: Starting a virtual machine



- 18 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Connect**.
- 19 In the **Virtual Machine Connection** window, press the **Enter** key.

Figure 4: Appliance installation start screen



The appliance installation process takes about 15 minutes, and should complete with no additional input.

Configuring the Control Center host mode

Perform this procedure immediately after creating and starting a Control Center host. All Control Center deployments must include one system configured as the master host.

- 1 Gain access to the console interface of the Control Center host through your hypervisor console interface.

Figure 5: Initial hypervisor console login prompt

```

YOU HAVE NOT CHOSEN A ROLE FOR THIS APPLIANCE.
PLEASE LOGIN TO CHOOSE ROLE AND ACTIVATE UCS Performance Manager

Welcome to UCS Performance Manager

After initial setup, the Control Center UI can be accessed by
browsing to:

  https://ucspm:50443
  (default username/password is ccuser/ucspm)

Ensure that ucspm is resolvable to 10.88.121.248, either through your
DNS system or through a HOSTS entry on the browser client. For more
information refer to the installation notes.

You can log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. The
root password defaults to 'ucspm'

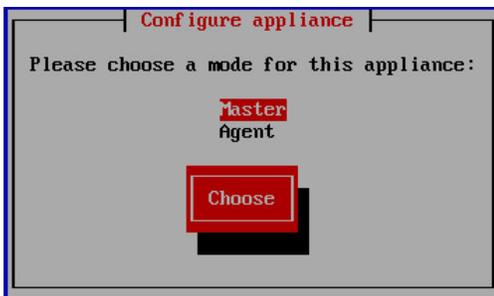
Linux Kernel 3.10.0-327.el7.x86_64 on an x86_64
ucspm login: _

```

- 2 Log in as the `root` user.
The initial password is `ucspm`.
- 3 The system prompts you to enter a new password for `root`.

Note Passwords must include a minimum of eight characters, with at least one character from three of the following character classes: uppercase letter, lowercase letter, digit, and special.

- 4 The system prompts you to enter a new password for `ccuser`.
The `ccuser` account is the default account for gaining access to the Control Center browser interface.
- 5 Select the master role for the host.



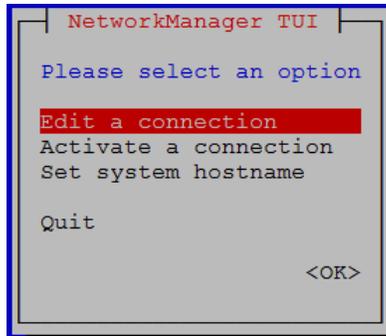
- a In the **Configure appliance** menu, press the **Tab** key to select the **Choose** button.
 - b Press the **Enter** key.
- The system reboots.

Edit a connection

The default configuration for network connections is DHCP. To configure static IPv4 addressing, perform this procedure.

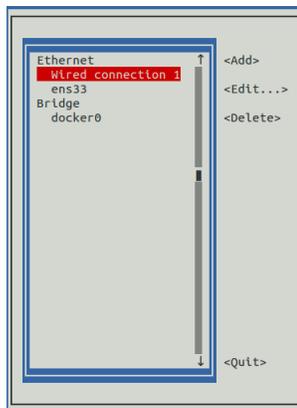
- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.
 - b Press the **Tab** key to select the **Run** button.

- c Press the **Enter** key.



- 4 On the **NetworkManager TUI** menu, select **Edit a connection**, and then press the **Return** key. The TUI displays the connections that are available on this host.

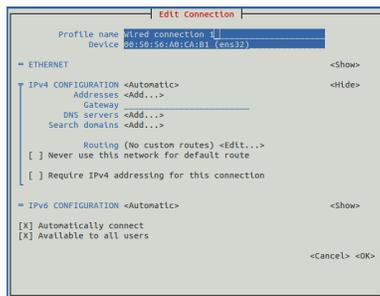
Figure 6: Example: Available connections



- 5 Use the down-arrow key to select **Wired Connection 1**, and then press the **Return** key.

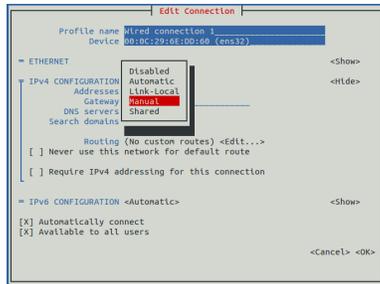
Note Do not use the TUI to edit the `docker0` connection. For more information, see [Configuring the Docker virtual bridge](#) on page 132.

Figure 7: Example: Edit Connection screen



Use the **Tab** key and the arrow keys to navigate among options in the **Edit Connection** screen, and use the **Return** key to toggle an option or to display a menu of options.

- 6 Optional: If the **IPv4 CONFIGURATION** area is not visible, select its display option (**<Show>**), and then press the **Return** key.
- 7 In the **IPv4 CONFIGURATION** area, select **<Automatic>**, and then press the **Return** key.

Figure 8: Example: IPv4 Configuration options

- 8 In the submenu, use the down-arrow key to select **Manual**, and then press the **Return** key.

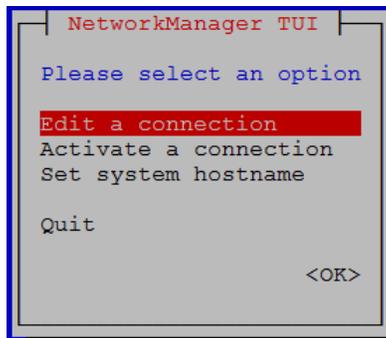
Note For static networking, the option next to **IPv4 CONFIGURATION** must be **Manual**. If it is **Automatic**, the host uses an address from a DHCP server.

- 9 Enter an IPv4 address in CIDR notation.
 - a Use the **Tab** key or the down arrow key to select the **<Add...>** option next to **Addresses**, and then press the **Return** key.
 - b In the **Addresses** field, enter an IPv4 address, followed by the solidus character (/) and then the prefix length.
For more information, see [CIDR prefix lengths for commonly-used netmasks](#) on page 133.
 - c Press the **Return** key.
- 10 Configure the **Gateway** and **DNS servers** fields with IPv4 addresses.
- 11 Use the **Tab** key or the down arrow key to select the **<OK>** option at the bottom of the **Edit Connection** screen, and then press the **Return** key.
- 12 In the available connections screen, use the **Tab** key to select the **<Quit>** option, and then press the **Return** key.
- 13 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

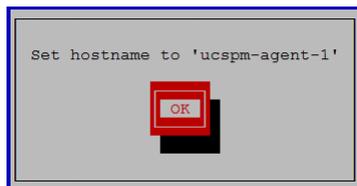
Set system hostname

The default hostname of a Control Center host is `ucspm`. To change the hostname, perform this procedure.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.
 - b Press the **Tab** key to select the **Run** button.
 - c Press the **Enter** key.



- 4 Display the hostname entry field.
 - a In the **NetworkManager TUI** menu, use the down-arrow key to select **Set system hostname**.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.
- 5 In the **Hostname** field, enter the new hostname.
You may enter either a hostname or a fully-qualified domain name.
- 6 Press the **Tab** key twice to select the **OK** button, and then press the **Enter** key.



- 7 In the confirmation dialog, press the **Return** key.
- 8 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

Adding a disk for backups to Hyper-V guest systems

This procedure is not necessary on VMware vSphere guest systems, only Microsoft Hyper-V guest systems. Perform this procedure to add disk storage for backups.

To perform this procedure, you must be logged in to the Hyper-V host of the Cisco UCS Performance Manager guest system as Administrator, or as a user with Administrator privileges.

- 1 In the left column, select the server that is hosting the Cisco UCS Performance Manager guest system, and then right-click to select **New > Hard Disk...**
- 2 In the **New Virtual Hard Disk Wizard** dialog, navigate to the **Choose Disk Format** panel.
- 3 Click the **VHDX** radio button, and then click the **Next** button.
- 4 In the **Choose Disk Type** panel, click the **Dynamically expanding** radio button, and then click the **Next** button.
- 5 In the **Specify Name and Location** panel, enter a name for the disk in the **Name** field, and then click the **Next** button.
- 6 In the **Configure Disk** panel, click the **Create a new blank virtual hard disk** radio button, enter the disk size in the **Size** field, and then click the **Next** button.
Cisco recommends 300GB.
- 7 In the **Summary** panel, review the virtual disk settings, and then click the **Finish** button.

- 8 In **Hyper-V Manager**, right-click the virtual machine of the Control Center master host, and then select **Settings...**
- 9 In the **Settings** dialog, select **SCSI Controller** from the **Hardware** list in the left column.
- 10 In the **SCSI Controller** area on the right side, select **Hard Drive**, and then click the **Add** button.
- 11 In the **Hard Drive** area, click the **Virtual hard disk** radio button, and then click the **Browse** button.
- 12 In the **Open** dialog, select the hard disk image created previously, and then click the **Open** button.
- 13 In the **Settings** dialog, click the **OK** button.

Preparing a disk for backups

Use this procedure to format the second disk for Control Center backups, and mount it in the master host filesystem.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as **root**.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Verify the status of the disk to format.

The disk is mounted as `/dev/sdb`. Best practice: Always verify a device or partition before formatting it, which destroys all data on a device.

```
lsblk -p --output=NAME,SIZE,TYPE,MOUNTPOINT /dev/sdb
```

Example output:

```
NAME          SIZE TYPE MOUNTPOINT
/dev/sdb      300G disk
```

- 4 Create and label an XFS file system.

```
mkfs -t xfs -L BACKUPS /dev/sdb
```

- 5 Set the permissions bits of the filesystem mount point.

```
chmod 777 /opt/serviced/var/backups
```

- 6 Create an entry in the `/etc/fstab` file.

```
echo "/dev/sdb /opt/serviced/var/backups xfs defaults 0 0" \
  >> /etc/fstab
```

- 7 Mount the file system, and then verify it mounted correctly.

```
mount -a && mount | grep backups
```

Example result:

```
/dev/sdb1 on /opt/serviced/var/backups type xfs
(rw,relatime,attr2,inode64,noquota)
```

Deploying Cisco UCS Performance Manager

Perform this procedure on logging in to Control Center for the first time.

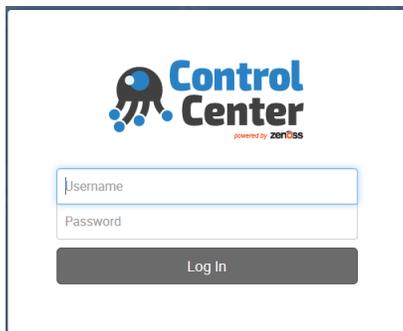
- 1 Display the login page of the Control Center browser interface.
Replace *IP-Address* with the IP address of the Control Center virtual machine:

```
https://IP-Address:50443
```

You can use the hostname of the Control Center virtual machine instead of its IP address, if name resolution of the hostname is configured in your environment.

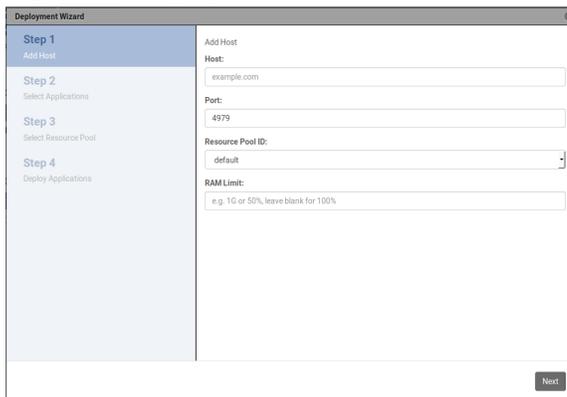
Note The web server that listens for Control Center interface requests typically takes 1-2 minutes to start after the the Control Center master host is started.

Figure 9: Control Center login page



- 2 At the login page, enter `ccuser` and its password.

Figure 10: Deployment Wizard



If the Deployment Wizard does not display automatically, then click **+ Application**, located at the right side of the page.

- 3 In the **Deployment Wizard**, add the master host to the `default` resource pool.

The host to add is the Control Center master host.

- a In the **Host** field, enter the hostname or IP address of the Control Center master host.

If you enter a hostname, all hosts in your Control Center cluster must be able to resolve the name, either through an entry in `/etc/hosts`, or through a nameserver on your network.

- b Skip the **Port** field.

This field specifies the port for remote procedure calls; the correct value is 4979.

- c In the **Resource Pool ID** field, select `default` from the list.
 - d In the **RAM Limit** field, enter the amount of non-system RAM to allocate to Control Center and Cisco UCS Performance Manager.
The amount may be specified as an absolute value or as a percentage:
 - To specify an absolute amount of non-system RAM, enter a number followed by M for megabytes, G for gigabytes, or T for terabytes. For example, 65536M, 64G, and 0.0625T are equivalent values.
 - To specify a percentage of non-system RAM, enter a number between 0 and 100 followed by the percent sign (%) character.

If you do not specify a value, the amount of non-system RAM allocated to Control Center and Cisco UCS Performance Manager is 100%.
 - e At the bottom of the **Deployment Wizard**, click **Next**.
- 4 Select the application to deploy.
 - a Select `ucspm`.
 - b At the bottom of the **Deployment Wizard**, click **Next**.
 - 5 Select the resource pool for the application.
 - a Select `default`.
 - b At the bottom of the **Deployment Wizard**, click **Next**.
 - 6 Choose a deployment ID and deploy Cisco UCS Performance Manager.
 - a In the **Deployment ID** field, enter a name for this deployment of Cisco UCS Performance Manager.
 - b At the bottom of the **Deployment Wizard**, click **Deploy**.

Figure 11: Cisco UCS Performance Manager is deployed

The screenshot shows the Cisco Control Center interface. The top navigation bar includes 'Applications', 'Resource Pools', 'Hosts', 'Logs', 'Backup / Restore', and user information. The main content area is titled 'Applications' and contains a table with the following data:

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	✓	Internal	N/A	N/A	N/A
ucspm (v2.0.1)	Cisco UCS Performance Manager	⊖	Test	default	https://ucspm-cc-master-50443 https://cc-master	▶ Start ■ Stop ○ Delete

Below the table, there is a section for 'Application Templates' with one entry:

Application Template	ID	Description	Actions
ucspm (v2.0.1)	59f1337508ecf73bd27c2283694f2ce5	Cisco UCS Performance Manager	○ Delete

- 7 At the top of the page, click **Logout**.
The control is located at the right side of the page.

Note Do not start Cisco UCS Performance Manager at this time.

If you plan to migrate data from a Cisco UCS Performance Manager version 1.1.x system, do not perform any other tasks in this guide at this time. Instead, refer to the *Cisco UCS Performance Manager Migration Guide*.

Otherwise, proceed to the next chapter.

3

Enabling access to browser interfaces

Control Center and Cisco UCS Performance Manager have independent browser interfaces served by independent web servers. Both web servers are configured to use SSL/TLS communications.

The Control Center web server listens at the hostname of the Control Center master host and port 50443. For a Control Center master host with the fully-qualified domain name (FQDN) `cc-master.example.com`, the hostname URL is `https://cc-master:50443`. As always, you may substitute an IP address for the hostname portion of the URL.

The Cisco UCS Performance Manager web server listens at a *port public endpoint* and a *virtual host public endpoint*.

- The default *port public endpoint* is the hostname of the Control Center master host and port 443. For the FQDN `cc-master.example.com`, the URL of the default port public endpoint is `https://cc-master`. If the Control Center master host has more than one network interface, you can configure additional port public endpoints with different hostnames. Also, you can disable SSL/TLS communications for a port public endpoint, if desired.

To use a port public endpoint to gain access to the Cisco UCS Performance Manager browser interface, no additional network name resolution entries are required. The default entries for the network interface(s) of the Control Center master host are sufficient.

- The default *virtual host public endpoint* is the text `ucspm` prepended to the hostname of the Control Center master host and port 50443. For the FQDN `cc-master.example.com`, the URL of the default virtual host public endpoint is `https://ucspm.cc-master:50443`. You can change the name of the default virtual host and configure additional virtual host public endpoints, if desired.

To use a virtual host public endpoint to gain access to the Cisco UCS Performance Manager browser interface, you must add name resolution entries for the virtual host to the DNS servers in your environment or to the hosts files of individual client systems.

The following sections provide additional information about public endpoints, and instructions for creating public endpoints and for configuring virtual host name resolution.

Creating public endpoints

This section describes how to create a port public endpoint and a virtual host public endpoint. The following table outlines the process for each.

Port public endpoint	Virtual host public endpoint
1 Create the endpoint	1 Create the endpoint

Port public endpoint	Virtual host public endpoint
2 Configure the Zope service	2 Configure the Zope service
	3 Configure virtual host name resolution

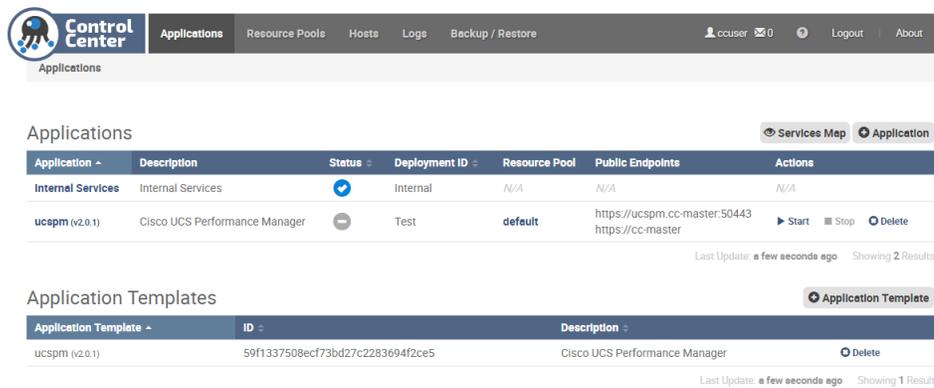
To change an existing public endpoint, create a new endpoint and then delete the existing endpoint.

Note Virtual host public endpoints must use SSL/TLS communications. Port public endpoints can communicate with or without SSL/TLS.

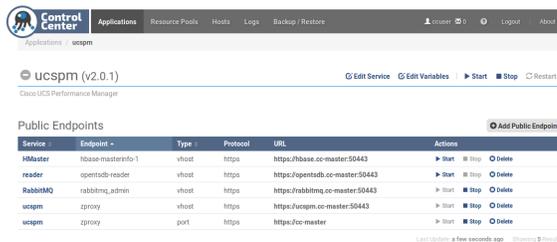
Creating a port public endpoint

Use this procedure to create a new port public endpoint. Port public endpoints can communicate with or without SSL/TLS.

- 1 Log in to the Control Center browser interface.



- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).



- 3 Click **+ Add Public Endpoint**, located above the **Public Endpoints** table, on the right side.

Add Public Endpoint

VHost public endpoints are accessible by hostname (eg, `https://zenoss.mckraken`), while **Port** public endpoints are accessible by ip:port or hostname:port (eg, `myhost:54321` or `10.87.1.100:54321`).

Type:
 Port VHost

Service - Endpoint:
 HMaster - hbase-master-1

Host:
 cc-master

Port:
 54321

Protocol:
 HTTPS

After the public endpoint is added, the selected service will be restarted if currently running.

The default view of the **Add Public Endpoint** dialog displays the fields for creating a port public endpoint.

4 Define a new port public endpoint.

- a In the **Type** area, click **Port**.
- b From the **Service - Endpoint** list, select **ucspm - zproxy**.

The selection is the last entry in the list.

- c In the **Host** field, enter a hostname or IP address that is assigned to a network interface on the Control Center master host.

The default value is the hostname that was added with the Deployment Wizard when Cisco UCS Performance Manager was initially deployed. If the Control Center master host has more than one network interface, you may add the hostname or IP address assigned to one of the other interfaces.

- d In the **Port** field, enter a safe, unused port number greater than or equal to 1024 and less than or equal to 65535.

For a list of ports considered unsafe, see [Unsafe ports on Chrome](#). For the list of ports used by the Control Center master host, see [Security considerations](#) on page 131.

- e In the **Protocol** field, select **HTTPS** or **HTTP**.

You can set up a secure proxy server to handle HTTP requests sent to a port public endpoint, if desired.

- f Click **Add and Restart Service**.

Configure the **Zope** service to use the new port public endpoint. Choose one of the configuration options in the following table.

Zope configuration	Procedure
HTTPS and the default secure proxy server	Configuring Zope for HTTPS and the default secure proxy server on page 25
HTTP and no proxy server	Configuring Zope for HTTP and no proxy server on page 27
HTTP and a secure proxy server other than the default	Configuring Zope for HTTP and a secure proxy server on page 28

Note When you configure Zope for HTTP protocol and no proxy server, you can only gain access to the Cisco UCS Performance Manager browser interface through port public endpoints configured for HTTP. Virtual host public endpoints must use HTTPS protocol, so any existing virtual host public endpoints stop working.

Configuring Zope for HTTPS and the default secure proxy server

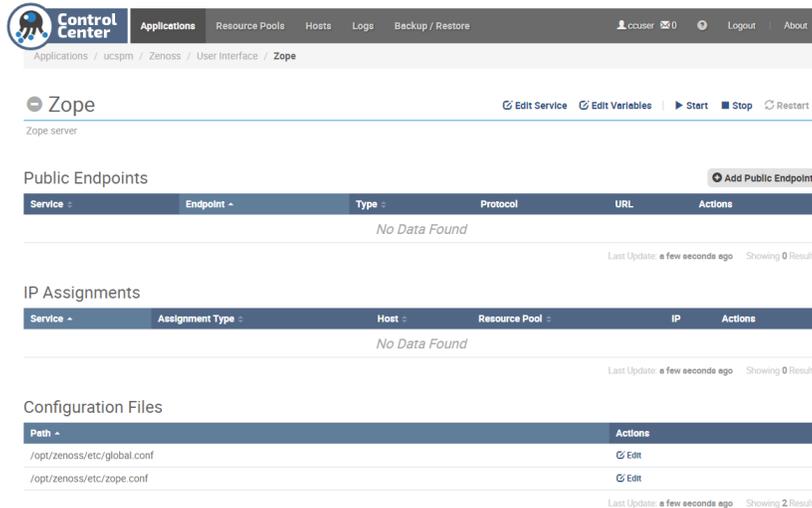
Before performing this procedure, create a port public endpoint or a virtual host public endpoint to use the HTTPS protocol.

Use this procedure to configure the **Zope** service for SSL/TLS communications and the secure proxy server that is included in Cisco UCS Performance Manager.

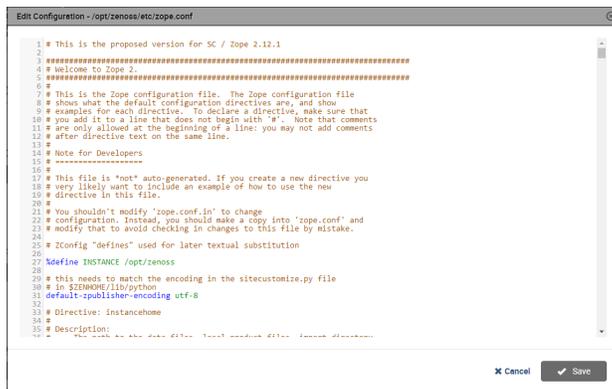
- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.

The Control Center browser interface displays the details page of the **Zope** service.

- 4 Scroll to the top of the **Zope** service details page.



- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the **/opt/zenoss/etc/zope.conf** file.



- 6 Configure Zope for secure communications with the proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the **cgi-environment** directive.

The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for SSL/TLS communications:

```
<cgi-environment>
  HTTPS ON
</cgi-environment>
```

- 7 Configure the Beaker add-on product to use secure communications.
 - a In the **Edit Configuration** dialog, scroll down to the **product-config** directive.

The directive is at the bottom the file, on or near line 1122.

- b Set the value of the `session.secure` key to `True`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

Next steps:

- If you created a port public endpoint before performing this procedure, the endpoint is ready to use.
- If you created a virtual host public endpoint before performing this procedure, proceed to [Configuring name resolution for virtual hosts](#) on page 32.

Configuring Zope for HTTP and no proxy server

Before performing this procedure, create a port public endpoint to use the HTTP protocol. For more information, see [Creating a port public endpoint](#) on page 24.

Use this procedure to configure the **Zope** service for insecure communications with Cisco UCS Performance Manager browser interface clients.

Note When you configure Zope for insecure communications, any existing virtual host public endpoints stop working.

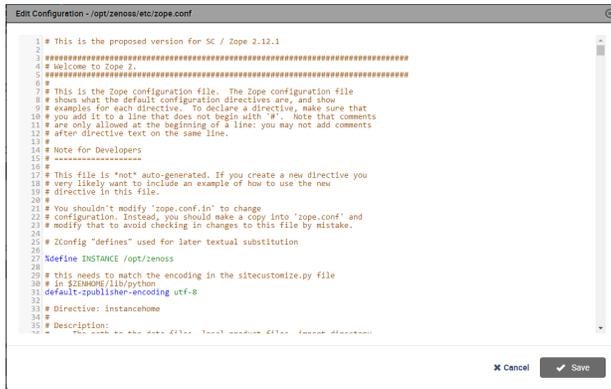
- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.
The Control Center browser interface displays the details page of the **Zope** service.
- 4 Scroll to the top of the **Zope** service details page.

The screenshot shows the Control Center interface for the Zope service. The breadcrumb trail is: Applications / ucspm / Zenoss / User Interface / Zope. The service name is Zope, and it is currently stopped. There are three tables displayed:

- Public Endpoints:** A table with columns: Service, Endpoint, Type, Protocol, URL, Actions. It shows "No Data Found".
- IP Assignments:** A table with columns: Service, Assignment Type, Host, Resource Pool, IP, Actions. It shows "No Data Found".
- Configuration Files:** A table with columns: Path, Actions. It lists two files:

Path	Actions
/opt/zenoss/etc/global.conf	Edit
/opt/zenoss/etc/zope.conf	Edit

- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the `/opt/zenoss/etc/zope.conf` file.



- 6 Configure Zope for insecure communications with the proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the `cgi-environment` directive.

The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for insecure communications:

```
<cgi-environment>
  HTTPS OFF
</cgi-environment>
```

- 7 Configure the Beaker add-on product to use insecure communications.
 - a In the **Edit Configuration** dialog, scroll down to the `product-config` directive.

The directive is at the bottom the file, on or near line 1122.
 - b Set the value of the `session.secure` key to `False`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

Configuring Zope for HTTP and a secure proxy server

Before performing this procedure, create a port public endpoint to use the HTTP protocol. For more information, see [Creating a port public endpoint](#) on page 24.

Use this procedure to configure the **Zope** service for SSL/TLS communications and a secure proxy server that is available on your network.

- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.

The Control Center browser interface displays the details page of the **Zope** service.
- 4 Scroll to the top of the **Zope** service details page.

The screenshot shows the Control Center interface for the Zope server. At the top, there are navigation tabs for Applications, Resource Pools, Hosts, Logs, and Backup / Restore. The main content area is titled 'Zope' and includes buttons for 'Edit Service', 'Edit Variables', 'Start', 'Stop', and 'Restart'. Below this, there are three tables: 'Public Endpoints', 'IP Assignments', and 'Configuration Files'. The 'Configuration Files' table has two rows, each with a path and an 'Edit' action button.

- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the `/opt/zenoss/etc/zope.conf` file.

The screenshot shows the 'Edit Configuration' dialog for the file `/opt/zenoss/etc/zope.conf`. The dialog contains a text editor with the following content:

```

1 # This is the proposed version for SC / Zope 2.12.1
2
3 #####
4 # Welcome to Zope 2.
5 #####
6
7 # This is the Zope configuration file. The Zope configuration file
8 # shows what the default configuration directives are, and show
9 # examples for each directive. To declare a directive, make sure that
10 # you add it to a line that does not begin with "#". Note that comments
11 # are only allowed at the beginning of a line; you may not add comments
12 # after directive text on the same line.
13 #
14 # Note for Developers
15 # =====
16 #
17 # This file is "not" auto-generated. If you create a new directive you
18 # very likely want to include an example of how to use the new
19 # directive in this file.
20 #
21 # You shouldn't modify 'zope.conf.in' to change
22 # configuration. Instead, you should make a copy into 'zope.conf' and
23 # modify that to avoid checking in changes to this file by mistake.
24 #
25 # Zconfig "defines" used for later textual substitution
26 #
27 #define INSTANCE /opt/zenoss
28 #
29 # this needs to match the encoding in the sitecustomize.py file
30 # in $ZENHOME/lib/python
31 #default-publisher-encoding utf-8
32 #
33 # Directive: instancehome
34 #
35 # Description: ...

```

At the bottom of the dialog, there are 'Cancel' and 'Save' buttons.

- 6 Configure Zope for secure communications with your proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the `cgi-environment` directive. The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for SSL/TLS communications:

```

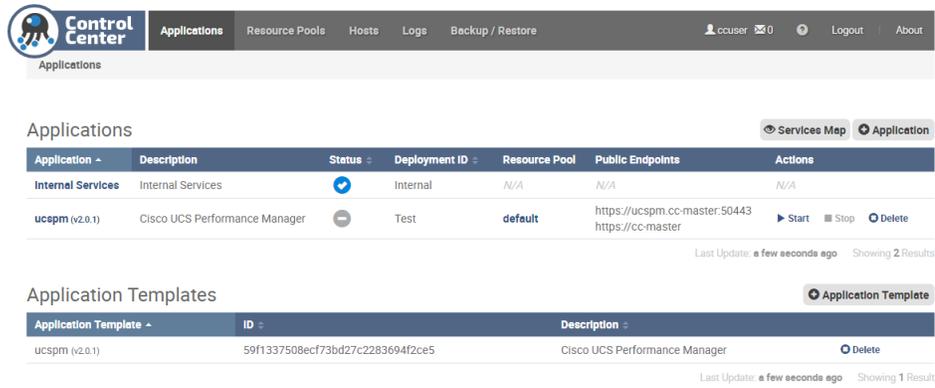
<cgi-environment>
  HTTPS ON
</cgi-environment>

```
- 7 Configure the Beaker add-on product to use secure communications.
 - a In the **Edit Configuration** dialog, scroll down to the `product-config` directive. The directive is at the bottom the file, on or near line 1122.
 - b Set the value of the `session.secure` key to `True`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

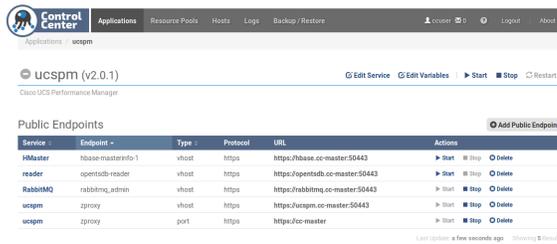
Creating a virtual host public endpoint

Use this procedure to create a new virtual host public endpoint. Virtual host public endpoints must use SSL/TLS communications.

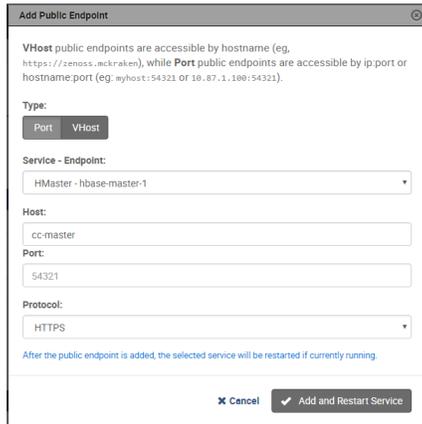
- 1 Log in to the Control Center browser interface.



2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).



3 Click **+ Add Public Endpoint**, located above the **Public Endpoints** table, on the right side.



The default view of the **Add Public Endpoint** dialog displays the fields for creating a port public endpoint.

4 Define a new virtual host public endpoint.

a In the **Type** area, click **VHost**.

Add Public Endpoint

VHost public endpoints are accessible by hostname (eg. `https://zenoss.mckraken`), while **Port** public endpoints are accessible by ip port or hostname:port (eg. `myhost:54321` or `10.87.1.100:54321`).

Type:

Port VHost

Service - Endpoint:

HMaster - hbase-master-1

VHost Hostname:

After the public endpoint is added, the selected service will be restarted if currently running.

Cancel Add and Restart Service

b From the **Service - Endpoint** list, select **ucspm - zproxy**.

The selection is the last entry in the list.

c In the **VHost Hostname** field, enter a virtual hostname.

The following strings of text are valid in this field:

- A fully-qualified domain name (FQDN). Any string of text that includes one or more full stop characters (.) is treated as an FQDN.
- A string of text that contains only letters and one or more hyphen characters (-). The string is prepended to the hostname of the Control Center master host, with a full stop character (.) separating the string and the hostname.

d Click **Add and Restart Service**.

Configuring Zope for HTTPS and the default secure proxy server

Before performing this procedure, create a port public endpoint or a virtual host public endpoint to use the HTTPS protocol.

Use this procedure to configure the **Zope** service for SSL/TLS communications and the secure proxy server that is included in Cisco UCS Performance Manager.

- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.
The Control Center browser interface displays the details page of the **Zope** service.
- 4 Scroll to the top of the **Zope** service details page.

Control Center Applications Resource Pools Hosts Logs Backup / Restore user Logout About

Applications / ucspm / Zenoss / User Interface / Zope

Zope Edit Service Edit Variables Start Stop Restart

Zope server

Public Endpoints Add Public Endpoint

Service	Endpoint	Type	Protocol	URL	Actions
No Data Found					

Last Update: a few seconds ago Showing 0 Results

IP Assignments

Service	Assignment Type	Host	Resource Pool	IP	Actions
No Data Found					

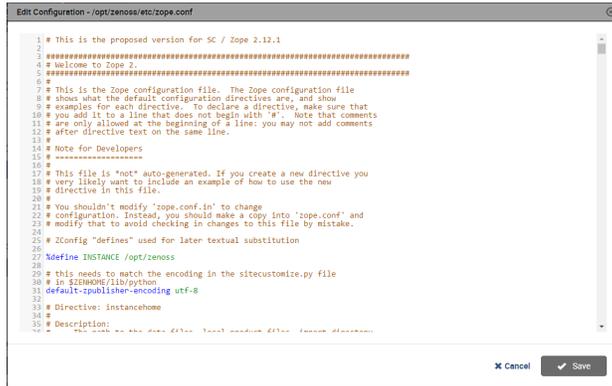
Last Update: a few seconds ago Showing 0 Results

Configuration Files

Path	Actions
/opt/zenoss/etc/global.conf	Edit
/opt/zenoss/etc/zope.conf	Edit

Last Update: a few seconds ago Showing 2 Results

- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the `/opt/zenoss/etc/zope.conf` file.



- 6 Configure Zope for secure communications with the proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the `cgi-environment` directive.

The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for SSL/TLS communications:

```
<cgi-environment>
  HTTPS ON
</cgi-environment>
```

- 7 Configure the Beaker add-on product to use secure communications.
 - a In the **Edit Configuration** dialog, scroll down to the `product-config` directive.

The directive is at the bottom the file, on or near line 1122.
 - b Set the value of the `session.secure` key to `True`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

Next steps:

- If you created a port public endpoint before performing this procedure, the endpoint is ready to use.
- If you created a virtual host public endpoint before performing this procedure, proceed to [Configuring name resolution for virtual hosts](#) on page 32.

Configuring name resolution for virtual hosts

To enable access to browser interfaces by virtual hosts, add name resolution entries to the DNS servers in your environment or to the hosts files of individual client systems.

- On Windows client systems, the hosts file is `C:\Windows\System32\drivers\etc\hosts`.
- Linux and OS/X client systems, the hosts file is `/etc/hosts`.

Name resolution syntax

The following line shows the syntax of the entry to add to a name resolution file:

```
IP-Address FQDN Hostname ucspm.Hostname
```

For example, the following entry identifies a Control Center master host at IP address 192.0.2.12, hostname `cc-master`, in the `example.com` domain.

```
192.0.2.12 cc-master.example.com cc-master ucspm.cc-master
```

Configuring name resolution on a Windows 7 system

To perform this procedure, you need Windows Administrator privileges.

- 1 Log in to the Windows 7 system as a user with Administrator privileges.
- 2 From the **Start** menu, highlight **All Programs > Accessories > Notepad**.
- 3 Right click, and then select **Run as administrator**.
- 4 From the Notepad **File** menu, select **Open**.
- 5 In the **File name** field of the **Open** window, enter `C:\Windows\System32\drivers\etc\hosts`.
- 6 Add a name resolution entry to the end of the file.
For more information, see [Name resolution syntax](#) on page 32.
- 7 Save the file, and then exit Notepad.

Configuring name resolution on a Linux or OS/X system

To perform this procedure, you need superuser privileges on the client system.

- 1 Log in to the client system as `root` or as a user with `sudo` privileges.
- 2 Open the `/etc/hosts` file in a text editor.
- 3 Add a name resolution entry to the end of the file.
For more information, see [Name resolution syntax](#) on page 32.
- 4 Save the file, and then close the editor.

Part II: Creating a multi-host deployment

The chapters in this part include all of the required and optional procedures for creating a multi-host deployment of Cisco UCS Performance Manager. The procedures support either a fresh install of Cisco UCS Performance Manager or the conversion of a single-host deployment to a multi-host deployment. To install a single-host deployment, see [Creating a single-host deployment](#) on page 11.

A multi-host Cisco UCS Performance Manager deployment includes one Control Center master host and three Control Center agent hosts. Fewer agent hosts is not supported, and additional agent hosts are rarely necessary.

A multi-host deployment requires five static IPv4 addresses:

- One for the Control Center master host.
- Three for the Control Center agents hosts, so that any two of the three hosts can participate in the ZooKeeper cluster.
- One for a virtual IP address, so that services which publish an IP address can run on any one of the three agent hosts. The virtual IP address must be on the same subnet as the other static addresses.

If you are converting a single-host deployment to a multi-host deployment, you need four additional static IP addresses in the same subnet as the Control Center master host.

Note To create a fresh multi-host deployment, perform the required procedures in all of the chapters in this part, in order. To convert a single-host deployment to a multi-host deployment, skip the first two chapters, and then perform the required procedures in the remaining chapters, in order.

When all of the installation procedures are completed, proceed to [Managing Cisco UCS Performance Manager with Control Center](#) on page 114.

4

Creating a Control Center master host

This chapter describes how to install a Cisco UCS Performance Manager virtual appliance as a Control Center master host, using either VMware vSphere or Microsoft Hyper-V.

Note If you plan to migrate data from a version 1.1.x system, please ensure that the version 1.1.x system and the version 2.0.x system can use a common datastore or datastore cluster.

Creating a virtual machine

You may create a virtual machine for the Cisco UCS Performance Manager appliance with VMware vSphere or Microsoft Hyper-V. Choose one of the procedures in this section.

Creating a virtual machine with vSphere

To perform this task, you need:

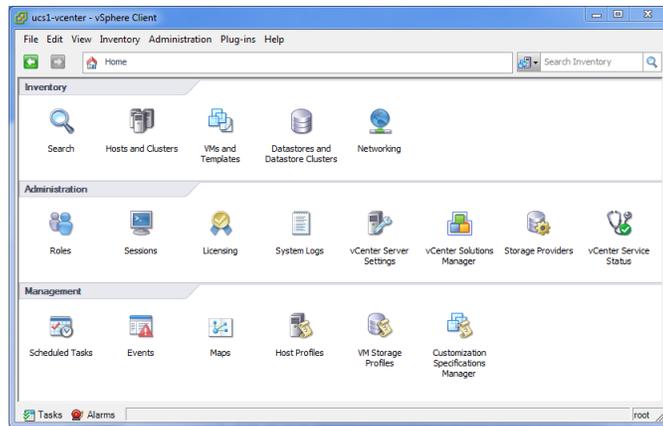
- A VMware vSphere client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

Use this procedure to install the Cisco UCS Performance Manager OVA package as a virtual machine managed by vSphere Server. The procedure includes steps to add a disk for backups.

The procedure is slightly different with different versions of VMware vSphere Client.

Note VMware vSphere Client 5.0.0 does not include a library that is needed to deploy compressed OVA files. You may uncompress the OVA package and then deploy it, or download and install *the missing library*. Cisco recommends installing the library.

- 1 Download the Cisco UCS Performance Manager OVA file from the *Cisco UCS Performance Manager* site to your workstation.
- 2 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home** view.

Figure 12: vSphere client Home view

- 3 From the **File** menu, select **Deploy OVF Template....**
- 4 In the **Source** panel, specify the path of the Cisco UCS Performance Manager package, and then click **Next >**.
- 5 In the **OVF Template Details** panel, click **Next >**.
- 6 In the **Name and Location** panel, provide a name and a location for the server.
 - a In the **Name** field, enter a new name or use the default.
 - b In the **Inventory Location** area, select a data center for the virtual machine.
 - c Click **Next >**.
- 7 In the **Host / Cluster** panel, select a host system, and then click **Next >**.
- 8 In the **Storage** panel, select a storage system with sufficient space for your UCS system, and then click **Next >**.
- 9 In the **Disk Format** panel, select **Thin Provision**, and then click **Next >**.
- 10 In the **Ready to Complete** panel, review the deployment settings, and then click **Finish**.
Please do not check the check box labeled **Power on after deployment**.
- 11 Navigate to the new virtual machine's **Getting Started** tab, and then click the **Edit virtual machine settings** link.
- 12 On the **Hardware** tab, click the **Add...** button.
- 13 In the **Add Hardware** dialog, select **Hard Disk**, and then click the **Next** button.
- 14 In the **Select a Disk** pane, click the **Create a new virtual disk** radio button, and then click the **Next** button.
- 15 In the **Create a Disk** pane, configure the virtual disk.
 - a In the **Capacity** area, set the disk size.
Cisco recommends 300GB.
 - b In the **Disk Provisioning** area, choose the option you prefer.
 - c In the **Location** area, choose the option you prefer.
 - d Click the **Next** button.
- 16 In the **Advanced Options** pane, configure the mode.
 - a In the **Mode** area, check the **Independent** check box.
 - b Click the **Persistent** radio button.
 - c Click the **Next** button.
- 17 In the **Ready to Complete** pane, confirm the virtual disk configuration, and then click the **Finish** button.
- 18 At the bottom of the **Virtual Machine Properties** dialog, click the **OK** button.
- 19 On the new virtual machine's **Getting Started** tab, click the **Power on virtual machine** link.

Creating a virtual machine with Hyper-V

To perform this task, you need:

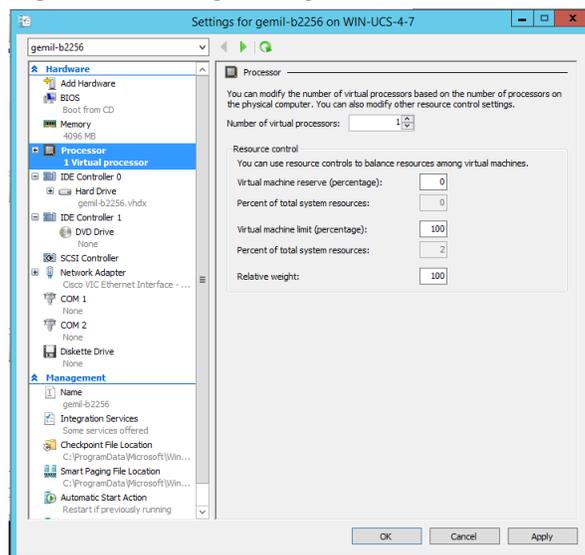
- A Microsoft Remote Desktop client

- Administrator privileges on a Microsoft Hyper-V server
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

Use this procedure to install the Cisco UCS Performance Manager appliance as a virtual machine managed by Microsoft Hyper-V.

- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Download the Cisco UCS Performance Manager ISO file from the [Cisco UCS Performance Manager](#) site to the Hyper-V host.
- 3 Start **Hyper-V Manager**.
- 4 In the left column, select a server to host the virtual machine.
- 5 From the **Action** menu, select **New > Virtual Machine....**
- 6 In the **New Virtual Machine Wizard** dialog, display the **Specify Name and Location** panel.
If the first panel displayed is the **Before You Begin** panel, click **Next**.
- 7 In the **Specify Name and Location** panel, provide a name for the virtual machine, and then click **Next**.
- 8 In the **Specify Generation** panel, select **Generation 1**, and then click **Next**.
- 9 In the **Assign Memory** panel, enter 65536 (64GB) in the **Startup memory** field, and then click **Next**.
- 10 In the **Configure Networking** panel, select **Cisco VIC Ethernet Interface - Virtual Switch**, and then click **Next**.
- 11 In the **Connect Virtual Hard Disk** panel, select **Create a virtual hard disk**, enter 300 in the **Size** field, and then click **Next**.
- 12 In the **Installation Options** panel, specify the Cisco UCS Performance Manager ISO package.
 - a Select **Install an operating system from a bootable CD/DVD-ROM**.
 - b Select **Image file (.iso)**, and then specify the location of the Cisco UCS Performance Manager ISO image file.
 - c Click **Next**.
- 13 In the **Summary** panel, review the virtual machine specification, and then click **Finish**.
Hyper-V Manager creates the new virtual machine, and then closes the **New Virtual Machine Wizard** dialog.
- 14 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Settings....**
- 15 In the **Hardware** area of the **Settings** dialog, select **Processor**.

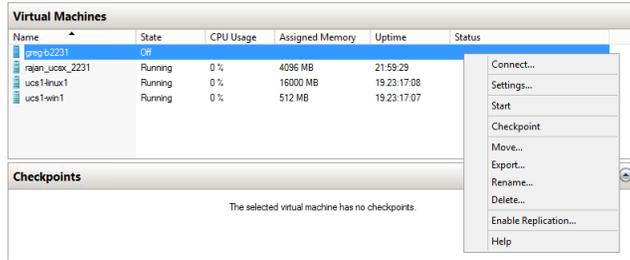
Figure 13: Settings dialog, Processor selected



- 16 In the **Processor** area, enter 8 in the **Number of virtual processors**, and then click **OK**.

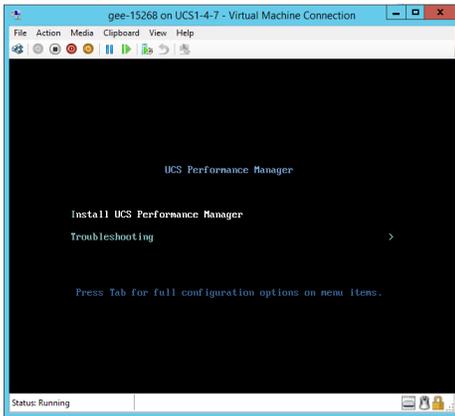
- 17 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Start**.

Figure 14: Starting a virtual machine



- 18 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Connect**.
- 19 In the **Virtual Machine Connection** window, press the **Enter** key.

Figure 15: Appliance installation start screen



The appliance installation process takes about 15 minutes, and should complete with no additional input.

Configuring the Control Center host mode

Perform this procedure immediately after creating and starting a Control Center host. All Control Center deployments must include one system configured as the master host.

- 1 Gain access to the console interface of the Control Center host through your hypervisor console interface.

Figure 16: Initial hypervisor console login prompt

```

YOU HAVE NOT CHOSEN A ROLE FOR THIS APPLIANCE.
PLEASE LOGIN TO CHOOSE ROLE AND ACTIVATE UCS Performance Manager

Welcome to UCS Performance Manager

After initial setup, the Control Center UI can be accessed by
browsing to:

  https://ucspm:50443
  (default username/password is ccuser/ucspm)

Ensure that ucspm is resolvable to 10.88.121.248, either through your
DNS system or through a HOSTS entry on the browser client. For more
information refer to the installation notes.

You can log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. The
root password defaults to 'ucspm'

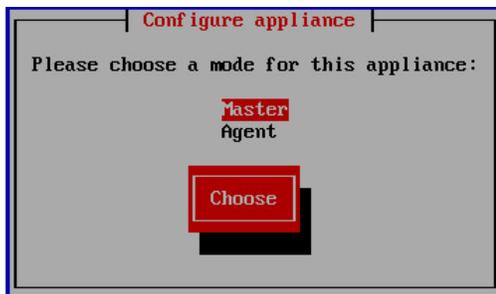
Linux Kernel 3.10.0-327.el7.x86_64 on an x86_64
ucspm login: _

```

- 2 Log in as the `root` user.
The initial password is `ucspm`.
- 3 The system prompts you to enter a new password for `root`.

Note Passwords must include a minimum of eight characters, with at least one character from three of the following character classes: uppercase letter, lowercase letter, digit, and special.

- 4 The system prompts you to enter a new password for `ccuser`.
The `ccuser` account is the default account for gaining access to the Control Center browser interface.
- 5 Select the master role for the host.



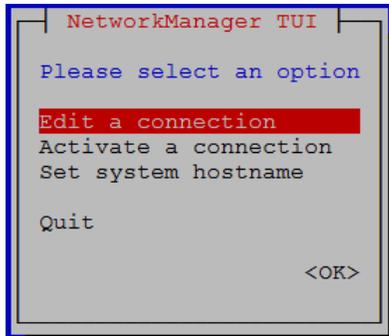
- a In the **Configure appliance** menu, press the **Tab** key to select the **Choose** button.
 - b Press the **Enter** key.
- The system reboots.

Edit a connection

The default configuration for network connections is DHCP. To configure static IPv4 addressing, perform this procedure.

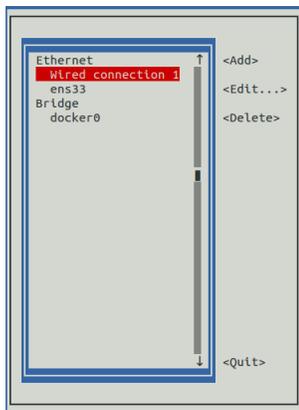
- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.
 - b Press the **Tab** key to select the **Run** button.

- c Press the **Enter** key.



- 4 On the **NetworkManager TUI** menu, select **Edit a connection**, and then press the **Return** key. The TUI displays the connections that are available on this host.

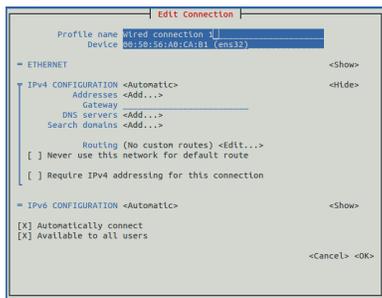
Figure 17: Example: Available connections



- 5 Use the down-arrow key to select **Wired Connection 1**, and then press the **Return** key.

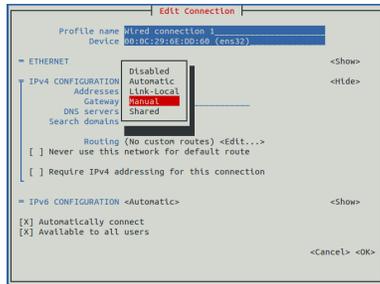
Note Do not use the TUI to edit the `docker0` connection. For more information, see [Configuring the Docker virtual bridge](#) on page 132.

Figure 18: Example: Edit Connection screen



Use the **Tab** key and the arrow keys to navigate among options in the **Edit Connection** screen, and use the **Return** key to toggle an option or to display a menu of options.

- 6 Optional: If the **IPv4 CONFIGURATION** area is not visible, select its display option (**<Show>**), and then press the **Return** key.
- 7 In the **IPv4 CONFIGURATION** area, select **<Automatic>**, and then press the **Return** key.

Figure 19: Example: IPv4 Configuration options

- 8 In the submenu, use the down-arrow key to select **Manual**, and then press the **Return** key.

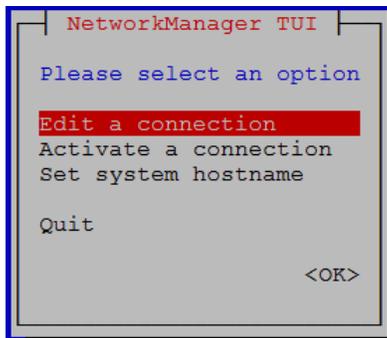
Note For static networking, the option next to **IPv4 CONFIGURATION** must be **Manual**. If it is **Automatic**, the host uses an address from a DHCP server.

- 9 Enter an IPv4 address in CIDR notation.
 - a Use the **Tab** key or the down arrow key to select the **<Add...>** option next to **Addresses**, and then press the **Return** key.
 - b In the **Addresses** field, enter an IPv4 address, followed by the solidus character (/) and then the prefix length.
For more information, see [CIDR prefix lengths for commonly-used netmasks](#) on page 133.
 - c Press the **Return** key.
- 10 Configure the **Gateway** and **DNS servers** fields with IPv4 addresses.
- 11 Use the **Tab** key or the down arrow key to select the **<OK>** option at the bottom of the **Edit Connection** screen, and then press the **Return** key.
- 12 In the available connections screen, use the **Tab** key to select the **<Quit>** option, and then press the **Return** key.
- 13 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

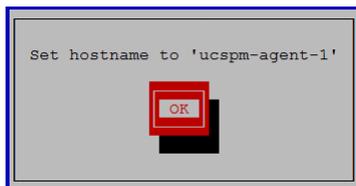
Set system hostname

The default hostname of a Control Center host is `ucspm`. To change the hostname, perform this procedure.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.
 - b Press the **Tab** key to select the **Run** button.
 - c Press the **Enter** key.



- 4 Display the hostname entry field.
 - a In the **NetworkManager TUI** menu, use the down-arrow key to select **Set system hostname**.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.
- 5 In the **Hostname** field, enter the new hostname.
You may enter either a hostname or a fully-qualified domain name.
- 6 Press the **Tab** key twice to select the **OK** button, and then press the **Enter** key.



- 7 In the confirmation dialog, press the **Return** key.
- 8 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

Adding a disk for backups to Hyper-V guest systems

This procedure is not necessary on VMware vSphere guest systems, only Microsoft Hyper-V guest systems. Perform this procedure to add disk storage for backups.

To perform this procedure, you must be logged in to the Hyper-V host of the Cisco UCS Performance Manager guest system as Administrator, or as a user with Administrator privileges.

- 1 In the left column, select the server that is hosting the Cisco UCS Performance Manager guest system, and then right-click to select **New > Hard Disk...**
- 2 In the **New Virtual Hard Disk Wizard** dialog, navigate to the **Choose Disk Format** panel.
- 3 Click the **VHDX** radio button, and then click the **Next** button.
- 4 In the **Choose Disk Type** panel, click the **Dynamically expanding** radio button, and then click the **Next** button.
- 5 In the **Specify Name and Location** panel, enter a name for the disk in the **Name** field, and then click the **Next** button.
- 6 In the **Configure Disk** panel, click the **Create a new blank virtual hard disk** radio button, enter the disk size in the **Size** field, and then click the **Next** button.
Cisco recommends 300GB.
- 7 In the **Summary** panel, review the virtual disk settings, and then click the **Finish** button.

- 8 In **Hyper-V Manager**, right-click the virtual machine of the Control Center master host, and then select **Settings...**
- 9 In the **Settings** dialog, select **SCSI Controller** from the **Hardware** list in the left column.
- 10 In the **SCSI Controller** area on the right side, select **Hard Drive**, and then click the **Add** button.
- 11 In the **Hard Drive** area, click the **Virtual hard disk** radio button, and then click the **Browse** button.
- 12 In the **Open** dialog, select the hard disk image created previously, and then click the **Open** button.
- 13 In the **Settings** dialog, click the **OK** button.

Preparing a disk for backups

Use this procedure to format the second disk for Control Center backups, and mount it in the master host filesystem.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Verify the status of the disk to format.

The disk is mounted as `/dev/sdb`. Best practice: Always verify a device or partition before formatting it, which destroys all data on a device.

```
lsblk -p --output=NAME,SIZE,TYPE,MOUNTPOINT /dev/sdb
```

Example output:

```
NAME          SIZE TYPE MOUNTPOINT
/dev/sdb      300G disk
```

- 4 Create and label an XFS file system.

```
mkfs -t xfs -L BACKUPS /dev/sdb
```

- 5 Set the permissions bits of the filesystem mount point.

```
chmod 777 /opt/serviced/var/backups
```

- 6 Create an entry in the `/etc/fstab` file.

```
echo "/dev/sdb /opt/serviced/var/backups xfs defaults 0 0" \
  >> /etc/fstab
```

- 7 Mount the file system, and then verify it mounted correctly.

```
mount -a && mount | grep backups
```

Example result:

```
/dev/sdb1 on /opt/serviced/var/backups type xfs
(rw,relatime,attr2,inode64,noquota)
```

Deploying Cisco UCS Performance Manager

Perform this procedure on logging in to Control Center for the first time.

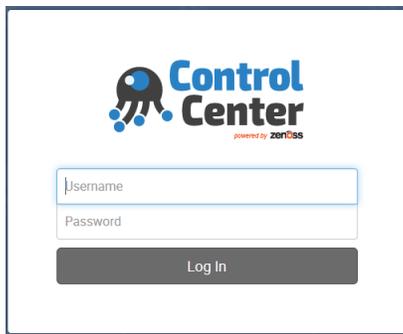
- 1 Display the login page of the Control Center browser interface.
Replace *IP-Address* with the IP address of the Control Center virtual machine:

```
https://IP-Address:50443
```

You can use the hostname of the Control Center virtual machine instead of its IP address, if name resolution of the hostname is configured in your environment.

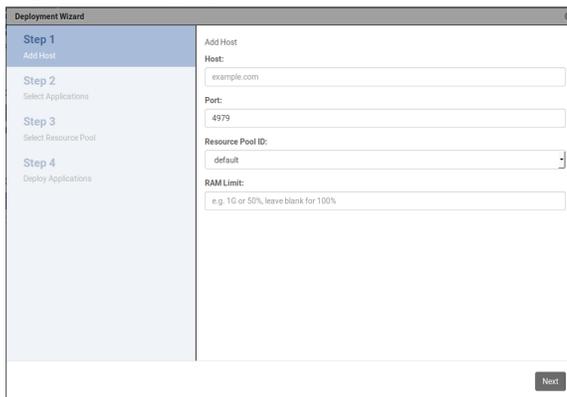
Note The web server that listens for Control Center interface requests typically takes 1-2 minutes to start after the the Control Center master host is started.

Figure 20: Control Center login page



- 2 At the login page, enter `ccuser` and its password.

Figure 21: Deployment Wizard



If the Deployment Wizard does not display automatically, then click **+ Application**, located at the right side of the page.

- 3 In the **Deployment Wizard**, add the master host to the `default` resource pool.

The host to add is the Control Center master host.

- a In the **Host** field, enter the hostname or IP address of the Control Center master host.

If you enter a hostname, all hosts in your Control Center cluster must be able to resolve the name, either through an entry in `/etc/hosts`, or through a nameserver on your network.

- b Skip the **Port** field.

This field specifies the port for remote procedure calls; the correct value is 4979.

- c In the **Resource Pool ID** field, select `default` from the list.
 - d In the **RAM Limit** field, enter the amount of non-system RAM to allocate to Control Center and Cisco UCS Performance Manager.
The amount may be specified as an absolute value or as a percentage:
 - To specify an absolute amount of non-system RAM, enter a number followed by M for megabytes, G for gigabytes, or T for terabytes. For example, 65536M, 64G, and 0.0625T are equivalent values.
 - To specify a percentage of non-system RAM, enter a number between 0 and 100 followed by the percent sign (%) character.

If you do not specify a value, the amount of non-system RAM allocated to Control Center and Cisco UCS Performance Manager is 100%.
 - e At the bottom of the **Deployment Wizard**, click **Next**.
- 4 Select the application to deploy.
 - a Select `ucspm`.
 - b At the bottom of the **Deployment Wizard**, click **Next**.
 - 5 Select the resource pool for the application.
 - a Select `default`.
 - b At the bottom of the **Deployment Wizard**, click **Next**.
 - 6 Choose a deployment ID and deploy Cisco UCS Performance Manager.
 - a In the **Deployment ID** field, enter a name for this deployment of Cisco UCS Performance Manager.
 - b At the bottom of the **Deployment Wizard**, click **Deploy**.

Figure 22: Cisco UCS Performance Manager is deployed

The screenshot shows the Control Center interface with the 'Applications' tab selected. The 'Applications' table lists two items: 'Internal Services' and 'ucspm (v2.0.1)'. The 'ucspm (v2.0.1)' application is shown with a status of 'Test', a deployment ID of 'Test', and a resource pool of 'default'. The public endpoints are listed as 'https://ucspm-cc-master-50443' and 'https://cc-master'. The 'Actions' column for this application includes 'Start', 'Stop', and 'Delete' buttons. Below the table, the 'Application Templates' section shows a single template for 'ucspm (v2.0.1)' with ID '59f1337508ecf73bd27c2283694f2ce5' and description 'Cisco UCS Performance Manager'.

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	✓	Internal	N/A	N/A	N/A
ucspm (v2.0.1)	Cisco UCS Performance Manager	⊖	Test	default	https://ucspm-cc-master-50443 https://cc-master	▶ Start ■ Stop ○ Delete

Application Template	ID	Description	Actions
ucspm (v2.0.1)	59f1337508ecf73bd27c2283694f2ce5	Cisco UCS Performance Manager	○ Delete

- 7 At the top of the page, click **Logout**.
The control is located at the right side of the page.

Note Do not start Cisco UCS Performance Manager at this time.

If you plan to migrate data from a Cisco UCS Performance Manager version 1.1.x system, do not perform any other tasks in this guide at this time. Instead, refer to the *Cisco UCS Performance Manager Migration Guide*.

Otherwise, proceed to the next chapter.

5

Enabling access to browser interfaces

Control Center and Cisco UCS Performance Manager have independent browser interfaces served by independent web servers. Both web servers are configured to use SSL/TLS communications.

The Control Center web server listens at the hostname of the Control Center master host and port 50443. For a Control Center master host with the fully-qualified domain name (FQDN) `cc-master.example.com`, the hostname URL is `https://cc-master:50443`. As always, you may substitute an IP address for the hostname portion of the URL.

The Cisco UCS Performance Manager web server listens at a *port public endpoint* and a *virtual host public endpoint*.

- The default *port public endpoint* is the hostname of the Control Center master host and port 443. For the FQDN `cc-master.example.com`, the URL of the default port public endpoint is `https://cc-master`. If the Control Center master host has more than one network interface, you can configure additional port public endpoints with different hostnames. Also, you can disable SSL/TLS communications for a port public endpoint, if desired.

To use a port public endpoint to gain access to the Cisco UCS Performance Manager browser interface, no additional network name resolution entries are required. The default entries for the network interface(s) of the Control Center master host are sufficient.

- The default *virtual host public endpoint* is the text `ucspm` prepended to the hostname of the Control Center master host and port 50443. For the FQDN `cc-master.example.com`, the URL of the default virtual host public endpoint is `https://ucspm.cc-master:50443`. You can change the name of the default virtual host and configure additional virtual host public endpoints, if desired.

To use a virtual host public endpoint to gain access to the Cisco UCS Performance Manager browser interface, you must add name resolution entries for the virtual host to the DNS servers in your environment or to the hosts files of individual client systems.

The following sections provide additional information about public endpoints, and instructions for creating public endpoints and for configuring virtual host name resolution.

Creating public endpoints

This section describes how to create a port public endpoint and a virtual host public endpoint. The following table outlines the process for each.

Port public endpoint	Virtual host public endpoint
1 Create the endpoint	1 Create the endpoint

Port public endpoint	Virtual host public endpoint
2 Configure the Zope service	2 Configure the Zope service
	3 Configure virtual host name resolution

To change an existing public endpoint, create a new endpoint and then delete the existing endpoint.

Note Virtual host public endpoints must use SSL/TLS communications. Port public endpoints can communicate with or without SSL/TLS.

Creating a port public endpoint

Use this procedure to create a new port public endpoint. Port public endpoints can communicate with or without SSL/TLS.

- 1 Log in to the Control Center browser interface.

The screenshot shows the Control Center interface. The top navigation bar includes 'Applications', 'Resource Pools', 'Hosts', 'Logs', and 'Backup / Restore'. The main content area is titled 'Applications' and contains a table with the following data:

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	✓	Internal	N/A	N/A	N/A
ucspm (v2.0.1)	Cisco UCS Performance Manager	⊖	Test	default	https://ucspm.cc-master:50443 https://cc-master	▶ Start ⊞ Stop ○ Delete

Below the Applications table, there is a section for 'Application Templates' with a table showing the 'ucspm (v2.0.1)' template:

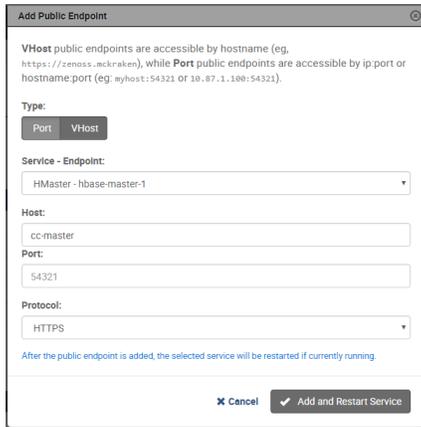
Application Template	ID	Description	Actions
ucspm (v2.0.1)	59f1337508ecf73bd27c2283694f2ce5	Cisco UCS Performance Manager	○ Delete

- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).

The screenshot shows the Control Center interface for the 'ucspm (v2.0.1)' application. The main content area is titled 'ucspm (v2.0.1)' and contains a table with the following data:

Service	Endpoint	Type	Protocol	URL	Actions
IMaster	hbase-master-info-1	vhost	https	https://hbase.cc-master:50443	▶ Start ⊞ Stop ○ Delete
reader	opentsdb-reader	vhost	https	https://opentsdb.cc-master:50443	▶ Start ⊞ Stop ○ Delete
RabbitMQ	rabbitmq_admin	vhost	https	https://rabbitmq.cc-master:50443	▶ Start ⊞ Stop ○ Delete
ucspm	zproxy	vhost	https	https://ucspm.cc-master:50443	▶ Start ⊞ Stop ○ Delete
ucspm	zproxy	port	https	https://cc-master	▶ Start ⊞ Stop ○ Delete

- 3 Click **+ Add Public Endpoint**, located above the **Public Endpoints** table, on the right side.



The default view of the **Add Public Endpoint** dialog displays the fields for creating a port public endpoint.

4 Define a new port public endpoint.

- a In the **Type** area, click **Port**.
- b From the **Service - Endpoint** list, select **ucspm - zproxy**.

The selection is the last entry in the list.

- c In the **Host** field, enter a hostname or IP address that is assigned to a network interface on the Control Center master host.

The default value is the hostname that was added with the Deployment Wizard when Cisco UCS Performance Manager was initially deployed. If the Control Center master host has more than one network interface, you may add the hostname or IP address assigned to one of the other interfaces.

- d In the **Port** field, enter a safe, unused port number greater than or equal to 1024 and less than or equal to 65535.

For a list of ports considered unsafe, see [Unsafe ports on Chrome](#). For the list of ports used by the Control Center master host, see [Security considerations](#) on page 131.

- e In the **Protocol** field, select **HTTPS** or **HTTP**.

You can set up a secure proxy server to handle HTTP requests sent to a port public endpoint, if desired.

- f Click **Add and Restart Service**.

Configure the **Zope** service to use the new port public endpoint. Choose one of the configuration options in the following table.

Zope configuration	Procedure
HTTPS and the default secure proxy server	Configuring Zope for HTTPS and the default secure proxy server on page 25
HTTP and no proxy server	Configuring Zope for HTTP and no proxy server on page 27
HTTP and a secure proxy server other than the default	Configuring Zope for HTTP and a secure proxy server on page 28

Note When you configure Zope for HTTP protocol and no proxy server, you can only gain access to the Cisco UCS Performance Manager browser interface through port public endpoints configured for HTTP. Virtual host public endpoints must use HTTPS protocol, so any existing virtual host public endpoints stop working.

Configuring Zope for HTTPS and the default secure proxy server

Before performing this procedure, create a port public endpoint or a virtual host public endpoint to use the HTTPS protocol.

Use this procedure to configure the **Zope** service for SSL/TLS communications and the secure proxy server that is included in Cisco UCS Performance Manager.

- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.

The Control Center browser interface displays the details page of the **Zope** service.

- 4 Scroll to the top of the **Zope** service details page.

The screenshot shows the Control Center interface for the Zope service. At the top, there are navigation tabs for Applications, Resource Pools, Hosts, Logs, Backup/Restore, and user information. Below the navigation, the Zope service name is displayed with control buttons for Edit Service, Edit Variables, Start, Stop, and Restart. There are three main sections: Public Endpoints (No Data Found), IP Assignments (No Data Found), and Configuration Files. The Configuration Files table lists two files: /opt/zenoss/etc/global.conf and /opt/zenoss/etc/zope.conf, each with an Edit button.

- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the **/opt/zenoss/etc/zope.conf** file.

```

1 # This is the proposed version for SC / Zope 2.12.1
2
3 #####
4 # Welcome to Zope 2.
5 #####
6 #
7 # This is the Zope configuration file. The Zope configuration file
8 # shows what the default configuration directives are, and show
9 # examples for each directive. To declare a directive, make sure that
10 # you add it to a line that does not begin with "#". Note that comments
11 # are only allowed at the beginning of a line; you may not add comments
12 # after directive text on the same line.
13 #
14 # Note for Developers
15 # =====
16 #
17 # This file is "not" auto-generated. If you create a new directive you
18 # very likely want to include an example of how to use the new
19 # directive in this file.
20 #
21 # You shouldn't modify 'zope.conf.in' to change
22 # configuration. Instead, you should make a copy into 'zope.conf' and
23 # modify that to avoid checking in changes to this file by mistake.
24 #
25 # Zconfig "defines" used for later textual substitution
26 #
27 #define INSTANCE /opt/zenoss
28 #
29 # this needs to match the encoding in the sitecustomize.py file
30 # in $ZENHOME/lib/python
31 # default-publisher-encoding utf-8
32 #
33 # directive: instancehome
34 #
35 # Description: ...

```

- 6 Configure Zope for secure communications with the proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the **cgi-environment** directive.

The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for SSL/TLS communications:

```

<cgi-environment>
  HTTPS ON
</cgi-environment>

```

- 7 Configure the Beaker add-on product to use secure communications.
 - a In the **Edit Configuration** dialog, scroll down to the **product-config** directive.

The directive is at the bottom the file, on or near line 1122.

- b Set the value of the `session.secure` key to `True`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

Next steps:

- If you created a port public endpoint before performing this procedure, the endpoint is ready to use.
- If you created a virtual host public endpoint before performing this procedure, proceed to [Configuring name resolution for virtual hosts](#) on page 32.

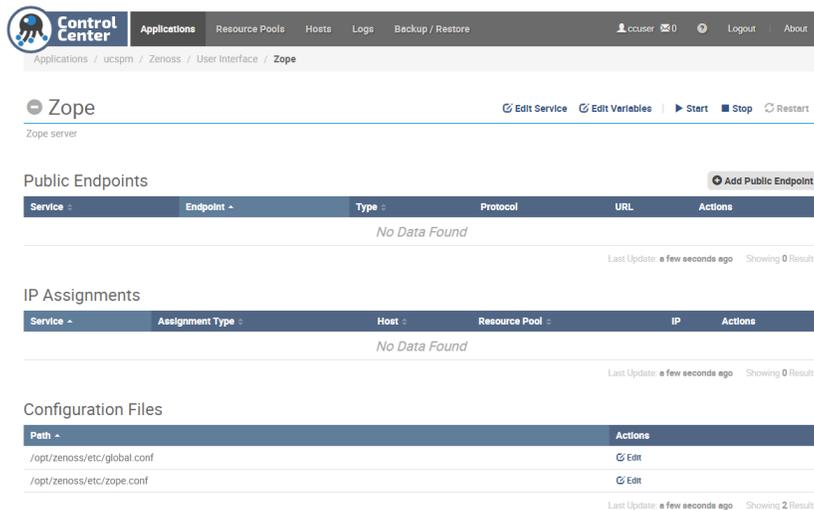
Configuring Zope for HTTP and no proxy server

Before performing this procedure, create a port public endpoint to use the HTTP protocol. For more information, see [Creating a port public endpoint](#) on page 24.

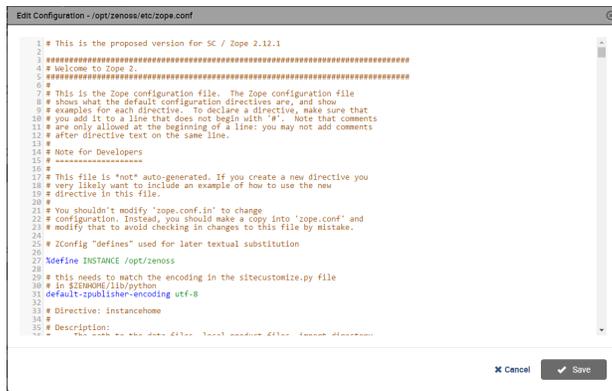
Use this procedure to configure the **Zope** service for insecure communications with Cisco UCS Performance Manager browser interface clients.

Note When you configure Zope for insecure communications, any existing virtual host public endpoints stop working.

- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.
The Control Center browser interface displays the details page of the **Zope** service.
- 4 Scroll to the top of the **Zope** service details page.



- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the `/opt/zenoss/etc/zope.conf` file.



- 6 Configure Zope for insecure communications with the proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the `cgi-environment` directive.
The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for insecure communications:

```
<cgi-environment>
  HTTPS OFF
</cgi-environment>
```

- 7 Configure the Beaker add-on product to use insecure communications.
 - a In the **Edit Configuration** dialog, scroll down to the `product-config` directive.
The directive is at the bottom the file, on or near line 1122.
 - b Set the value of the `session.secure` key to `False`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

Configuring Zope for HTTP and a secure proxy server

Before performing this procedure, create a port public endpoint to use the HTTP protocol. For more information, see [Creating a port public endpoint](#) on page 24.

Use this procedure to configure the **Zope** service for SSL/TLS communications and a secure proxy server that is available on your network.

- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.
The Control Center browser interface displays the details page of the **Zope** service.
- 4 Scroll to the top of the **Zope** service details page.

The screenshot shows the Control Center interface for the Zope server. At the top, there are navigation tabs for Applications, Resource Pools, Hosts, Logs, and Backup / Restore. The main content area is titled 'Zope' and includes a status bar with 'Edit Service', 'Edit Variables', 'Start', 'Stop', and 'Restart' buttons. Below this are three tables: 'Public Endpoints', 'IP Assignments', and 'Configuration Files'. The 'Configuration Files' table has two entries, both with an 'Edit' button in the 'Actions' column.

- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the `/opt/zenoss/etc/zope.conf` file.

The screenshot shows the 'Edit Configuration' dialog for the file `/opt/zenoss/etc/zope.conf`. The dialog contains a text area with the following content:

```

1 # This is the proposed version for SC / Zope 2.12.1
2
3 #####
4 # Welcome to Zope 2.
5 #####
6
7 # This is the Zope configuration file. The Zope configuration file
8 # shows what the default configuration directives are, and show
9 # examples for each directive. To declare a directive, make sure that
10 # you add it to a line that does not begin with "#". Note that comments
11 # are only allowed at the beginning of a line; you may not add comments
12 # after directive text on the same line.
13 #
14 # Note for Developers
15 #
16 #
17 # This file is "not" auto-generated. If you create a new directive you
18 # very likely want to include an example of how to use the new
19 # directive in this file.
20 #
21 # You shouldn't modify 'zope.conf.in' to change
22 # configuration. Instead, you should make a copy into 'zope.conf' and
23 # modify that to avoid checking in changes to this file by mistake.
24 #
25 # Zconfig "defines" used for later textual substitution
26 #
27 # Define INSTANCE /opt/zenoss
28 #
29 # this needs to match the encoding in the sitecustomize.py file
30 # in $ZENHOME/lib/python
31 # default-publisher-encoding utf-8
32 #
33 # Directive: instancehome
34 #
35 # Description: ...

```

- 6 Configure Zope for secure communications with your proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the `cgi-environment` directive. The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for SSL/TLS communications:

```

<cgi-environment>
  HTTPS ON
</cgi-environment>

```

- 7 Configure the Beaker add-on product to use secure communications.
 - a In the **Edit Configuration** dialog, scroll down to the `product-config` directive. The directive is at the bottom the file, on or near line 1122.
 - b Set the value of the `session.secure` key to `True`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

Creating a virtual host public endpoint

Use this procedure to create a new virtual host public endpoint. Virtual host public endpoints must use SSL/TLS communications.

- 1 Log in to the Control Center browser interface.

The screenshot shows the Control Center interface. At the top, there's a navigation bar with 'Applications' selected. Below it, there's a table of applications. The 'ucspm (v2.0.1)' application is highlighted. Below the applications table, there's a table of application templates, also showing 'ucspm (v2.0.1)'.

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	✔	Internal	N/A	N/A	N/A
ucspm (v2.0.1)	Cisco UCS Performance Manager	⊖	Test	default	https://ucspm.cc-master:50443 https://cc-master	▶ Start ■ Stop ○ Delete

Application Template	ID	Description	Actions
ucspm (v2.0.1)	59f11337508ecf73bd27c2283694f2ce5	Cisco UCS Performance Manager	○ Delete

- In the **Application** column of the **Applications** table, click the application name (**ucspm**).

The screenshot shows the details page for the 'ucspm (v2.0.1)' application. Below the application name, there's a 'Public Endpoints' table. The '+ Add Public Endpoint' button is highlighted in the top right corner of the table.

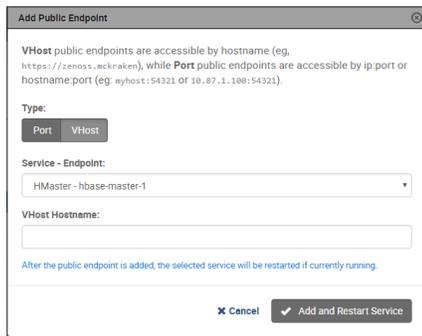
Service	Endpoint	Type	Protocol	URL	Actions
hMaster	hbase-master-1	vhost	https	https://hbase.cc-master:50443	▶ Start ■ Stop ○ Delete
reader	opentdb-reader	vhost	https	https://opentdb.cc-master:50443	▶ Start ■ Stop ○ Delete
rabbitMQ	rabbitmq_admin	vhost	https	https://rabbitmq.cc-master:50443	▶ Start ■ Stop ○ Delete
ucspm	zproxy	vhost	https	https://ucspm.cc-master:50443	▶ Start ■ Stop ○ Delete
ucspm	zproxy	port	https	https://cc-master	▶ Start ■ Stop ○ Delete

- Click **+ Add Public Endpoint**, located above the **Public Endpoints** table, on the right side.

The screenshot shows the 'Add Public Endpoint' dialog box. It has a title bar and a close button. The main content area contains a text block explaining VHost and Port endpoints. Below that, there are radio buttons for 'Port' and 'VHost', with 'VHost' selected. There are also several input fields: 'Service - Endpoint' (a dropdown menu), 'Host', 'Port', and 'Protocol' (a dropdown menu). At the bottom, there are 'Cancel' and 'Add and Restart Service' buttons.

The default view of the **Add Public Endpoint** dialog displays the fields for creating a port public endpoint.

- Define a new virtual host public endpoint.
 - In the **Type** area, click **VHost**.



b From the **Service - Endpoint** list, select **ucspm - zproxy**.

The selection is the last entry in the list.

c In the **VHost Hostname** field, enter a virtual hostname.

The following strings of text are valid in this field:

- A fully-qualified domain name (FQDN). Any string of text that includes one or more full stop characters (.) is treated as an FQDN.
- A string of text that contains only letters and one or more hyphen characters (-). The string is prepended to the hostname of the Control Center master host, with a full stop character (.) separating the string and the hostname.

d Click **Add and Restart Service**.

Configuring Zope for HTTPS and the default secure proxy server

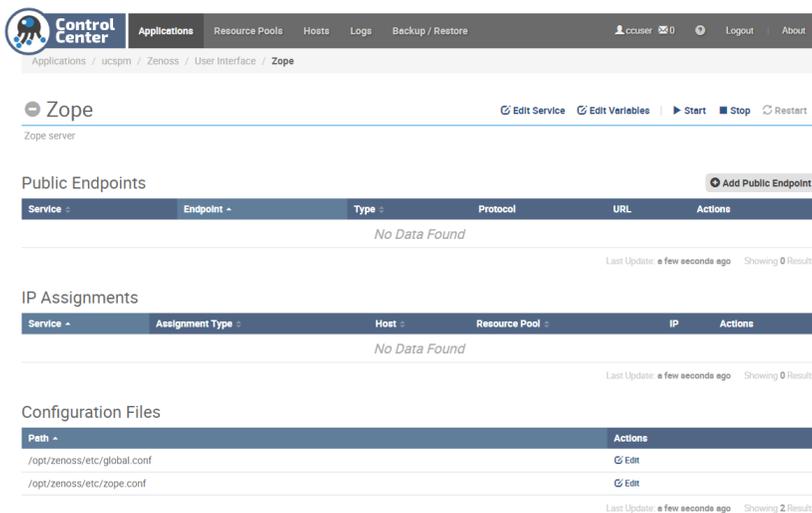
Before performing this procedure, create a port public endpoint or a virtual host public endpoint to use the HTTPS protocol.

Use this procedure to configure the **Zope** service for SSL/TLS communications and the secure proxy server that is included in Cisco UCS Performance Manager.

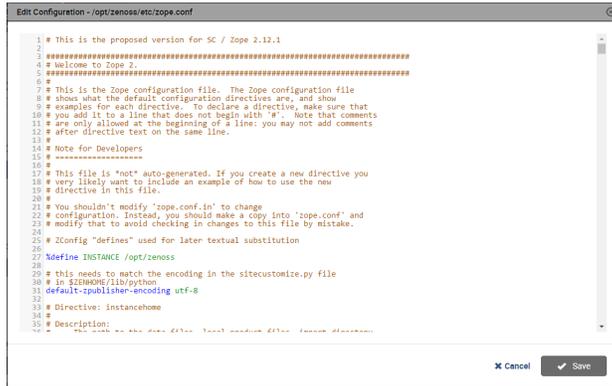
- 1 Log in to the Control Center browser interface.
- 2 In the **Application** column of the **Applications** table, click the application name (**ucspm**).
- 3 Scroll down to the bottom of the **Services** table, and then click **Zope**.

The Control Center browser interface displays the details page of the **Zope** service.

4 Scroll to the top of the **Zope** service details page.



- 5 In the **Actions** column of the **Configuration Files** table, click the **Edit** control of the `/opt/zenoss/etc/zope.conf` file.



- 6 Configure Zope for secure communications with the proxy server.
 - a In the **Edit Configuration** dialog, scroll down to the `cgi-environment` directive.

The directive is about one-third of the way down from the top of the file, on or near line 380.
 - b Configure the proxy server for SSL/TLS communications:

```
<cgi-environment>
  HTTPS ON
</cgi-environment>
```

- 7 Configure the Beaker add-on product to use secure communications.
 - a In the **Edit Configuration** dialog, scroll down to the `product-config` directive.

The directive is at the bottom the file, on or near line 1122.
 - b Set the value of the `session.secure` key to `True`.
- 8 At the bottom of the **Edit Configuration** dialog, click **Save**.

Next steps:

- If you created a port public endpoint before performing this procedure, the endpoint is ready to use.
- If you created a virtual host public endpoint before performing this procedure, proceed to [Configuring name resolution for virtual hosts](#) on page 32.

Configuring name resolution for virtual hosts

To enable access to browser interfaces by virtual hosts, add name resolution entries to the DNS servers in your environment or to the hosts files of individual client systems.

- On Windows client systems, the hosts file is `C:\Windows\System32\drivers\etc\hosts`.
- Linux and OS/X client systems, the hosts file is `/etc/hosts`.

Name resolution syntax

The following line shows the syntax of the entry to add to a name resolution file:

```
IP-Address FQDN Hostname ucspm.Hostname
```

For example, the following entry identifies a Control Center master host at IP address 192.0.2.12, hostname `cc-master`, in the `example.com` domain.

```
192.0.2.12 cc-master.example.com cc-master ucspm.cc-master
```

Configuring name resolution on a Windows 7 system

To perform this procedure, you need Windows Administrator privileges.

- 1 Log in to the Windows 7 system as a user with Administrator privileges.
- 2 From the **Start** menu, highlight **All Programs > Accessories > Notepad**.
- 3 Right click, and then select **Run as administrator**.
- 4 From the Notepad **File** menu, select **Open**.
- 5 In the **File name** field of the **Open** window, enter `C:\Windows\System32\drivers\etc\hosts`.
- 6 Add a name resolution entry to the end of the file.
For more information, see [Name resolution syntax](#) on page 32.
- 7 Save the file, and then exit Notepad.

Configuring name resolution on a Linux or OS/X system

To perform this procedure, you need superuser privileges on the client system.

- 1 Log in to the client system as `root` or as a user with `sudo` privileges.
- 2 Open the `/etc/hosts` file in a text editor.
- 3 Add a name resolution entry to the end of the file.
For more information, see [Name resolution syntax](#) on page 32.
- 4 Save the file, and then close the editor.

6

Creating Control Center agent hosts

This chapter describes how to install a Cisco UCS Performance Manager virtual appliance as a Control Center agent host, using either VMware vSphere or Microsoft Hyper-V. Repeat the procedures in this chapter three times to create three agent hosts.

Creating a virtual machine

You may create a virtual machine for the Cisco UCS Performance Manager appliance with VMware vSphere or Microsoft Hyper-V. Choose one of the procedures in this section.

Creating a virtual machine with vSphere

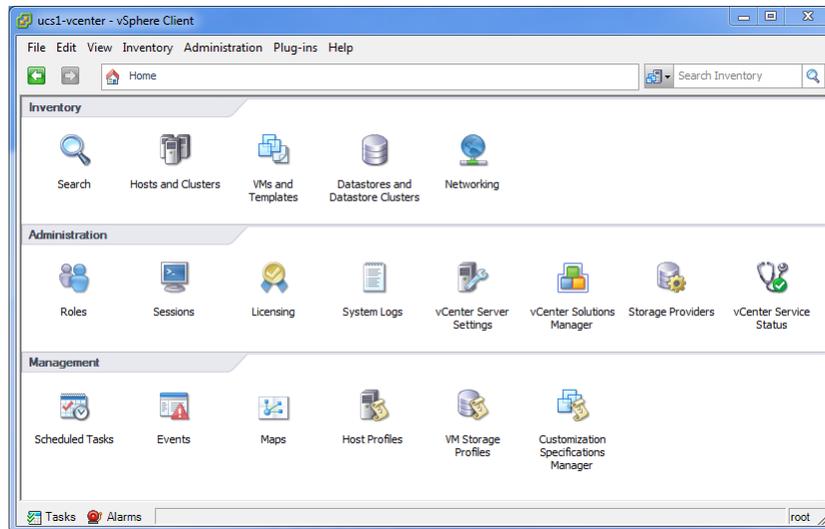
To perform this task, you need a VMware vSphere client.

This procedure installs the Cisco UCS Performance Manager OVA package as a virtual machine managed by vSphere Server version 5.0.0, using VMware vSphere Client 5.0.0. The procedure is slightly different with different versions of VMware vSphere Client.

- 1 Download the Cisco UCS Performance Manager OVA file from the [Cisco UCS Performance Manager](#) site to your workstation, if necessary.

Note The same OVA package is used for both master host and agent host virtual machines.

- 2 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home** view.

Figure 23: vSphere client Home view

- 3 From the **File** menu, select **Deploy OVF Template....**
- 4 In the **Source** panel, specify the path of the Cisco UCS Performance Manager package, and then click **Next >**.
- 5 In the **OVF Template Details** panel, click **Next >**.
- 6 In the **Name and Location** panel, provide a name and a location for the server.
 - a In the **Name** field, enter a new name.
 - b In the **Inventory Location** area, select a data center for the virtual machine.
 - c Click **Next >**.
- 7 In the **Host / Cluster** panel, select a host system, and then click **Next >**.
- 8 In the **Storage** panel, select a storage system with sufficient space for your UCS system, and then click **Next >**.
- 9 In the **Disk Format** panel, select **Thin Provision**, and then click **Next >**.
- 10 In the **Ready to Complete** panel, review the deployment settings, and then click **Finish**.
You may check the check box labeled **Power on after deployment**, if desired.
- 11 Optional: On the new virtual machine's **Getting Started** tab, click the **Power on virtual machine** link, if necessary.

Creating a virtual machine with Hyper-V

To perform this task, you need:

- A Microsoft Remote Desktop client
- Administrator privileges on a Microsoft Hyper-V server

This procedure installs the Cisco UCS Performance Manager appliance as a virtual machine managed by Microsoft Hyper-V.

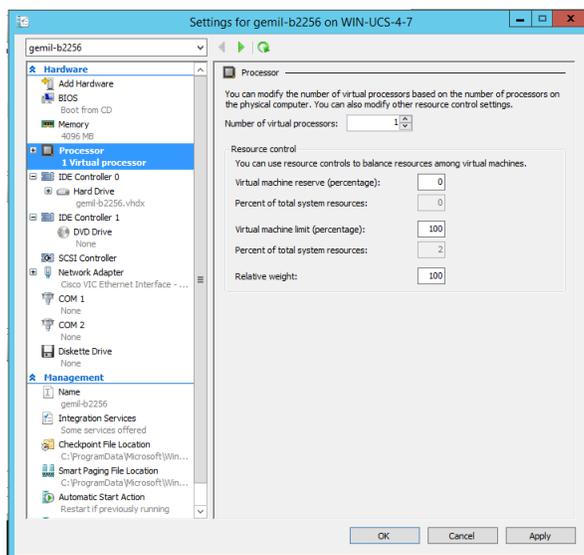
- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Download the Cisco UCS Performance Manager ISO file from the [Cisco UCS Performance Manager](#) site to the Hyper-V host, if necessary.

Note The same OVA package is used for both master host and agent host virtual machines.

- 3 Start **Hyper-V Manager**.
- 4 In the left column, select a server to host the virtual machine.
- 5 From the **Action** menu, select **New > Virtual Machine....**

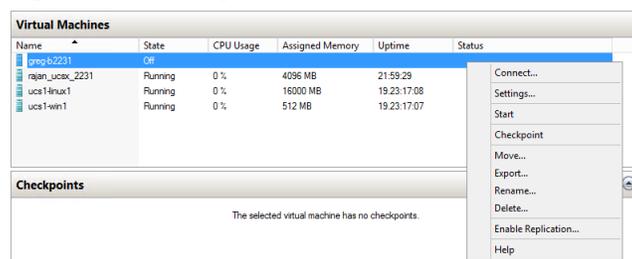
- 6 In the **New Virtual Machine Wizard** dialog, display the **Specify Name and Location** panel.
If the first panel displayed is the **Before You Begin** panel, click **Next >**.
- 7 In the **Specify Name and Location** panel, provide a name for the virtual machine, and then click **Next >**.
- 8 In the **Specify Generation** panel, select **Generation 1**, and then click **Next >**.
- 9 In the **Assign Memory** panel, enter 40960 (40GB) in the **Startup memory** field, and then click **Next >**.
- 10 In the **Configure Networking** panel, select **Cisco VIC Ethernet Interface - Virtual Switch**, and then click **Next >**.
- 11 In the **Connect Virtual Hard Disk** panel, select **Create a virtual hard disk**, enter 140 in the **Size** field, and then click **Next >**.
- 12 In the **Installation Options** panel, specify the Cisco UCS Performance Manager ISO package.
 - a Select **Install an operating system from a bootable CD/DVD-ROM**.
 - b Select **Image file (.iso)**, and then specify the location of the Cisco UCS Performance Manager ISO image file.
 - c Click **Next >**.
- 13 In the **Summary** panel, review the virtual machine specification, and then click **Finish**.
Hyper-V Manager creates the new virtual machine, and then closes the **New Virtual Machine Wizard** dialog.
- 14 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Settings...**
- 15 In the **Hardware** area of the **Settings** dialog, select **Processor**.

Figure 24: Settings dialog, Processor selected



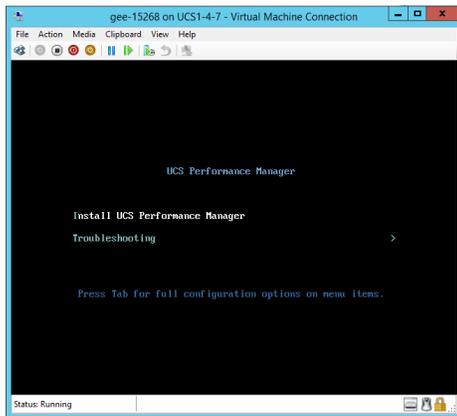
- 16 In the **Processor** area, enter 8 in the **Number of virtual processors** field, and then click **OK**.
- 17 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Start**.

Figure 25: Starting a virtual machine



- 18 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Connect**.
- 19 In the **Virtual Machine Connection** window, press the **Enter** key.

Figure 26: Appliance installation start screen



The appliance installation process takes about 15 minutes, and should complete with no additional input.

Configuring the virtual machine mode

Perform this procedure immediately after creating and starting a virtual machine for Cisco UCS Performance Manager. A Cisco UCS Performance Manager deployment may include three systems configured as agent hosts.

- 1 Gain access to the console interface of the Control Center host through your hypervisor console interface.

Figure 27: Initial hypervisor console login prompt

```

YOU HAVE NOT CHOSEN A ROLE FOR THIS APPLIANCE.
PLEASE LOGIN TO CHOOSE ROLE AND ACTIVATE UCS Performance Manager

Welcome to UCS Performance Manager

After initial setup, the Control Center UI can be accessed by
browsing to:

  https://ucspm:58443
  (default username/password is ccuser/ucspm)

Ensure that ucspm is resolvable to 10.88.121.248, either through your
DNS system or through a HOSTS entry on the browser client. For more
information refer to the installation notes.

You can log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. The
root password defaults to 'ucspm'

Linux Kernel 3.10.0-327.el7.x86_64 on an x86_64
ucspm login: _

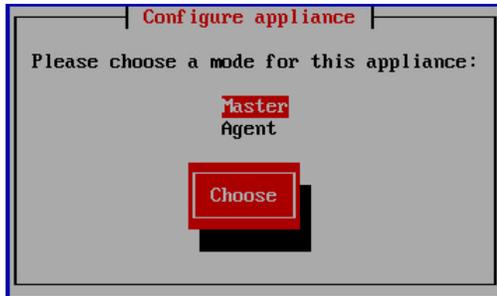
```

- 2 Log in as the `root` user.
The initial password is `ucspm`.
- 3 The system prompts you to enter a new password for `root`.

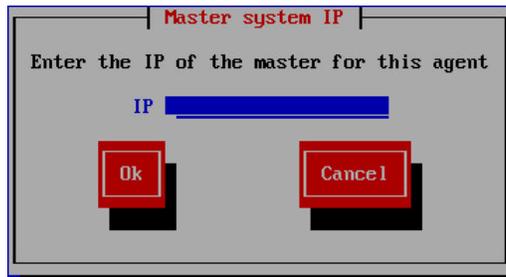
Note Passwords must include a minimum of eight characters, with at least one character from three of the following character classes: uppercase letter, lowercase letter, digit, and special.

- 4 The system prompts you to enter a new password for `ccuser`.
The `ccuser` account is the default account for gaining access to the Control Center browser interface.

- 5 Select the agent role for the virtual machine.



- a In the **Configure appliance** menu, press the down-arrow key to select **Agent**.
- b Press the the **Tab** key to select the **Choose** button, and then the **Enter** key.

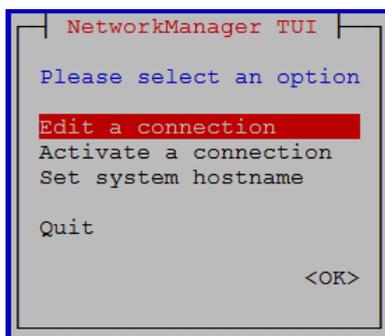


- c In the **IP** field, enter the hostname, fully-qualified domain name, or IPv4 address of the master host.
If you enter the hostname or fully-qualified domain name of the master host, you need an entry in the `/etc/hosts` file of the agent host, or a nameserver on your network, that resolves the name to its IPv4 address.
- d Press the the **Tab** key to select the **Ok** button, and then the **Enter** key.
The system reboots.

Edit a connection

The default configuration for network connections is DHCP. To configure static IPv4 addressing, perform this procedure.

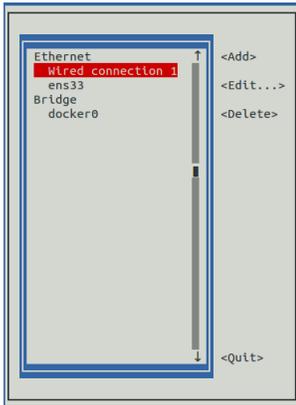
- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.
 - b Press the **Tab** key to select the **Run** button.
 - c Press the **Enter** key.



- 4 On the **NetworkManager TUI** menu, select **Edit a connection**, and then press the **Return** key.

The TUI displays the connections that are available on this host.

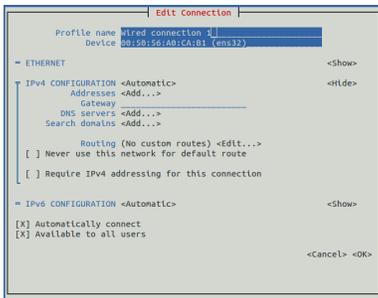
Figure 28: Example: Available connections



- 5 Use the down-arrow key to select **Wired Connection 1**, and then press the **Return** key.

Note Do not use the TUI to edit the `docker0` connection. For more information, see [Configuring the Docker virtual bridge](#) on page 132.

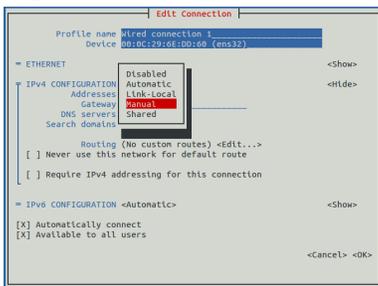
Figure 29: Example: Edit Connection screen



Use the **Tab** key and the arrow keys to navigate among options in the **Edit Connection** screen, and use the **Return** key to toggle an option or to display a menu of options.

- 6 Optional: If the **IPv4 CONFIGURATION** area is not visible, select its display option (**<Show>**), and then press the **Return** key.
- 7 In the **IPv4 CONFIGURATION** area, select **<Automatic>**, and then press the **Return** key.

Figure 30: Example: IPv4 Configuration options



- 8 In the submenu, use the down-arrow key to select **Manual**, and then press the **Return** key.

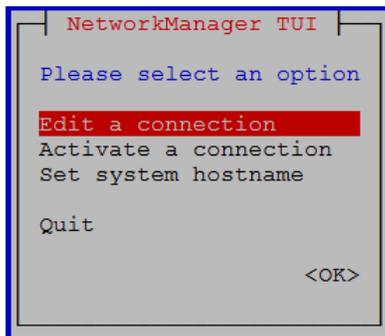
Note For static networking, the option next to **IPv4 CONFIGURATION** must be **Manual**. If it is **Automatic**, the host uses an address from a DHCP server.

- 9 Enter an IPv4 address in CIDR notation.
 - a Use the **Tab** key or the down arrow key to select the **<Add...>** option next to **Addresses**, and then press the **Return** key.
 - b In the **Addresses** field, enter an IPv4 address, followed by the solidus character (/) and then the prefix length.
For more information, see [CIDR prefix lengths for commonly-used netmasks](#) on page 133.
 - c Press the **Return** key.
- 10 Configure the **Gateway** and **DNS servers** fields with IPv4 addresses.
- 11 Use the **Tab** key or the down arrow key to select the **<OK>** option at the bottom of the **Edit Connection** screen, and then press the **Return** key.
- 12 In the available connections screen, use the **Tab** key to select the **<Quit>** option, and then press the **Return** key.
- 13 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

Set system hostname

The default hostname of a Control Center host is `ucspm`. To change the hostname, perform this procedure.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.
 - b Press the **Tab** key to select the **Run** button.
 - c Press the **Enter** key.



- 4 Display the hostname entry field.
 - a In the **NetworkManager TUI** menu, use the down-arrow key to select **Set system hostname**.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.
- 5 In the **Hostname** field, enter the new hostname.
You may enter either a hostname or a fully-qualified domain name.
- 6 Press the **Tab** key twice to select the **OK** button, and then press the **Enter** key.



- 7 In the confirmation dialog, press the **Return** key.
- 8 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

Optional: Editing the /etc/hosts file

This procedure is optional. Perform this procedure to ensure that the Control Center cluster can continue to operate when network nameservers are unavailable.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

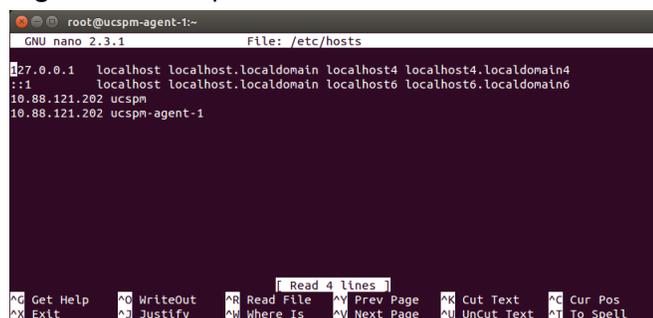
The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 4 Open the `/etc/hosts` file in a text editor.
 - a Start the editor.

```
nano /etc/hosts
```

Figure 31: Example nano session



Use the up-arrow and down-arrow keys to select lines, and the right-arrow and left-arrow keys to select characters on a line.

- b Optional: On agent hosts, the file may include two entries with the same the IP address. Remove the first of the two entries, which maps the IP address to the `ucspm` hostname.
- c Add entries for the Control Center master host and for each agent host.
- d Save the file and exit the editor.

- To save, press **Control-o**. To exit, press **Control-x**.
- 5 Return to the **Appliance Administration** menu.

```
exit
```

- 6 Exit the **Appliance Administration** menu.
 - a Use the down-arrow key to select **Exit**.
 - b Press the **Tab** key, and then press the **Return** key.

7

Enabling NTP on Microsoft Hyper-V guests

Like most distributed applications, Control Center requires a common time source. The procedures in this section enable *NTP* to synchronize the system clocks of all hosts in your Control Center cluster.

You may configure NTP to rely on public time servers or on a private master server.

- If all of the hosts in your Control Center cluster can access the internet, configure NTP to rely on public time servers.
- If none of the hosts in your Control Center cluster can access the internet, configure NTP to rely on a private master server.

Note The procedures in this section are required only for multi-host deployments running as Microsoft Hyper-V guests. VMware vSphere guests use an hourly `crontab` job to synchronize their system clocks with the host.

Configuring NTP for public time servers

This procedure uses the default configuration of NTP to synchronize system clocks with public time servers. If all of the hosts in your Control Center cluster can access the internet, repeat this procedure on each host in the cluster, starting with the Control Center master host.

Note Do not perform this procedure on VMware vSphere guests.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Stop Control Center.

```
systemctl stop serviced
```

- 4 Synchronize the system clock and enable the NTP daemon.

- a Set the system time.

```
ntpdate -u -g
```

- b Enable the ntpd daemon.

```
systemctl enable ntpd
```

- c Configure ntpd to start when the system starts.

Currently, an unresolved issue associated with NTP prevents ntpd from restarting correctly after a reboot, and the following commands provide a workaround to ensure that it does.

```
echo "systemctl start ntpd" >> /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local
```

- d Start ntpd.

```
systemctl start ntpd
```

- 5 Start Control Center.

```
systemctl start serviced
```

Configuring an NTP master server

This procedure configures an NTP master server on the Control Center master host. Perform this procedure only if the host does not have internet access.

Note Do not perform this procedure on VMware vSphere guests.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as root.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Create a backup of the NTP configuration file.

```
cp -p /etc/ntp.conf /etc/ntp.conf.orig
```

- 4 Edit the NTP configuration file./

- a Open `/etc/ntp.conf` with a text editor.
- b Replace all of the lines in the file with the following lines:

```
# Use the local clock
server 127.127.1.0 prefer
fudge 127.127.1.0 stratum 10
driftfile /var/lib/ntp/drift
broadcastdelay 0.008
```

```
# Give localhost full access rights
```

```
restrict 127.0.0.1

# Grant access to client hosts
restrict ADDRESS_RANGE mask NETMASK nomodify notrap
```

- c Replace ADDRESS_RANGE with the range of IPv4 network addresses that are allowed to query this NTP server.

For example, the following IP addresses are assigned to the hosts in an Control Center cluster:

```
203.0.113.10
203.0.113.11
203.0.113.12
203.0.113.13
```

For the preceding addresses, the value for ADDRESS_RANGE is 203.0.113.0.

- d Replace NETMASK with the IPv4 network mask that corresponds with the address range. For example, the network mask for 203.0.113.0 is 255.255.255.0.
 - e Save the file and exit the editor.
- 5 Stop Control Center.

```
systemctl stop serviced
```

- 6 Enable and start the NTP daemon.
- a Enable the ntpd daemon.

```
systemctl enable ntpd
```

- b Configure ntpd to start when the system starts.

Currently, an unresolved issue associated with NTP prevents ntpd from restarting correctly after a reboot, and the following commands provide a workaround to ensure that it does.

```
echo "systemctl start ntpd" >> /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local
```

- c Start ntpd.

```
systemctl start ntpd
```

- 7 Start Control Center.

```
systemctl start serviced
```

Configuring NTP clients

This procedure configures agent hosts to synchronize their clocks with the NTP server on the Control Center master host. Perform this procedure only if the hosts do not have internet access, and repeat this procedure on each agent host in your Control Center cluster.

Note Do not perform this procedure on VMware vSphere guests.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as *root*.

- a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
- b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Create a backup of the NTP configuration file.

```
cp -p /etc/ntp.conf /etc/ntp.conf.orig
```

- 4 Edit the NTP configuration file./

- a Open `/etc/ntp.conf` with a text editor.
- b Replace all of the lines in the file with the following lines:

```
# Point to the master time server
server MASTER_ADDRESS

restrict default ignore
restrict 127.0.0.1
restrict MASTER_ADDRESS mask 255.255.255.255 nomodify notrap noquery

driftfile /var/lib/ntp/drift
```

- c Replace both instances of `MASTER_ADDRESS` with the IPv4 address of the host where the NTP server is running (the Control Center master host).
- d Save the file and exit the editor.
- 5 Stop Control Center.

```
systemctl stop serviced
```

- 6 Synchronize the clock with the master server.

```
ntpdate -gq
```

- 7 Enable and start the NTP daemon.

- a Enable the `ntpd` daemon.

```
systemctl enable ntpd
```

- b Configure `ntpd` to start when the system starts.

Currently, an unresolved issue associated with NTP prevents `ntpd` from restarting correctly after a reboot, and the following commands provide a workaround to ensure that it does.

```
echo "systemctl start ntpd" >> /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local
```

- c Start `ntpd`.

```
systemctl start ntpd
```

- 8 Start Control Center.

```
systemctl start serviced
```

8

Configuring the master host

The default installation of the Control Center master host configures it for migration tasks and for single-host deployments. The procedures in this section change the default configuration to multi-host.

For information about setting up collectors for Control Center, refer to the *Cisco UCS Performance Manager Administration Guide*.

Note Before performing the procedures in this chapter, stop Cisco UCS Performance Manager. For more information, see [Shutting down a Control Center master host](#) on page 115.

Optional: Editing the /etc/hosts file

This procedure is optional. Perform this procedure to ensure that the Control Center cluster can continue to operate when network nameservers are unavailable.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Open the `/etc/hosts` file in a text editor.

The following steps use the *nano* editor.

- a Start the editor.

```
nano /etc/hosts
```

Figure 32: Example nano session

Use the up-arrow and down-arrow keys to select lines, and the right-arrow and left-arrow keys to select characters on a line.

- b Optional: On agent hosts, the file may include two entries with the same the IP address. Remove the first of the two entries, which maps the IP address to the ucspm hostname.
- c Add entries for the Control Center master host and for each agent host.
- d Save the file and exit the editor.

To save, press **Control-o**. To exit, press **Control-x**.

- 4 Return to the **Appliance Administration** menu.

```
exit
```

- 5 Exit the **Appliance Administration** menu.
 - a Use the down-arrow key to select **Exit**.
 - b Press the **Tab** key, and then press the **Return** key.

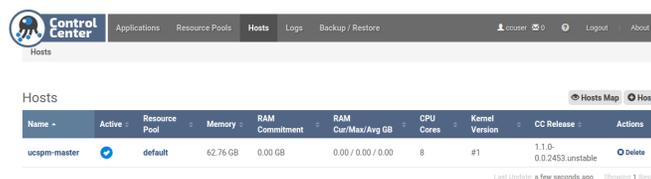
Adding agent hosts to the default resource pool

Use this procedure to add agent hosts to the Control Center default resource pool.

- 1 Display the login page of the Control Center browser interface.
Replace *HostName* with the name or IP address of the Control Center master host.

```
https://HostName:50443
```

- 2 At the login page, enter `ccuser` and its password.
- 3 At the top of the page, click **Hosts**.

Figure 33: Hosts page

- 4 On the **Hosts** page, click the **+ Host** button.
The button is at the right side of the page.

Figure 34: Add Host dialog

- 5 In the **Add Host** dialog, add one of the agent hosts to the `default` resource pool.
 - a In the **Host** field, enter the hostname or IP address of an agent host.
 - b Skip the **Port** field.
The default value, 4979, is correct.
 - c In the **Resource Pool ID** field, select `default` from the list.
 - d In the **RAM Commitment** field, enter the amount of non-system RAM to devote to Control Center.
Cisco recommends leaving the field blank or entering 100%.
 - e At the bottom of the **Add Host** dialog, click **Add Host**.
- 6 Repeat the preceding two steps for each agent host.

Identifying network device names

Use this procedure to identify the network device name on each agent host in a Control Center cluster.

Note Control Center uses the `ip` command to bind device names to a virtual IP address. The interface names of all agent hosts must be identical.

- 1 Display the login page of the Control Center browser interface.
Replace *HostName* with the name or IP address of the Control Center master host.

```
https://HostName:50443
```

- 2 At the login page, enter `ccuser` and its password.
- 3 At the top of the page, click **Hosts**.

Figure 35: Hosts page

Name	Active	Resource Pool	Memory	RAM Commitment	RAM Cur/Max/Avg GB	CPU Cores	Kernel Version	CC Release	Actions
ucspn-master	Active	default	62.76 GB	0.00 GB	0.00 / 0.00 / 0.00	8	#1	1.1.0-0.0.2453 unstable	Delete

- 4 Display the network device name of an agent host.
 - a In the column of the **Hosts** table, click the name of an agent host.
 - b On the host's detail page, scroll down to the **IPs** table.
The device name is displayed in the **Interface** column.
 - c Make a note of the device name, for use in a subsequent procedure.
- 5 Repeat the preceding step for each agent host.

Adding a virtual IP address to the default pool

Use this procedure to add a virtual IP address to the Control Center `default` resource pool.

- 1 Display the login page of the Control Center browser interface.
Replace `HostName` with the name or IP address of the Control Center master host.

```
https://HostName:50443
```

- 2 At the login page, enter `ccuser` and its password.
- 3 At the top of the page, click **Resource Pools**.

Figure 36: Resource Pools page

Resource Pool	CPU Cores	Memory Usage	Created	Last Modified	Actions
default	28	37.38 GB / 146.71 GB	Nov 11, 2015 12:43:20 PM	Nov 11, 2015 12:43:20 PM	Delete

- 4 In the **Resource Pool** column of the **Resource Pool** table, click `default`.

Figure 37: Default resource pool

Resource Pool	CPU Cores	Memory	Created	Last Modified
default	24	188.29 GB	Aug 13, 2016 5:20:56 AM	Aug 15, 2016 5:15:21 AM

IP	Netmask	Bind Interface	Action
No Data Found			

Name	Memory	CPU Cores	Kernel Version
ucpm-agent-1	62.76 GB	8	#1
ucpm-agent-2	62.76 GB	8	#1
ucpm-agent-3	62.76 GB	8	#1

- 5 At the right side of the **Virtual IPs** table, click **Add Virtual IP**.

Figure 38: Add Virtual IP dialog box

- 6 Add a virtual IP address to the `default` pool.
 - a In the **IP** field, enter an unused IPv4 address that is in the same subnet as the other hosts in the pool.
 - b In the **Netmask** field, enter the netmask of the subnet.
 - c In the **Interface** field, enter the network device name that all of the agent hosts share.

Moving the master host to a new pool

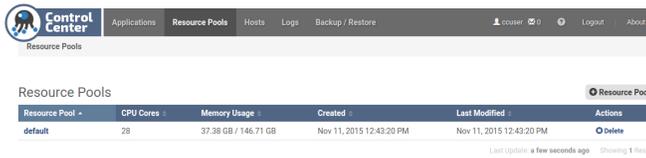
This procedure creates a new resource pool for the Control Center master host, and moves it to the new pool.

- 1 Display the login page of the Control Center browser interface.
Replace *HostName* with the name or IP address of the Control Center master host.

```
https://HostName:50443
```

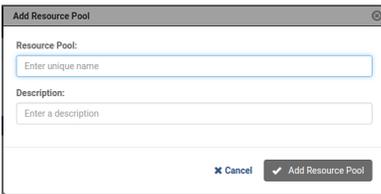
- 2 At the login page, enter `ccuser` and its password.
- 3 At the top of the page, click **Resource Pools**.

Figure 39: Resource Pools page



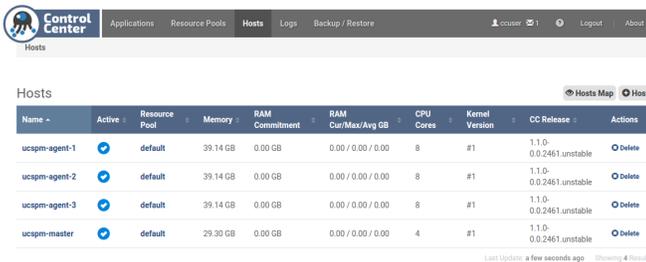
- 4 On the **Resource Pools** page, click the **+ Resource Pool** button.
The button is at the right side of the page.

Figure 40: Add Resource Pool dialog



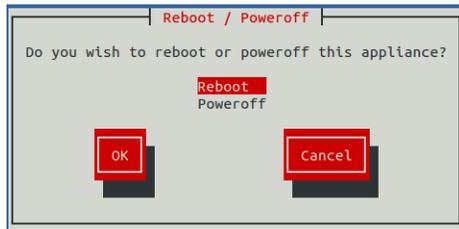
- 5 In the **Add Resource Pool** dialog, create a resource pool named `master`.
 - a In the **Resource Pool** field, enter `master`.
You may use a different name, if desired.
 - b Optional: In the **Description** field, enter descriptive text, if desired.
 - c At the bottom of the **Add Resource Pool** dialog, click **Add Resource Pool**.
- 6 At the top of the page, click **Hosts**.

Figure 41: Hosts page with 4 hosts

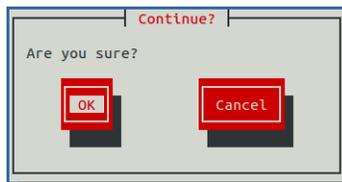


- 7 Remove the Control Center master host from the `default` resource pool.
 - a In the **Actions** column of the **Hosts** table, click the **Delete** control of the Control Center master host.
In the preceding example, the master host is named `ucspm-master`.
 - b In the **Remove Host** dialog, click the **Remove Host** button.
- 8 Add the Control Center master host to the `master` resource pool.
 - a Click the **+ Host** button.
The button is at the right side of the page.
 - b In the **Host** field, enter the hostname or IP address of the master host.
 - c Skip the **Port** field.
The default value, 4979, is correct.

- d In the **Resource Pool ID** field, select `master` from the list.
 - e In the **RAM Commitment** field, enter the amount of non-system RAM to devote to Control Center.
Cisco recommends leaving the field blank or entering 100%.
 - f At the bottom of the **Add Host** dialog, click **Add Host**.
- 9 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
 - 10 Log in as the `root` user.
 - 11 In the **Appliance Administration** menu, select the **Reboot / Poweroff System** option.



- 12 Select **Reboot**.
- 13 Press the **Tab** key to highlight **OK**, and then press the **Return** key.



- 14 Select **OK**, and then press the **Return** key.
The system reboots.

Changing IP assignments

Use this procedure to change the IP assignments of the **RabbitMQ**, **zenmail**, and **zenpop3** services. When the master host is moved to a new resource pool, the services need new IP addresses.

- 1 Display the login page of the Control Center browser interface.
Replace *HostName* with the name or IP address of the Control Center master host.

```
https://HostName:50443
```

- 2 At the login page, enter `ccuser` and its password.

Figure 42: Landing page

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	●	Internal	N/A	N/A	N/A
ucspm (v2.0.1)	Cisco UCS Performance Manager	●	Test	default	https://ucspm.cc-master:50443 https://cc-master	▶ Start ■ Stop ● Delete

Application Template	ID	Description	Actions
ucspm (v2.0.1)	59f1337508ecf73bd27c2283694f2ce5	Cisco UCS Performance Manager	● Delete

- 3 In the **Application** column of the **Applications** table, click **ucspm**, and then scroll down to the **IP Assignments** table.
- 4 In the **Actions** column of the **RabbitMQ** service, click the **Assign** control.

Figure 43: Assign IP dialog box

The **Service**, **Endpoint**, and **Port** fields are locked.

- 5 From the **IP** list, select the virtual IP address assigned to the **default** resource pool, and then click **Assign IP**.
- 6 Repeat the previous two steps for the other services in the **IP Assignments** table.

Reducing master host resources

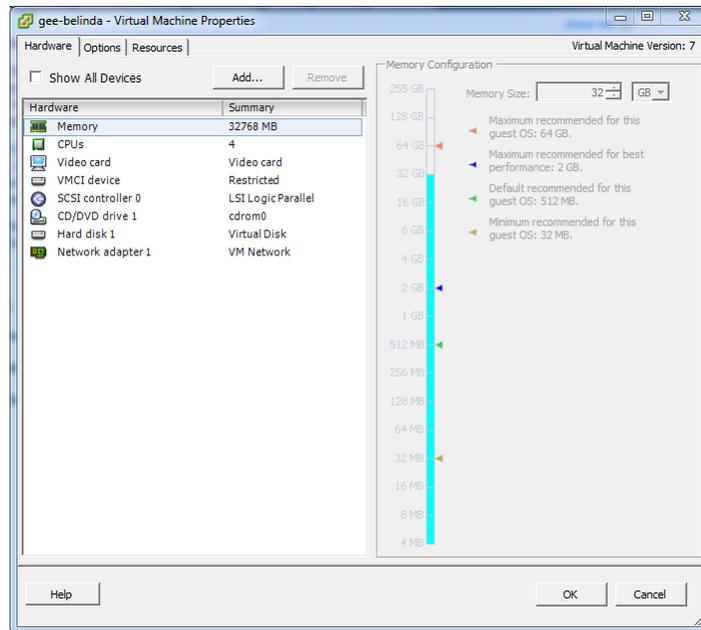
Perform one of the procedures in this section to reduce the amount of RAM and the number of CPU cores that are dedicated to the Control Center master host.

Reducing master host resources with vSphere

To perform this task, you need a VMware vSphere client.

This procedure reduces the amount of RAM and the number of CPU cores that are dedicated to the Control Center master host, using VMware vSphere Client 5.0.0. The procedure is slightly different with different versions of VMware vSphere Client.

- 1 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home > Inventory > Inventory** view.
- 2 In the left column, right-click on the name of the Control Center master host.
- 3 On the **Getting Started** tab, click the **Shut down the virtual machine** link.
- 4 When the system is shut down, click the **Edit virtual machine settings** link.

Figure 44: Virtual Machine Properties dialog

- 5 In the **Hardware** table on the left side, select **Memory**.
- 6 In the **Memory Configuration** area on the right side, change the value in the **Memory Size** field from 64GB to 30GB.
- 7 In the **Hardware** table, select **CPUs**.
- 8 In the **Number of virtual sockets** field, change the value from 8 to 4.
- 9 At the bottom of the **Virtual Machine Properties** dialog, click the **OK** button.

Reducing master host resources with Hyper-V

To perform this task, you need:

- A Microsoft Remote Desktop client
- Administrator privileges on a Microsoft Hyper-V server

This procedure reduces the amount of RAM and the number of CPU cores that are dedicated to the Control Center master host, using Microsoft Hyper-V Manager.

- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Start **Hyper-V Manager**.
- 3 In **Hyper-V Manager**, right-click the name of the Control Center master host, and then select **Shut Down...**
- 4 When the master host state is **Off**, right-click name of the Control Center master host, and then select **Settings...**
- 5 In the **Hardware** area of the **Settings** dialog, select **Memory**.
- 6 In the **Memory** area, change the value in the **Startup RAM** field from 65536 to 30720.
- 7 In the **Hardware** area of the **Settings** dialog, select **Processor**.
- 8 In the **Processor** area, change the value in the **Number of virtual processors** field from 8 to 4, and then click **OK**.

Restarting the master host

Perform one of the procedures in this section to restart the Control Center master host.

Restarting the master host with vSphere

To perform this task, you need a VMware vSphere client.

- 1 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home > Inventory > Inventory** view.
- 2 In the left column, right-click on the name of the Control Center master host.
- 3 On the **Summary** tab, click the **Power On** link.

Restarting the master host with Hyper-V

To perform this task, you need:

- A Microsoft Remote Desktop client
 - Administrator privileges on a Microsoft Hyper-V server
- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
 - 2 Start **Hyper-V Manager**.
 - 3 In **Hyper-V Manager**, right-click the name of the Control Center master host, and then select **Start**.

9

Configuring a ZooKeeper cluster

Control Center relies on [Apache ZooKeeper](#) to distribute and manage application services. ZooKeeper maintains the definitions of each service and the list of services assigned to each host. The scheduler, which runs on the master host, determines the assignments and sends them to the ZooKeeper node that is serving as the leader. All Control Center agent hosts retrieve the assignments and service definitions and start containers for the services as required. The procedures in this section create a ZooKeeper cluster on the master host and two agent hosts.

One of the agent hosts is not used in the cluster. ZooKeeper requires an odd number of hosts in a cluster, and the Control Center master host is always a member. You may choose any two of the three agent hosts to participate in the cluster.

Note The Control Center configuration file of the host that is not a member of the ZooKeeper cluster must be updated with the list of hosts that are members of the ZooKeeper cluster. The required procedure is included in this section.

The procedures in this section rely on common definitions for temporary variables that identify the IPv4 address of each host in the ZooKeeper cluster. ZooKeeper requires IP addresses for cluster configuration, and the variables simplify the configuration process. The following table identifies the temporary variables, the names and values of which must be identical on each host.

Variable	Value
node1	IPv4 address of the Control Center master host
node2	IPv4 address of Control Center agent host A
node1	IPv4 address of Control Center agent host B

Note Before performing the procedures in this chapter, stop Cisco UCS Performance Manager. For more information, see [Shutting down a Control Center master host](#) on page 115.

Example multi-host ZooKeeper configuration

This example shows the ZooKeeper environment variables in the `/etc/defaults/serviced` configuration file of each host in a 4-node Control Center cluster. The settings in this example are also provided in the subsequent procedures.

Note The value of the `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable is formatted to fit the available space. In the configuration file, the variable and value are on the same line.

Master host and ZooKeeper cluster node, 198.51.100.135:

```
SERVICED_ISVCS_ZOOKEEPER_ID=1
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@0.0.0.0:2888:3888,\
  2@198.51.100.136:2888:3888,3@198.51.100.137:2888:3888
```

Agent host and ZooKeeper cluster node, 198.51.100.136:

```
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=2
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
  2@0.0.0.0:2888:3888,3@198.51.100.137:2888:3888
```

Agent host and ZooKeeper cluster node, 198.51.100.137:

```
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=3
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
  2@198.51.100.136:2888:3888,3@0.0.0.0:2888:3888
```

Agent host, 198.51.100.138:

```
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
```

Configuring the master host

Use this procedure to configure a ZooKeeper cluster on the master host.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Define the IP address variables for each node in the ZooKeeper cluster.
Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

- 4 Set the ID of this node in the ZooKeeper cluster to 1.

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=1" >> /etc/default/serviced
```

- 5 Specify the hosts in the ZooKeeper cluster.

You may copy the following text from this document and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
  >> /etc/default/serviced
```

- 6 Specify the hosts in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its cluster. To achieve this, replace the IP address of the master host with 0.0.0.0.

You may copy the following of text and paste it in your console:

```
q1="1@0.0.0.0:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
  >> /etc/default/serviced
```

- 7 Verify the ZooKeeper environment variables.

```
egrep '^[^#]*SERVICED' /etc/default/serviced | egrep '_Z(OO|K)'
```

The following example shows the environment variables for a master host with IP address 198.51.100.135.

Note The value of the `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable is formatted to fit the available space. The result of the `egrep` command shows the variable and value on the same line.

```
SERVICED_ISVCS_ZOOKEEPER_ID=1
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@0.0.0.0:2888:3888,\
  2@198.51.100.136:2888:3888,3@198.51.100.137:2888:3888
```

Configuring agent host A

Use this procedure to configure a ZooKeeper cluster on the agent host designated as *Agent-Host-A-IP*.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Define the IP address variables for each node in the ZooKeeper cluster. Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

- 4 Set the ZooKeeper start flag.

```
echo "SERVICED_ISVCS_START=zookeeper" >> /etc/default/serviced
```

- 5 Set the ID of this node in the ZooKeeper cluster .

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=2" >> /etc/default/serviced
```

- 6 Remove the default setting for the ZooKeeper cluster.

```
sed -i.bak '/SERVICED_ZK=/ d' /etc/default/serviced
```

- 7 Specify the hosts in the ZooKeeper cluster.

You may copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 8 Specify the hosts in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its cluster. To achieve this, replace the IP address of the current node with 0.0.0.0.

```
q1="1@${node1}:2888:3888"
q2="2@0.0.0.0:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

- 9 Verify the ZooKeeper environment variables.

```
egrep '^[^#]*SERVICED' /etc/default/serviced \
| egrep '(CS_ZO|_ZK|CS_ST)'
```

The following example shows the environment variables for an agent host with IP address 198.51.100.136.

Note The value of the `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable is formatted to fit the available space. The result of the `egrep` command shows the variable and value on the same line.

```
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=2
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
2@0.0.0.0:2888:3888,3@198.51.100.137:2888:3888
```

Configuring agent host B

Use this procedure to configure a ZooKeeper cluster on the agent host designated as *Agent-Host-B-IP*.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Define the IP address variables for each node in the ZooKeeper cluster.

Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

- 4 Set the ZooKeeper start flag.

```
echo "SERVICED_ISVCS_START=zookeeper" >> /etc/default/serviced
```

- 5 Set the ID of this node in the ZooKeeper cluster .

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=3" >> /etc/default/serviced
```

- 6 Remove the default setting for the ZooKeeper cluster.

```
sed -i.bak '/SERVICED_ZK=/ d' /etc/default/serviced
```

- 7 Specify the hosts in the ZooKeeper cluster.

You may copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 8 Specify the hosts in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its cluster. To achieve this, replace the IP address of the current node with 0.0.0.0.

```
q1="1@${node1}:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@0.0.0.0:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

- 9 Verify the ZooKeeper environment variables.

```
egrep '^[^#]*SERVICED' /etc/default/serviced \
| egrep '(CS_ZO|_ZK|CS_ST)'
```

The following example shows the environment variables for an agent host with IP address 198.51.100.137.

Note The value of the *SERVICED_ISVCS_ZOOKEEPER_QUORUM* variable is formatted to fit the available space. The result of the *egrep* command shows the variable and value on the same line.

```
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=3
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
2@198.51.100.136:2888:3888,3@0.0.0.0:2888:3888
```

Starting a ZooKeeper cluster

Use this procedure to start a ZooKeeper cluster.

The window of time for starting a ZooKeeper ensemble is relatively short. The goal of this procedure is to restart Control Center on each ensemble node at about the same time, so that each node can participate in electing the leader.

- 1 Log in to the Control Center master host.
- 2 In a separate window, log in to the second node of the ZooKeeper ensemble (*Agent-Host-A-IP*).
- 3 In another separate window, log in to the third node of the ZooKeeper ensemble (*Agent-Host-B-IP*).
- 4 On the master host, stop and start `serviced`.

```
systemctl stop serviced && systemctl start serviced
```

- 5 On both resource pool hosts, stop and start `serviced`.

```
systemctl stop serviced && systemctl start serviced
```

- 6 On the master host, check the status of the ZooKeeper cluster.

```
{ echo stats; sleep 1; } | nc localhost 2181 | grep Mode
{ echo stats; sleep 1; } | nc Agent-Host-A-IP 2181 | grep Mode
{ echo stats; sleep 1; } | nc Agent-Host-B-IP 2181 | grep Mode
```

Note This is the only method available to verify the status of a ZooKeeper cluster.

Updating the agent host that is not in the ZooKeeper cluster

The Control Center configuration file of the host that is not a member of the ZooKeeper cluster must be updated, even though it is not in the cluster. Use this procedure to update the configuration file.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Define the IP address variables for each node in the ZooKeeper cluster. Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

- 4 Remove the default setting for the ZooKeeper cluster.

```
sed -i.bak '/SERVICED_ZK=/ d' /etc/default/serviced
```

- 5 Specify the hosts in the ZooKeeper cluster. You may copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

6 Verify the setting.

```
egrep '^[^#]*SERVICED_ZK' /etc/default/serviced
```

The following example shows the environment variable for an agent host that is not a node in the ZooKeeper cluster:

```
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
```

7 Restart the Control Center daemon.

```
systemctl stop serviced && systemctl start serviced
```

Part III: Performing upgrades

The chapters in this part describe how to upgrade single-host and multi-host deployments on VMware vSphere and Microsoft Hyper-V systems. The following table shows the supported upgrade paths.

From version	To version
Cisco UCS Performance Manager 2.0.0	Cisco UCS Performance Manager 2.0.2
Cisco UCS Performance Manager 2.0.1	Cisco UCS Performance Manager 2.0.2

Upgrading Cisco UCS Performance Manager on vSphere systems

10

This appendix describes how to upgrade Cisco UCS Performance Manager on vSphere systems.

Note Cisco strongly recommends checking the integrity of Cisco UCS Performance Manager databases before performing an upgrade. For more information, see [Using Zenoss Toolbox](#) on page 136. In addition, Cisco strongly recommends creating a backup before performing an upgrade. Backups can be created with the Control Center backup feature or with the vSphere backup feature. However, before using the vSphere backup feature, Cisco UCS Performance Manager, Control Center, and the Control Center master host must be shut down cleanly and completely. For more information, see [Shutting down a Control Center master host](#) on page 115.

The upgrade steps depends on the deployment type, as outlined in the following table.

Single-host deployments	Multi-host deployments
<ol style="list-style-type: none"> 1 Prepare to upgrade Cisco UCS Performance Manager. 2 Attach the upgrade ISO to the Cisco UCS Performance Manager virtual machine. 3 Stop Cisco UCS Performance Manager. 4 Perform the upgrade. 5 Start Cisco UCS Performance Manager. 	<ol style="list-style-type: none"> 1 Prepare to upgrade Cisco UCS Performance Manager. 2 On the master host, stop Cisco UCS Performance Manager, and then stop Control Center. 3 On each agent host: <ol style="list-style-type: none"> a Attach the upgrade ISO to the virtual machine. b Perform the upgrade. 4 On the master host, attach the upgrade ISO. 5 Perform the upgrade. 6 Start Cisco UCS Performance Manager.

For optimum results, Cisco recommends reviewing the upgrade procedures before performing the upgrade.

Note The procedures in this appendix are deployment-specific. That is, the procedures only upgrade a single-host deployment to a single-host deployment and likewise for multi-host deployments. To change your deployment type from single-host to multi-host, first follow the instructions for upgrading a single-host deployment, and then follow the instructions in [Creating a multi-host deployment](#) on page 34.

All upgrades of Cisco UCS Performance Manager include an upgrade of the virtual machine operating system. The upgrades include a new kernel version, which fixes an `fsttrim` bug.

Upgrading single-host deployments

To upgrade a single-host deployment, perform each procedure in this section.

Preparing to upgrade

Perform this procedure before upgrading your deployment.

- 1 Verify that Cisco UCS Performance Manager is operating normally.
 - a Log in to the Control Center browser interface as `ccuser`.
 - b In the **Application** column of the **Applications** table, click **ucspm**.
 - c Verify that all of the services in the **IP Assignments** table have valid IP addresses.
 - d Scroll down to the **Services** table, and then verify that none of the child services have failing health checks.
- 2 Check the integrity of Cisco UCS Performance Manager databases.
For more information, see [Using Zenoss Toolbox](#) on page 136.
- 3 Create a backup of Cisco UCS Performance Manager.
Backups can be created with the Control Center backup feature or with the backup feature of your hypervisor.

Note Before using the hypervisor backup feature, Cisco UCS Performance Manager, Control Center, and the Control Center master host must be shut down cleanly and completely. For more information, see [Shutting down a Control Center master host](#) on page 115.

Attaching an update ISO with vSphere

To perform this task, you need:

- A VMware vSphere client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

This procedure attaches an Cisco UCS Performance Manager update ISO file to the CD/DVD drive of the Control Center host.

- 1 Download the Cisco UCS Performance Manager update ISO file from the [Cisco UCS Performance Manager](#) site to your workstation.
- 2 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges.
- 3 With the **View** menu, enable **Toolbar** and **Show VMs in Inventory**.
- 4 In the **Inventory** list, select the name of the Control Center host.
- 5 Enable the CD/DVD drive of the Control Center master host.
 - a On the **Summary** page, click **Edit Settings**.
 - b In the **Hardware** table of the **Virtual Machine Properties** dialog, select **CD/DVD drive 1**.
 - c In the **Device Type** area, click **Client Device**.
 - d At the bottom of the **Virtual Machine Properties** dialog, click **OK**.
- 6 Attach the update ISO file to the the Control Center master host.
 - a In the toolbar, click the CD/DVD drive icon.
 - b From the menu, select **CD/DVD drive 1 > Connect to ISO image on local disk...**
 - c In the **Open** dialog, select the update ISO file, and then click the **Open** button.

Stopping Cisco UCS Performance Manager

Use this procedure to stop Cisco UCS Performance Manager.

- 1 Log in to the Control Center browser interface as `ccuser`.

The screenshot shows the Control Center web interface. At the top, there is a navigation bar with tabs for Applications, Resource Pools, Hosts, Logs, and Backup / Restore. The main content area is divided into two sections: Applications and Application Templates. The Applications section contains a table with columns for Application, Description, Status, Deployment ID, Resource Pool, Public Endpoints, and Actions. The Application Templates section contains a table with columns for Application Template, ID, and Description.

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	✓	Internal	N/A	N/A	N/A
ucspm (v2.0.1)	Cisco UCS Performance Manager	✓	Test	default	https://ucspm.ucspm:50443 https://ucspm	▶ Start ■ Stop ○ Delete

Application Template	ID	Description
ucspm (v2.0.1)	970566e6d1bbae54bc028d295a8b9d0e	Cisco UCS Performance Manager

- 2 In the **Actions** column of the **Applications** table, click the **Stop** control of **ucspm**.
- 3 In the **Stop Service** dialog, click **Stop Service and 46 Children**.

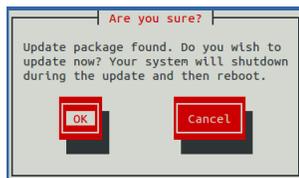
Updating appliance software

Before performing this procedure, attach the update ISO file to the Control Center host. For more information, see [Attaching an update ISO with vSphere](#).

This option updates the Control Center and Cisco UCS Performance Manager software on a host.

Note The upgrade software creates a complete record of its work. The file name is `/tmp/upgrade-ucspm-TimeStamp.log`. To preserve the file, copy it from `/tmp` to different location before stopping or restarting the virtual machine.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, use the down arrow key to select **Update System**, and then press the **Return** key.



- To cancel the update, press the **Tab** key, and then press the **Return** key.

Result: The **Appliance Administration** menu returns to the top level.

- To update the system, press the **Return** key.

Result: The **Appliance Administration** menu is replaced by progress messages as the upgrade process begins.

On success, the following message is displayed:

```
Script done, file is /var/log/serviced/script-2016-08-03-190832-root.log
Looking up service UCSPM
Service UCSPM has version
Set new version 2.0.2
Saving new version of UCSPM
Updated ucspm.
Restarting ucspm...
Restarted ucspm.
```

```
ucspm upgraded successfully.
```

In addition, the **Appliance Administration** menu returns to the top level.

On failure, one of the following messages is displayed:

```
Failed to stop all ucspm services.
Upgrade failed. Press any key to return.

Failed to stop serviced.
Upgrade failed. Press any key to return.

Failed to restart serviced.
Upgrade failed. Press any key to return.

Failed to upgrade serviced binary.
Upgrade failed. Press any key to return.

Error upgrading ucspm.
You may need to remove one or more preupgrade snapshots before retrying
this upgrade.
Upgrade failed. Press any key to return.
```

Contact Cisco Support before proceeding.

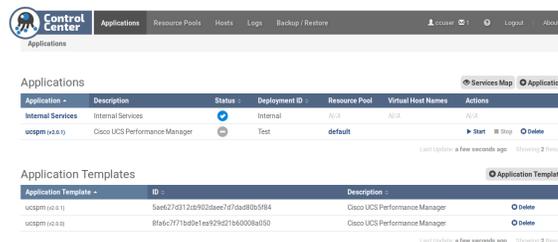
Starting Cisco UCS Performance Manager

Use this procedure to start Cisco UCS Performance Manager and verify the upgrade.

- 1 Display the login page of the Control Center browser interface.
Replace *HostName* with the name or IP address of the Control Center master host:

```
https://HostName
```

- 2 Log in as ccuser.



The screenshot shows the Cisco Control Center web interface. The top navigation bar includes 'Applications', 'Resource Pools', 'Hosts', 'Logs', 'Backup / Restore', and user information. The main content area is divided into two sections: 'Applications' and 'Application Templates'. Both sections have a table with columns for Application/Template name, Description, Status, Deployment ID, Resource Pool, Virtual Host Names, and Actions.

Application	Description	Status	Deployment ID	Resource Pool	Virtual Host Names	Actions
Internal Services	Internal Services	Running	Internal	UCS	UCS	Start Stop Delete
ucspm (v2.4.1)	Cisco UCS Performance Manager	Running	Test	default		Start Stop Delete

Application Template	ID	Description	Actions
ucspm (v2.4.1)	5a627d312ca902d0ee7d71dca880b5184	Cisco UCS Performance Manager	Delete
ucspm (v2.4.0)	8f6c7771bd5e1e929d21b60008a950	Cisco UCS Performance Manager	Delete

The **Applications** table shows the updated application, and the **Application Templates** table includes the old and new templates.

Note Do not attempt to add either the old or the new application template. The new template is already added and deployed.

- 3 In the **Actions** column of the **Applications** table, click the **Start** control of **ucspm**.
- 4 In the **Start Service** dialog, click **Start Service and 46 Children**.

Upgrading multi-host deployments

To upgrade a multi-host deployment, perform each procedure in this section.

Preparing to upgrade

Perform this procedure before upgrading your deployment.

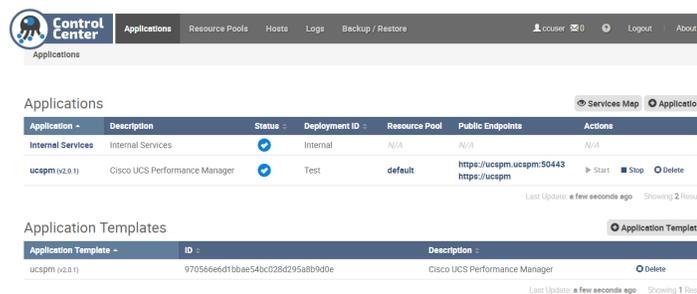
- 1 Verify that Cisco UCS Performance Manager is operating normally.
 - a Log in to the Control Center browser interface as `ccuser`.
 - b In the **Application** column of the **Applications** table, click **ucspm**.
 - c Verify that all of the services in the **IP Assignments** table have valid IP addresses.
 - d Scroll down to the **Services** table, and then verify that none of the child services have failing health checks.
- 2 Check the integrity of Cisco UCS Performance Manager databases.
For more information, see [Using Zenoss Toolbox](#) on page 136.
- 3 Create a backup of Cisco UCS Performance Manager.
Backups can be created with the Control Center backup feature or with the backup feature of your hypervisor.

Note Before using the hypervisor backup feature, Cisco UCS Performance Manager, Control Center, and the Control Center master host must be shut down cleanly and completely. For more information, see [Shutting down a Control Center master host](#) on page 115.

Stopping Cisco UCS Performance Manager and Control Center

Use this procedure to stop Cisco UCS Performance Manager and Control Center.

- 1 Log in to the Control Center browser interface as `ccuser`.



- 2 In the **Actions** column of the **Applications** table, click the **Stop** control of **ucspm**.
- 3 In the **Stop Service** dialog, click the **Stop Service and 47 Children** button.
- 4 Gain access to the Control Center master host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 5 Log in as the `root` user.
- 6 Use the **Down Arrow** key to select **Root Shell**, and then press the **Return** key.
The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~] #
```

- 7 Stop the Control Center service.

```
systemctl stop serviced
```

Updating agent hosts

Repeat each procedure in this section on each agent host in your deployment.

Attaching an update ISO with vSphere

To perform this task, you need:

- A VMware vSphere client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

This procedure attaches a Cisco UCS Performance Manager update ISO file to the CD/DVD drive of the Control Center host.

- 1 Download the Cisco UCS Performance Manager update ISO file from the [Cisco UCS Performance Manager](#) site to your workstation.
- 2 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges.
- 3 With the **View** menu, enable **Toolbar** and **Show VMs in Inventory**.
- 4 In the **Inventory** list, select the name of the Control Center host.
- 5 Enable the CD/DVD drive of the Control Center master host.
 - a On the **Summary** page, click **Edit Settings**.
 - b In the **Hardware** table of the **Virtual Machine Properties** dialog, select **CD/DVD drive 1**.
 - c In the **Device Type** area, click **Client Device**.
 - d At the bottom of the **Virtual Machine Properties** dialog, click **OK**.
- 6 Attach the update ISO file to the the Control Center master host.
 - a In the toolbar, click the CD/DVD drive icon.
 - b From the menu, select **CD/DVD drive 1 > Connect to ISO image on local disk...**
 - c In the **Open** dialog, select the update ISO file, and then click the **Open** button.

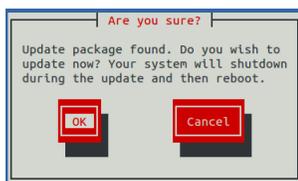
Updating appliance software

Before performing this procedure, attach the update ISO file to the Control Center host. For more information, see [Attaching an update ISO with vSphere](#).

This option updates the Control Center and Cisco UCS Performance Manager software on a host.

Note The upgrade software creates a complete record of its work. The file name is `/tmp/upgrade-ucspm-TimeStamp.log`. To preserve the file, copy it from `/tmp` to different location before stopping or restarting the virtual machine.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as [PuTTY](#).
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, use the down arrow key to select **Update System**, and then press the **Return** key.



- To cancel the update, press the **Tab** key, and then press the **Return** key.

Result: The **Appliance Administration** menu returns to the top level.

- To update the system, press the **Return** key.

Result: The **Appliance Administration** menu is replaced by progress messages as the upgrade process begins.

On success, the following message is displayed:

```
Script done, file is /var/log/serviced/script-2016-08-03-190832-root.log
Looking up service UCSPM
Service UCSPM has version
Set new version 2.0.2
Saving new version of UCSPM
Updated ucspm.
Restarting ucspm...
Restarted ucspm.
ucspm upgraded successfully.
```

In addition, the **Appliance Administration** menu returns to the top level.

On failure, one of the following messages is displayed:

```
Failed to stop all ucspm services.
Upgrade failed. Press any key to return.

Failed to stop serviced.
Upgrade failed. Press any key to return.

Failed to restart serviced.
Upgrade failed. Press any key to return.

Failed to upgrade serviced binary.
Upgrade failed. Press any key to return.

Error upgrading ucspm.
You may need to remove one or more preupgrade snapshots before retrying
this upgrade.
Upgrade failed. Press any key to return.
```

Contact Cisco Support before proceeding.

Updating the master host

Perform each procedure in this section on the Control Center master host.

Attaching an update ISO with vSphere

To perform this task, you need:

- A VMware vSphere client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

This procedure attaches a Cisco UCS Performance Manager update ISO file to the CD/DVD drive of the Control Center host.

- 1 Download the Cisco UCS Performance Manager update ISO file from the [Cisco UCS Performance Manager](#) site to your workstation.
- 2 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges.
- 3 With the **View** menu, enable **Toolbar** and **Show VMs in Inventory**.
- 4 In the **Inventory** list, select the name of the Control Center host.
- 5 Enable the CD/DVD drive of the Control Center master host.
 - a On the **Summary** page, click **Edit Settings**.
 - b In the **Hardware** table of the **Virtual Machine Properties** dialog, select **CD/DVD drive 1**.

- c In the **Device Type** area, click **Client Device**.
 - d At the bottom of the **Virtual Machine Properties** dialog, click **OK**.
- 6 Attach the update ISO file to the the Control Center master host.
- a In the toolbar, click the CD/DVD drive icon.
 - b From the menu, select **CD/DVD drive 1 > Connect to ISO image on local disk...**
 - c In the **Open** dialog, select the update ISO file, and then click the **Open** button.

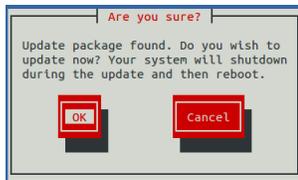
Updating appliance software

Before performing this procedure, attach the update ISO file to the Control Center host. For more information, see [Attaching an update ISO with vSphere](#).

This option updates the Control Center and Cisco UCS Performance Manager software on a host.

Note The upgrade software creates a complete record of its work. The file name is `/tmp/upgrade-ucspm-TimeStamp.log`. To preserve the file, copy it from `/tmp` to different location before stopping or restarting the virtual machine.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, use the down arrow key to select **Update System**, and then press the **Return** key.



- To cancel the update, press the **Tab** key, and then press the **Return** key.

Result: The **Appliance Administration** menu returns to the top level.

- To update the system, press the **Return** key.

Result: The **Appliance Administration** menu is replaced by progress messages as the upgrade process begins.

On success, the following message is displayed:

```
Script done, file is /var/log/serviced/script-2016-08-03-190832-root.log
Looking up service UCSPM
Service UCSPM has version
Set new version 2.0.2
Saving new version of UCSPM
Updated ucspm.
Restarting ucspm...
Restarted ucspm.
ucspm upgraded successfully.
```

In addition, the **Appliance Administration** menu returns to the top level.

On failure, one of the following messages is displayed:

```
Failed to stop all ucspm services.
Upgrade failed. Press any key to return.
```

```

Failed to stop serviced.
Upgrade failed. Press any key to return.

Failed to restart serviced.
Upgrade failed. Press any key to return.

Failed to upgrade serviced binary.
Upgrade failed. Press any key to return.

Error upgrading ucspm.
You may need to remove one or more preupgrade snapshots before retrying
this upgrade.
Upgrade failed. Press any key to return.

```

Contact Cisco Support before proceeding.

Updating a ZooKeeper cluster

Control Center relies on *Apache ZooKeeper* to keep its services in sync. The procedures in this section update your ZooKeeper cluster on the master host and two agent hosts.

One of the agent hosts is not used in the cluster. ZooKeeper requires an odd number of hosts in a cluster, and the Control Center master host is always a member. You may choose any two of the three agent hosts to participate in the cluster.

Note The Control Center configuration file of the host that is not a member of the ZooKeeper cluster must be updated, even though it is not in the cluster. The required procedure is included in this section.

Updating the ZooKeeper configuration on the master host

Use this procedure to update the ZooKeeper configuration on the master host.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as **root**.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Remove the existing ZooKeeper variables from the Control Center configuration file.

```

sed -i.bak -e '/SERVICED_ISVCS_ZOOKEEPER_ID/d' \
-e '/SERVICED_ISVCS_ZOOKEEPER_QUORUM/d' \
-e '/SERVICED_ZK/d' \
/etc/default/serviced

```

- 4 Create a variable for each node in the ZooKeeper cluster.

The variables are used in subsequent steps.

Note Define these variables identically on the master host and on each agent host in the ZooKeeper cluster.

Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

Note ZooKeeper requires IP addresses for cluster configuration.

- 5 Set the ID of this node in the ZooKeeper cluster to 1.

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=1" >> /etc/default/serviced
```

- 6 Specify the hosts in the ZooKeeper ensemble.
You may copy the following text from this document and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 7 Specify the hosts in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its cluster. To achieve this, replace the IP address of the master host with 0.0.0.0.

You may copy the following of text and paste it in your console:

```
q1="1@0.0.0.0:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

- 8 Verify the ZooKeeper environment variables.

```
egrep '^[^#]*SERVICED' /etc/default/serviced | egrep '_Z(OO|K)'
```

Updating the ZooKeeper configuration on the agent hosts

Use this procedure to update the ZooKeeper configuration on an agent host. Repeat this procedure on each Control Center agent host in the ZooKeeper cluster.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as **root**.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Remove the existing ZooKeeper variables from the Control Center configuration file.

```
sed -i.bak -e '/SERVICED_ISVCS_START/d' \
-e '/SERVICED_ISVCS_ZOOKEEPER_ID/d' \
-e '/SERVICED_ISVCS_ZOOKEEPER_QUORUM/d' \
-e '/SERVICED_ZK/d' \
/etc/default/serviced
```

- 4 Create a variable for each node in the ZooKeeper cluster.

The variables are used in subsequent steps.

Note Define these variables identically on the master host and on each agent host in the ZooKeeper cluster.

Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

Note ZooKeeper requires IP addresses for cluster configuration.

- 5 Set the ZooKeeper start flag.

```
echo "SERVICED_ISVCS_START=zookeeper" >> /etc/default/serviced
```

- 6 Set the ID of this node in the ZooKeeper cluster .

For *Agent-Host-A-IP* (node2), use the following command:

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=2" >> /etc/default/serviced
```

For *Agent-Host-B-IP* (node3), use the following command:

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=3" >> /etc/default/serviced
```

- 7 Specify the hosts in the ZooKeeper ensemble.

You may copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 8 Specify the hosts in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its cluster. To achieve this, replace the IP address of the current node with 0.0.0.0.

For *Agent-Host-A-IP* (node2), use the following command:

```
q1="1@${node1}:2888:3888"
q2="2@0.0.0.0:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

For *Agent-Host-B-IP* (node3), use the following command:

```
q1="1@${node1}:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@0.0.0.0:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

- 9 Configure ZooKeeper to start on the agent hosts.

```
echo "SERVICED_ISVCS_START=zookeeper" >> /etc/default/serviced
```

- 10 Verify the ZooKeeper environment variables.

```
egrep '^[^#]*SERVICED' /etc/default/serviced \
| egrep '(CS_ZO|_ZK|CS_ST)'
```

Starting a ZooKeeper cluster

Use this procedure to start a ZooKeeper cluster.

The window of time for starting a ZooKeeper ensemble is relatively short. The goal of this procedure is to restart Control Center on each ensemble node at about the same time, so that each node can participate in electing the leader.

- 1 Log in to the Control Center master host.
- 2 In a separate window, log in to the second node of the ZooKeeper ensemble (*Agent-Host-A-IP*).
- 3 In another separate window, log in to the third node of the ZooKeeper ensemble (*Agent-Host-B-IP*).
- 4 On the master host, stop and start `serviced`.

```
systemctl stop serviced && systemctl start serviced
```

- 5 On both resource pool hosts, stop and start `serviced`.

```
systemctl stop serviced && systemctl start serviced
```

- 6 On the master host, check the status of the ZooKeeper cluster.

```
{ echo stats; sleep 1; } | nc localhost 2181 | grep Mode
      { echo stats; sleep 1; } | nc Pool-Host-A-IP 2181 | grep
Mode
      { echo stats; sleep 1; } | nc Pool-Host-B-IP 2181 | grep
Mode
```

Updating the agent host that is not in the ZooKeeper cluster

The Control Center configuration file of the host that is not a member of the ZooKeeper cluster must be updated, even though it is not in the cluster. Use this procedure to update the configuration file.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Remove the existing ZooKeeper variable from the Control Center configuration file.

```
sed -i.bak -e '/SERVICED_ZK/d' /etc/default/serviced
```

- 4 Create a variable for each node in the ZooKeeper cluster.

Note Use the same variable declarations that you used on the hosts in the ZooKeeper cluster. Do not use the IP address of the current node.

Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

- Specify the hosts in the ZooKeeper ensemble.
You may copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- Verify the setting.

```
egrep '^[^#]*SERVICED_ZK' /etc/default/serviced
```

- Restart the Control Center daemon.

```
systemctl stop serviced && systemctl start serviced
```

Starting Cisco UCS Performance Manager

Use this procedure to start Cisco UCS Performance Manager and verify the upgrade.

- Display the login page of the Control Center browser interface.
Replace *HostName* with the name or IP address of the Control Center master host:

```
https://HostName
```

- Log in as ccuser.

Application	Description	Status	Deployment ID	Resource Pool	Virtual Host Names	Actions
Internal Services	Internal Services	Internal	N/A	N/A	N/A	
ucspm.uc.s.0	Cisco UCS Performance Manager	Test	default			Start Stop Delete

Application Template	ID	Description	Application Template
ucspm.uc.s.1	5a627c312a8903d8ee7d75a681b05f84	Cisco UCS Performance Manager	Delete
ucspm.uc.s.0	8f46c7f71bd1e1e829d2116d0008a850	Cisco UCS Performance Manager	Delete

The **Applications** table shows the updated application, and the **Application Templates** table includes the old and new templates.

Note Do not attempt to add either the old or the new application template. The new template is already added and deployed.

- In the **Actions** column of the **Applications** table, click the **Start** control of **ucspm**.
- In the **Start Service** dialog, click **Start Service and 46 Children**.

Upgrading Cisco UCS Performance Manager on Hyper-V systems

11

This appendix describes how to upgrade Cisco UCS Performance Manager on Hyper-V systems.

Note Cisco strongly recommends checking the integrity of Cisco UCS Performance Manager databases before performing an upgrade. For more information, see [Using Zenoss Toolbox](#) on page 136. In addition, Cisco strongly recommends creating a backup before performing an upgrade. Backups can be created with the Control Center backup feature or with the Hyper-V backup feature. However, before using the Hyper-V backup feature, Cisco UCS Performance Manager, Control Center, and the Control Center master host must be shut down cleanly and completely. For more information, see [Shutting down a Control Center master host](#) on page 115.

The upgrade steps depends on the deployment type, as outlined in the following table.

Single-host deployments	Multi-host deployments
<ol style="list-style-type: none"> 1 Prepare to upgrade Cisco UCS Performance Manager. 2 Attach the upgrade ISO to the Cisco UCS Performance Manager virtual machine. 3 Stop Cisco UCS Performance Manager. 4 Perform the upgrade. 5 Start Cisco UCS Performance Manager. 	<ol style="list-style-type: none"> 1 Prepare to upgrade Cisco UCS Performance Manager. 2 On the master host, stop Cisco UCS Performance Manager, and then stop Control Center. 3 On each agent host: <ol style="list-style-type: none"> a Attach the upgrade ISO to the virtual machine. b Perform the upgrade. 4 On the master host, attach the upgrade ISO. 5 Perform the upgrade. 6 Start Cisco UCS Performance Manager.

For optimum results, Cisco recommends reviewing the upgrade procedures before performing the upgrade.

Note The procedures in this appendix are deployment-specific. That is, the procedures only upgrade a single-host deployment to a single-host deployment and likewise for multi-host deployments. To change your deployment type from single-host to multi-host, first follow the instructions for upgrading a single-host deployment, and then follow the instructions in [Creating a multi-host deployment](#) on page 34.

All upgrades of Cisco UCS Performance Manager include an upgrade of the virtual machine operating system. The upgrades include a new kernel version, which fixes an `fstrim` bug.

Upgrading single-host deployments

To upgrade a single-host deployment, perform each procedure in this section.

Preparing to upgrade

Perform this procedure before upgrading your deployment.

- 1 Verify that Cisco UCS Performance Manager is operating normally.
 - a Log in to the Control Center browser interface as `ccuser`.
 - b In the **Application** column of the **Applications** table, click `ucspm`.
 - c Verify that all of the services in the **IP Assignments** table have valid IP addresses.
 - d Scroll down to the **Services** table, and then verify that none of the child services have failing health checks.
- 2 Check the integrity of Cisco UCS Performance Manager databases.
For more information, see [Using Zenoss Toolbox](#) on page 136.
- 3 Create a backup of Cisco UCS Performance Manager.
Backups can be created with the Control Center backup feature or with the backup feature of your hypervisor.

Note Before using the hypervisor backup feature, Cisco UCS Performance Manager, Control Center, and the Control Center master host must be shut down cleanly and completely. For more information, see [Shutting down a Control Center master host](#) on page 115.

Attaching an update ISO with Hyper-V

To perform this task, you need:

- A Microsoft Remote Desktop client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

This procedure attaches an Cisco UCS Performance Manager update ISO file to the CD/DVD drive of the Control Center host.

- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Download the Cisco UCS Performance Manager update ISO file from the [Cisco UCS Performance Manager](#) site to the Hyper-V host.
- 3 Start **Hyper-V Manager**.
- 4 In the **Virtual Machines** area of Hyper-V Manager, select the Control Center host, and then right-click to select **Settings...**
- 5 In the **Hardware** area of the **Settings** dialog, select **IDE Controller 1 > DVD Drive**.
- 6 In the **Media** area, click the **Image file** radio button, and then click **Browse...** button.
- 7 In the **Open** dialog, select the update ISO file, and then click the **Open** button.
- 8 At the bottom of the **Settings** dialog, click the **OK** button.

Stopping Cisco UCS Performance Manager

Use this procedure to stop Cisco UCS Performance Manager.

- 1 Log in to the Control Center browser interface as `ccuser`.

The screenshot shows the Cisco Control Center interface. At the top, there is a navigation bar with 'Applications' selected. Below the navigation bar, there are two tabs: 'Services Map' and 'Application'. The main content area is divided into two sections: 'Applications' and 'Application Templates'. The 'Applications' section contains a table with the following data:

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	Running	Internal	N/A	N/A	N/A
ucspm (v2.0.1)	Cisco UCS Performance Manager	Running	Test	default	https://ucspm.ucspm:50443 https://ucspm	Start Stop Delete

The 'Application Templates' section contains a table with the following data:

Application Template	ID	Description	Actions
ucspm (v2.0.1)	970566e6d1bbae54bc028d295a8b9d0e	Cisco UCS Performance Manager	Delete

- 2 In the **Actions** column of the **Applications** table, click the **Stop** control of **ucspm**.
- 3 In the **Stop Service** dialog, click **Stop Service and 46 Children**.

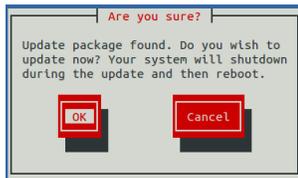
Updating appliance software

Before performing this procedure, attach the update ISO file to the Control Center host. For more information, see [Attaching an update ISO with Hyper-V](#).

This option updates the Control Center and Cisco UCS Performance Manager software on a host.

Note The upgrade software creates a complete record of its work. The file name is `/tmp/upgrade-ucspm-TimeStamp.log`. To preserve the file, copy it from `/tmp` to different location before stopping or restarting the virtual machine.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, use the down arrow key to select **Update System**, and then press the **Return** key.



- To cancel the update, press the **Tab** key, and then press the **Return** key.

Result: The **Appliance Administration** menu returns to the top level.

- To update the system, press the **Return** key.

Result: The **Appliance Administration** menu is replaced by progress messages as the operating system upgrade begins.

When the operating system upgrade completes, the following prompt displays:

```
Complete!
Serviced appears to be using a loopback thinpool device.
It is highly recommended that you migrate to an LVM device for
improved performance.

Press Escape to abort now, or any other key to continue.
```

If you choose to continue, additional progress messages are displayed as the upgrade process continues.

On success, the following message is displayed:

```
Script done, file is /var/log/serviced/script-2016-08-03-190832-root.log
Looking up service UCSPM
Service UCSPM has version
Set new version 2.0.2
Saving new version of UCSPM
Updated ucspm.
Restarting ucspm...
Restarted ucspm.
ucspm upgraded successfully.
```

In addition, the **Appliance Administration** menu returns to the top level.

On failure, one of the following messages is displayed:

```
Failed to stop all ucspm services.
Upgrade failed. Press any key to return.

Failed to stop serviced.
Upgrade failed. Press any key to return.

Failed to restart serviced.
Upgrade failed. Press any key to return.

Failed to upgrade serviced binary.
Upgrade failed. Press any key to return.

Error upgrading ucspm.
You may need to remove one or more preupgrade snapshots before retrying
this upgrade.
Upgrade failed. Press any key to return.
```

Contact Cisco Support before proceeding.

Starting Cisco UCS Performance Manager

Use this procedure to start Cisco UCS Performance Manager and verify the upgrade.

- 1 Display the login page of the Control Center browser interface.
Replace *HostName* with the name or IP address of the Control Center master host:

```
https://HostName
```

- 2 Log in as ccuser.

Application	Description	Status	Deployment ID	Resource Pool	Virtual Host Names	Actions
Internal Services	Internal Services	Running	Internal	ALL	ALL	
ucspm (v2.0.1)	Cisco UCS Performance Manager	Stopped	Test	default		Start Stop Delete

Application Template	ID	Description
ucspm (v2.0.1)	5ae627c5132e902dbee7475dc989b5f84	Cisco UCS Performance Manager
ucspm (v2.0.2)	8f6c7f77bd0e1e929d21b60008a050	Cisco UCS Performance Manager

The **Applications** table shows the updated application, and the **Application Templates** table includes the old and new templates.

Note Do not attempt to add either the old or the new application template. The new template is already added and deployed.

- 3 In the **Actions** column of the **Applications** table, click the **Start** control of **ucspm**.
- 4 In the **Start Service** dialog, click **Start Service and 46 Children**.

Upgrading multi-host deployments

To upgrade a multi-host deployment, perform each procedure in this section.

Preparing to upgrade

Perform this procedure before upgrading your deployment.

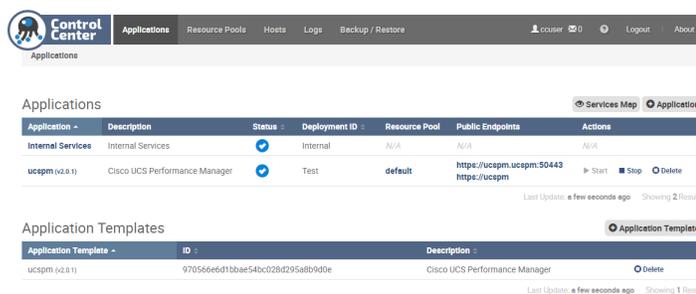
- 1 Verify that Cisco UCS Performance Manager is operating normally.
 - a Log in to the Control Center browser interface as `ccuser`.
 - b In the **Application** column of the **Applications** table, click **ucspm**.
 - c Verify that all of the services in the **IP Assignments** table have valid IP addresses.
 - d Scroll down to the **Services** table, and then verify that none of the child services have failing health checks.
- 2 Check the integrity of Cisco UCS Performance Manager databases.
For more information, see [Using Zenoss Toolbox](#) on page 136.
- 3 Create a backup of Cisco UCS Performance Manager.
Backups can be created with the Control Center backup feature or with the backup feature of your hypervisor.

Note Before using the hypervisor backup feature, Cisco UCS Performance Manager, Control Center, and the Control Center master host must be shut down cleanly and completely. For more information, see [Shutting down a Control Center master host](#) on page 115.

Stopping Cisco UCS Performance Manager and Control Center

Use this procedure to stop Cisco UCS Performance Manager and Control Center.

- 1 Log in to the Control Center browser interface as `ccuser`.



- 2 In the **Actions** column of the **Applications** table, click the **Stop** control of **ucspm**.
- 3 In the **Stop Service** dialog, click the **Stop Service and 47 Children** button.
- 4 Gain access to the Control Center master host, through the console interface of your hypervisor, or through a remote shell utility such as [PuTTY](#).
- 5 Log in as the `root` user.
- 6 Use the **Down Arrow** key to select **Root Shell**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 7 Stop the Control Center service.

```
systemctl stop serviced
```

Updating agent hosts

Repeat each procedure in this section on each agent host in your deployment.

Attaching an update ISO with Hyper-V

To perform this task, you need:

- A Microsoft Remote Desktop client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

This procedure attaches an Cisco UCS Performance Manager update ISO file to the CD/DVD drive of the Control Center host.

- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Download the Cisco UCS Performance Manager update ISO file from the [Cisco UCS Performance Manager](#) site to the Hyper-V host.
- 3 Start **Hyper-V Manager**.
- 4 In the **Virtual Machines** area of Hyper-V Manager, select the Control Center host, and then right-click to select **Settings...**
- 5 In the **Hardware** area of the **Settings** dialog, select **IDE Controller 1 > DVD Drive**.
- 6 In the **Media** area, click the **Image file** radio button, and then click **Browse...** button.
- 7 In the **Open** dialog, select the update ISO file, and then click the **Open** button.
- 8 At the bottom of the **Settings** dialog, click the **OK** button.

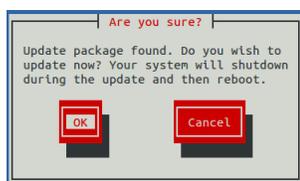
Updating appliance software

Before performing this procedure, attach the update ISO file to the Control Center host. For more information, see [Attaching an update ISO with Hyper-V](#).

This option updates the Control Center and Cisco UCS Performance Manager software on a host.

Note The upgrade software creates a complete record of its work. The file name is `/tmp/upgrade-ucspm-TimeStamp.log`. To preserve the file, copy it from `/tmp` to different location before stopping or restarting the virtual machine.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as [PuTTY](#).
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, use the down arrow key to select **Update System**, and then press the **Return** key.



- To cancel the update, press the **Tab** key, and then press the **Return** key.

Result: The **Appliance Administration** menu returns to the top level.

- To update the system, press the **Return** key.

Result: The **Appliance Administration** menu is replaced by progress messages as the operating system upgrade begins.

When the operating system upgrade completes, the following prompt displays:

```
Complete!
Serviced appears to be using a loopback thinpool device.
It is highly recommended that you migrate to an LVM device for
improved performance.

Press Escape to abort now, or any other key to continue.
```

If you choose to continue, additional progress messages are displayed as the upgrade process continues.

On success, the following message is displayed:

```
Script done, file is /var/log/serviced/script-2016-08-03-190832-root.log
Looking up service UCSPM
Service UCSPM has version
Set new version 2.0.2
Saving new version of UCSPM
Updated ucspm.
Restarting ucspm...
Restarted ucspm.
ucspm upgraded successfully.
```

In addition, the **Appliance Administration** menu returns to the top level.

On failure, one of the following messages is displayed:

```
Failed to stop all ucspm services.
Upgrade failed. Press any key to return.

Failed to stop serviced.
Upgrade failed. Press any key to return.

Failed to restart serviced.
Upgrade failed. Press any key to return.

Failed to upgrade serviced binary.
Upgrade failed. Press any key to return.

Error upgrading ucspm.
You may need to remove one or more preupgrade snapshots before retrying
this upgrade.
Upgrade failed. Press any key to return.
```

Contact Cisco Support before proceeding.

Updating the master host

Perform each procedure in this section on the Control Center master host.

Attaching an update ISO with Hyper-V

To perform this task, you need:

- A Microsoft Remote Desktop client
- Permission to download Cisco UCS Performance Manager software from the Cisco support site

This procedure attaches a Cisco UCS Performance Manager update ISO file to the CD/DVD drive of the Control Center host.

- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Download the Cisco UCS Performance Manager update ISO file from the [Cisco UCS Performance Manager](#) site to the Hyper-V host.
- 3 Start **Hyper-V Manager**.
- 4 In the **Virtual Machines** area of Hyper-V Manager, select the Control Center host, and then right-click to select **Settings....**
- 5 In the **Hardware** area of the **Settings** dialog, select **IDE Controller 1 > DVD Drive**.
- 6 In the **Media** area, click the **Image file** radio button, and then click **Browse...** button.
- 7 In the **Open** dialog, select the update ISO file, and then click the **Open** button.
- 8 At the bottom of the **Settings** dialog, click the **OK** button.

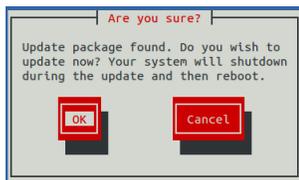
Updating appliance software

Before performing this procedure, attach the update ISO file to the Control Center host. For more information, see [Attaching an update ISO with Hyper-V](#).

This option updates the Control Center and Cisco UCS Performance Manager software on a host.

Note The upgrade software creates a complete record of its work. The file name is `/tmp/upgrade-ucspm-TimeStamp.log`. To preserve the file, copy it from `/tmp` to different location before stopping or restarting the virtual machine.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as [PuTTY](#).
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, use the down arrow key to select **Update System**, and then press the **Return** key.



- To cancel the update, press the **Tab** key, and then press the **Return** key.

Result: The **Appliance Administration** menu returns to the top level.

- To update the system, press the **Return** key.

Result: The **Appliance Administration** menu is replaced by progress messages as the operating system upgrade begins.

When the operating system upgrade completes, the following prompt displays:

```
Complete!
Serviced appears to be using a loopback thinpool device.
```

```
It is highly recommended that you migrate to an LVM device for
improved performance.
```

```
Press Escape to abort now, or any other key to continue.
```

If you choose to continue, additional progress messages are displayed as the upgrade process continues.

On success, the following message is displayed:

```
Script done, file is /var/log/serviced/script-2016-08-03-190832-root.log
Looking up service UCSPM
Service UCSPM has version
Set new version 2.0.2
Saving new version of UCSPM
Updated ucspm.
Restarting ucspm...
Restarted ucspm.
ucspm upgraded successfully.
```

In addition, the **Appliance Administration** menu returns to the top level.

On failure, one of the following messages is displayed:

```
Failed to stop all ucspm services.
Upgrade failed. Press any key to return.

Failed to stop serviced.
Upgrade failed. Press any key to return.

Failed to restart serviced.
Upgrade failed. Press any key to return.

Failed to upgrade serviced binary.
Upgrade failed. Press any key to return.

Error upgrading ucspm.
You may need to remove one or more preupgrade snapshots before retrying
this upgrade.
Upgrade failed. Press any key to return.
```

Contact Cisco Support before proceeding.

Updating a ZooKeeper cluster

Control Center relies on *Apache ZooKeeper* to keep its services in sync. The procedures in this section update your ZooKeeper cluster on the master host and two agent hosts.

One of the agent hosts is not used in the cluster. ZooKeeper requires an odd number of hosts in a cluster, and the Control Center master host is always a member. You may choose any two of the three agent hosts to participate in the cluster.

Note The Control Center configuration file of the host that is not a member of the ZooKeeper cluster must be updated, even though it is not in the cluster. The required procedure is included in this section.

Updating the ZooKeeper configuration on the master host

Use this procedure to update the ZooKeeper configuration on the master host.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Remove the existing ZooKeeper variables from the Control Center configuration file.

```
sed -i.bak -e '/SERVICED_ISVCS_ZOOKEEPER_ID/d' \
-e '/SERVICED_ISVCS_ZOOKEEPER_QUORUM/d' \
-e '/SERVICED_ZK/d' \
/etc/default/serviced
```

- 4 Create a variable for each node in the ZooKeeper cluster.

The variables are used in subsequent steps.

Note Define these variables identically on the master host and on each agent host in the ZooKeeper cluster.

Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

Note ZooKeeper requires IP addresses for cluster configuration.

- 5 Set the ID of this node in the ZooKeeper cluster to 1.

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=1" >> /etc/default/serviced
```

- 6 Specify the hosts in the ZooKeeper ensemble.

You may copy the following text from this document and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 7 Specify the hosts in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its cluster. To achieve this, replace the IP address of the master host with 0.0.0.0.

You may copy the following of text and paste it in your console:

```
q1="1@0.0.0.0:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

- 8 Verify the ZooKeeper environment variables.

```
egrep '^[^#]*SERVICED' /etc/default/serviced | egrep '_Z(OO|K)'
```

Updating the ZooKeeper configuration on the agent hosts

Use this procedure to update the ZooKeeper configuration on an agent host. Repeat this procedure on each Control Center agent host in the ZooKeeper cluster.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Remove the existing ZooKeeper variables from the Control Center configuration file.

```
sed -i.bak -e '/SERVICED_ISVCS_START/d' \
-e '/SERVICED_ISVCS_ZOOKEEPER_ID/d' \
-e '/SERVICED_ISVCS_ZOOKEEPER_QUORUM/d' \
-e '/SERVICED_ZK/d' \
/etc/default/serviced
```

- 4 Create a variable for each node in the ZooKeeper cluster.

The variables are used in subsequent steps.

Note Define these variables identically on the master host and on each agent host in the ZooKeeper cluster.

Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts to include in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

Note ZooKeeper requires IP addresses for cluster configuration.

- 5 Set the ZooKeeper start flag.

```
echo "SERVICED_ISVCS_START=zookeeper" >> /etc/default/serviced
```

- 6 Set the ID of this node in the ZooKeeper cluster.

For *Agent-Host-A-IP* (node2), use the following command:

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=2" >> /etc/default/serviced
```

For *Agent-Host-B-IP* (node3), use the following command:

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=3" >> /etc/default/serviced
```

- 7 Specify the hosts in the ZooKeeper ensemble.

You may copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 8 Specify the hosts in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its cluster. To achieve this, replace the IP address of the current node with 0.0.0.0.

For *Agent-Host-A-IP* (node2), use the following command:

```
q1="1@${node1}:2888:3888"
q2="2@0.0.0.0:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
  >> /etc/default/serviced
```

For *Agent-Host-B-IP* (node3), use the following command:

```
q1="1@${node1}:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@0.0.0.0:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
  >> /etc/default/serviced
```

- 9 Configure ZooKeeper to start on the agent hosts.

```
echo "SERVICED_ISVCS_START=zookeeper" >> /etc/default/serviced
```

- 10 Verify the ZooKeeper environment variables.

```
egrep '^[^#]*SERVICED' /etc/default/serviced \
  | egrep '(CS_ZO|_ZK|CS_ST)'
```

Starting a ZooKeeper cluster

Use this procedure to start a ZooKeeper cluster.

The window of time for starting a ZooKeeper ensemble is relatively short. The goal of this procedure is to restart Control Center on each ensemble node at about the same time, so that each node can participate in electing the leader.

- 1 Log in to the Control Center master host.
- 2 In a separate window, log in to the second node of the ZooKeeper ensemble (*Agent-Host-A-IP*).
- 3 In another separate window, log in to the third node of the ZooKeeper ensemble (*Agent-Host-B-IP*).
- 4 On the master host, stop and start serviced.

```
systemctl stop serviced && systemctl start serviced
```

- 5 On both resource pool hosts, stop and start serviced.

```
systemctl stop serviced && systemctl start serviced
```

- 6 On the master host, check the status of the ZooKeeper cluster.

```
{ echo stats; sleep 1; } | nc localhost 2181 | grep Mode
Mode
{ echo stats; sleep 1; } | nc Pool-Host-A-IP 2181 | grep
Mode
{ echo stats; sleep 1; } | nc Pool-Host-B-IP 2181 | grep
Mode
```

Updating the agent host that is not in the ZooKeeper cluster

The Control Center configuration file of the host that is not a member of the ZooKeeper cluster must be updated, even though it is not in the cluster. Use this procedure to update the configuration file.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Remove the existing ZooKeeper variable from the Control Center configuration file.

```
sed -i.bak -e '/SERVICED_ZK/d' /etc/default/serviced
```

- 4 Create a variable for each node in the ZooKeeper cluster.

Note Use the same variable declarations that you used on the hosts in the ZooKeeper cluster. Do not use the IP address of the current node.

Replace *Master-Host-IP* with the IP address of the Control Center master host, and replace *Agent-Host-A-IP* and *Agent-Host-B-IP* with the IP addresses of the agent hosts in the cluster:

```
node1=Master-Host-IP
node2=Agent-Host-A-IP
node3=Agent-Host-B-IP
```

- 5 Specify the hosts in the ZooKeeper ensemble.

You may copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 6 Verify the setting.

```
egrep '^[^#]*SERVICED_ZK' /etc/default/serviced
```

- 7 Restart the Control Center daemon.

```
systemctl stop serviced && systemctl start serviced
```

Starting Cisco UCS Performance Manager

Use this procedure to start Cisco UCS Performance Manager and verify the upgrade.

- 1 Display the login page of the Control Center browser interface.

Replace *HostName* with the name or IP address of the Control Center master host:

```
https://HostName
```

- 2 Log in as `ccuser`.

The screenshot shows the Control Center interface with two tables. The 'Applications' table has columns for Application, Description, Status, Deployment ID, Resource Pool, Virtual Host Names, and Actions. The 'Application Templates' table has columns for Application Template, ID, and Description.

Application	Description	Status	Deployment ID	Resource Pool	Virtual Host Names	Actions
Internal Services	Internal Services	Running	Internal	N/A	N/A	
ucspm (v.s.1)	Cisco UCS Performance Manager	Stopped	Test	default		Start Stop Delete

Application Template	ID	Description	Actions
ucspm (v.s.1)	5ae627c3112ab902d0ee77f15ad88db5f84	Cisco UCS Performance Manager	Delete
ucspm (v.s.0)	8fa6c7771bd8e1ea929d218d0008a8950	Cisco UCS Performance Manager	Delete

The **Applications** table shows the updated application, and the **Application Templates** table includes the old and new templates.

Note Do not attempt to add either the old or the new application template. The new template is already added and deployed.

- 3 In the **Actions** column of the **Applications** table, click the **Start** control of **ucspm**.
- 4 In the **Start Service** dialog, click **Start Service and 46 Children**.

Managing Cisco UCS Performance Manager with Control Center

A

This appendix describes how to use the Control Center browser interface to start and stop Cisco UCS Performance Manager. For more information about getting started with Cisco UCS Performance Manager, see the *Cisco UCS Performance Manager Getting Started Guide*.

Note If you completed migration, Cisco UCS Performance Manager is already started. You may proceed to the *Cisco UCS Performance Manager Getting Started Guide*.

Starting Cisco UCS Performance Manager

- 1 Display the login page of the Control Center browser interface.
Replace *HostName* with the hostname or IP address of the Control Center master host.

```
https://HostName:50443
```

Note The web server that listens for Control Center interface requests typically takes 1-2 minutes to start, after the the Control Center master host is powered on.

- 2 At the login page, enter `ccuser` and its password.

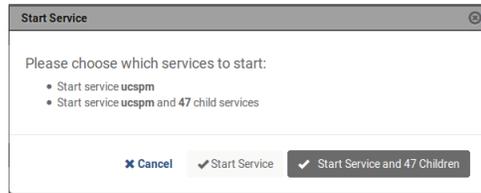
Figure 45: Landing page

The screenshot shows the Cisco Control Center interface. The top navigation bar includes 'Applications', 'Resource Pools', 'Hosts', 'Logs', and 'Backup / Restore'. The user 'ccuser' is logged in. The main content area is titled 'Applications' and contains a table with the following data:

Application	Description	Status	Deployment ID	Resource Pool	Public Endpoints	Actions
Internal Services	Internal Services	✓	Internal	N/A	N/A	N/A
ucspm (v2.0)	Cisco UCS Performance Manager	⊖	Test	default	https://ucspm.cc-master:50443 https://cc-master	▶ Start Stop Delete

Below the Applications table is the 'Application Templates' section, which contains one row for 'ucspm (v2.0)' with ID '59f1337508ecf73bd27c2283694f2ce5' and description 'Cisco UCS Performance Manager'.

- 3 In the **Actions** column of the **Applications** table, click the **Start** control of the **ucspm** row.

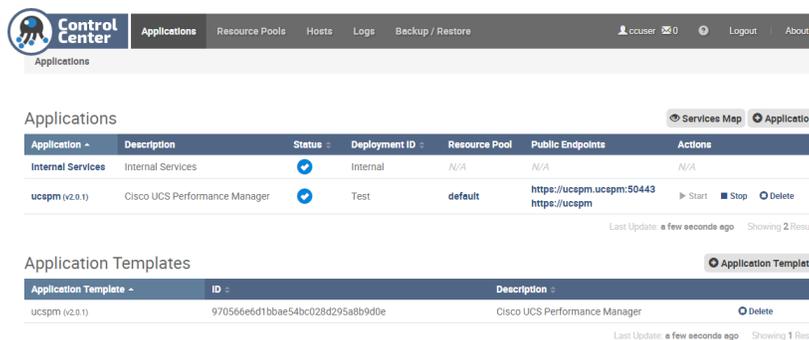
Figure 46: Start Service dialog

- 4 In the **Start Service** dialog, click **Start Service and 47 Children** button.
- 5 In the **Application** column of the **Applications** table, click **ucspm** in the **ucspm** row.
- 6 Scroll down to watch child services starting.
Typically, child services take 4-5 minutes to start. When no child service shows a red exclamation point icon, Cisco UCS Performance Manager is running.
- 7 Optional: Log in to the Cisco UCS Performance Manager interface, if desired.
 - a Scroll to the **Virtual Host Names** table.
 - b In the **URL** column, click the link of the last entry, which starts with **ucspm**.

Shutting down a Control Center master host

Control Center is a distributed system that relies on the system clock (and NTP) to coordinate Cisco UCS Performance Manager services. Consequently, pausing or stopping the Control Center master host can leave Cisco UCS Performance Manager in an unknown state, which requires manual intervention to repair. Cisco strongly recommends following this procedure to stop Cisco UCS Performance Manager, before pausing or stopping the master host.

- 1 Log in to the Control Center browser interface as `ccuser`.



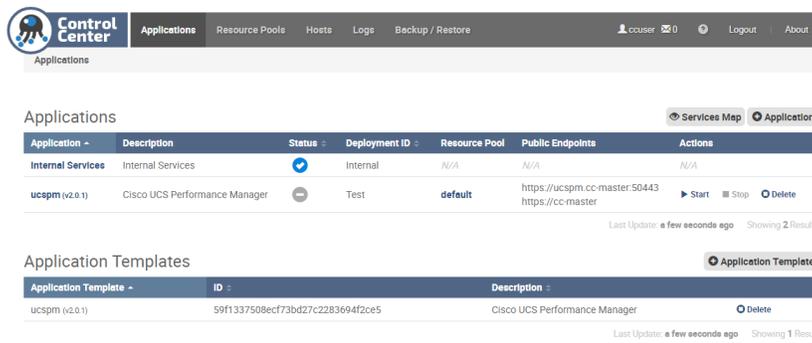
- 2 In the **Actions** column of the **Applications** table, click the **Stop** control of **ucspm**.
- 3 In the **Stop Service** dialog, click the **Stop Service and 47 Children** button.
- 4 Log out of the Control Center browser interface.
- 5 Use the normal hypervisor controls to shut down the Cisco UCS Performance Manager master host.

Removing migration software

This procedure removes the ZenPacks.zenoss.Import4 ZenPack from Cisco UCS Performance Manager, and removes the Imp4MariaDB and Imp4OpenTSDB services from Control Center.

If you plan to migrate data from a Cisco UCS Performance Manager version 1.1.x system, do not perform this procedure. Instead, proceed to the *Cisco UCS Performance Manager Migration Guide*.

- 1 Log in to the Control Center browser interface.



- 2 In the **Applications** table, click the name of the application to modify.
The name to click is **ucspm**.
- 3 Stop the **Imp4MariaDB** and **Imp4OpenTSDB** services, if necessary.
 - a Scroll down to the **Services** table, and then locate the **Imp4MariaDB** and **Imp4OpenTSDB** services.
The services are located in the **Infrastructure** hierarchy.
 - b In the **Actions** column, click the **Stop** control of the **Imp4MariaDB** and **Imp4OpenTSDB** services.
Stopped services have a grey circle icon in the **Instances** column.
- 4 Stop the services in the **Zenoss** hierarchy, and then verify that the services are stopped.
 - a In the **Services** table, scroll down to **Zenoss**.
 - b In the **Actions** column, click the **Stop** control of the **Zenoss** hierarchy.
 - c In the **Service** column, click **Zenoss**, and then scroll down.
Stopped services have a grey circle icon in the **Instances** column.
- 5 Create a snapshot.
 - a Log in to the Control Center master host as **root** or **ccuser**.
 - b Create a snapshot.

```
serviced service snapshot ucspm
```

The `serviced` command returns the ID of the new snapshot on completion.

- 6 Restart the **zeneventserver** and **Zope** services.
To restart the services with the CLI, enter the following command for each child service. Replace *Name* with the name of the service to start:

```
serviced service start Name
```

To restart the services with the browser interface, perform the following substeps:

- a Click the **Zenoss** service to expand its child services.
- b Scroll down to the **zeneventserver** service.
- c In the **Actions** column, click the **Start** control of the **zeneventserver** service.
- d Scroll down to the **Zope** service.
- e In the **Actions** column, click the **Start** control of the **Zope** service.

In the **Services** table, the Failing icon (a red circle with an exclamation point) in the **Status** column represents the cumulative result of one or more customized health checks. To view the status of individual health checks, move the pointer over the icon, which displays a pop-up.

When all of the health checks of the required services are passing, proceed to the next step.

- 7 Disable and stop the `import4` service.

```
systemctl disable import4 && systemctl stop import4
```

- 8 Remove the ZenPacks.zenoss.Import4 ZenPack.

```
serviced service run zope zenpack-manager \  
  uninstall ZenPacks.zenoss.Import4
```

- 9 Remove the **Imp4MariaDB** and **Imp4OpenTSDB** services.

```
serviced service rm Imp4MariaDB  
serviced service rm Imp4OpenTSDB
```

- 10 Refresh the Control Center browser interface, and then start the services in the **Zenoss** hierarchy.
 - a Select the window of the Control Center browser interface, and then press the **F5** key.
The **Imp4MariaDB** and **Imp4OpenTSDB** services remain in the Control Center browser interface until the window is refreshed, even though they are removed.
 - b In the **Actions** column of the **Zenoss** hierarchy, click the **Restart** control.

Adding storage to a Control Center master host

B

This appendix describes how to add storage to a Control Center master host for data collection.

The procedures in this appendix may be performed only after a Control Center master host is installed. Cisco UCS Performance Manager does not need to be stopped during this process.

Identifying block storage devices

Use this procedure to identify the block storage devices that are attached to the Control Center master host.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Display the block storage attached to the host.

```
lsblk -pdo NAME,HCTL,SIZE
```

Example output:

NAME	HCTL	SIZE
/dev/sda	2:0:0:0	293G
/dev/sr0	1:0:0:0	1024M

The example output shows two devices:

- One disk drive (/dev/sda)
- One CD-ROM drive (/dev/sr0)

Perform one of the following procedures:

- [Creating a virtual disk with vSphere](#) on page 119
- [Creating a virtual disk with Hyper-V](#) on page 119

Creating a virtual disk with vSphere

To perform this task, you need a VMware vSphere client.

- 1 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home > Inventory > Inventory** view.
- 2 In the left column, right-click on the Control Center master host virtual machine, and then select **Edit Settings...**
- 3 On the **Hardware** tab, click the **Add...** button.
- 4 In the **Add Hardware** dialog, select **Hard Disk**, and then click the **Next** button.
- 5 In the **Select a Disk** pane, click the **Create a new virtual disk** radio button, and then click the **Next** button.
- 6 In the **Create a Disk** pane, configure the virtual disk.
 - a In the **Capacity** area, set the disk size.
For backup storage, Cisco recommends 300GB. For data collection storage, Cisco recommends 150GB.
 - b In the **Disk Provisioning** area, choose the option you prefer.
 - c In the **Location** area, choose the option you prefer.
 - d Click the **Next** button.
- 7 In the **Advanced Options** pane, configure the mode.
 - a In the **Mode** area, check the **Independent** check box.
 - b Click the **Persistent** radio button.
 - c Click the **Next** button.
- 8 In the **Ready to Complete** pane, confirm the virtual disk configuration, and then click the **Finish** button.
- 9 At the bottom of the **Virtual Machine Properties** dialog, click the **OK** button.

Creating a virtual disk with Hyper-V

To perform this task, you need:

- A Microsoft Remote Desktop client
- Administrator privileges on a Microsoft Hyper-V server

- 1 Use a Microsoft Remote Desktop client to log in to a Hyper-V host as Administrator, or as a user with Administrator privileges.
- 2 Start **Hyper-V Manager**.
- 3 In the left column, select the server that is hosting the Control Center master host, and then right-click to select **New > Hard Disk...**
- 4 In the **New Virtual Hard Disk Wizard** dialog, navigate to the **Choose Disk Format** panel.
- 5 Click the **VHDX** radio button, and then click the **Next** button.
- 6 In the **Choose Disk Type** panel, click the **Dynamically expanding** radio button, and then click the **Next** button.
- 7 In the **Specify Name and Location** panel, enter a name for the disk in the **Name** field, and then click the **Next** button.
- 8 In the **Configure Disk** panel, click the **Create a new blank virtual hard disk** radio button, enter the disk size in the **Size** field, and then click the **Next** button.
For backup storage, Cisco recommends 300GB. For data collection storage, Cisco recommends 150GB.
- 9 In the **Summary** panel, review the virtual disk settings, and then click the **Finish** button.
- 10 In **Hyper-V Manager**, right-click the virtual machine of the Control Center master host, and then select **Settings...**
- 11 In the **Settings** dialog, select **SCSI Controller** from the **Hardware** list in the left column.
- 12 In the **SCSI Controller** area on the right side, select **Hard Drive**, and then click the **Add** button.
- 13 In the **Hard Drive** area, click the **Virtual hard disk** radio button, and then click the **Browse** button.
- 14 In the **Open** dialog, select the hard disk image created previously, and then click the **Open** button.

- 15 In the **Settings** dialog, click the **OK** button.

Identifying new block storage devices

Use this procedure to identify the new block storage device that is attached to the Control Center master host.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Start a command-line session as `root`.
 - a In the **Appliance Administration** menu, use the down-arrow key to select **Root Shell**.
 - b Press the **Tab** key to select **Run**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm ~]#
```

- 3 Rescan all SCSI storage.

```
for h in $(ls /sys/class/scsi_host)
do
  echo "--" > /sys/class/scsi_host/${h}/scan
done
```

- 4 Display the block storage attached to the host.

```
lsblk -pdo NAME,HCTL,SIZE
```

Example output:

NAME	HCTL	SIZE
/dev/sda	2:0:0:0	293G
/dev/sdb	2:0:1:0	300G
/dev/sr0	1:0:0:0	1024M

The example output shows a new drive, `/dev/sdb`. The new drive may be different on your host. Compare this output with the output of the same command before adding a device.

Preparing a device for data collection storage

This procedure prepares a storage device as a device mapper thin pool on a Control Center master host and adds it to the thin pool for applications. The storage can be used for application data or for snapshots.

- 1 Identify the current size of the thin pool for applications.

```
lvs -o lv_size serviced
```

Example result:

```
LSize
150.04g
```

In this example, the current size is 150GB. Record the size for use in a subsequent step.

- 2 Identify the device to prepare, and record its size.

Replace *Device* with the virtual disk added previously:

```
lsblk -p --output=NAME,SIZE,TYPE,MOUNTPOINT Device
```

Example output:

```
NAME          SIZE TYPE MOUNTPOINT
/dev/sdc      150G disk
```

In this example, the device to prepare is `/dev/sdc`, it is not mounted in the filesystem, and its size is 150GB. Record the size for use in a subsequent step.

3 Create a new physical volume.

Replace *Device* with the device identified previously:

```
pvcreate Device
```

On success, the `pvcreate` command displays the name of the new physical volume, which is the same name as the device.

4 Extend the volume group used for applications, `serviced`.

Replace *Physical-Volume* with the name of the physical volume created in the previous step:

```
vgextend serviced Physical-Volume
```

5 Add space to the thin pool for applications with the updated volume group.

Replace *New-Space* with the size of the partition, identified in the second step. Be sure to include the units ("G" for gigabytes):

```
lvextend -L+New-SpaceG serviced/serviced-pool
```

The `lvextend` command extends both the data and metadata areas of the thin pool.

6 Optional: Add storage space for application data.

The preceding steps expand the amount of storage available for snapshots. To use the additional storage for application data, perform this step.

- a** Add the size of the application data storage area, identified in the first step, to the size of the new partition, identified in the second step.
- b** Display the Control Center tenant ID.

```
ls /opt/serviced/var/volumes
```

Example result:

```
dovygh6m2gz4zgdzxb2ud70g9
```

c Update Control Center.

Replace *Tenant-ID* with the identifier displayed in the previous substep, and replace *Total-Space* with the total amount of application data storage space. Be sure to include the units ("G" for gigabytes):

```
serviced-storage resize -d /opt/serviced/var/volumes \
-o dm.thinpooldev=/dev/mapper/serviced-serviced--pool \
Tenant-ID Total-SpaceG
```

C

Using the Appliance Administration menu

This appendix describes the curses-based Appliance Administration menu, a text user interface (TUI).

Configure Network and DNS

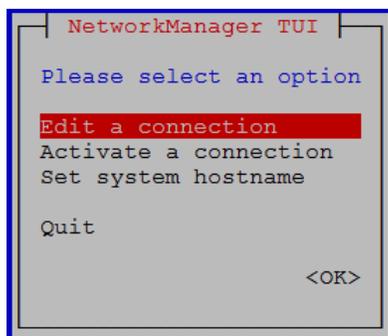
The **Configure Network and DNS** option invokes `nmtui`, the *NetworkManager* text user interface (TUI) tool. The `nmtui` utility provides submenus for editing and activating network connections, and for changing the hostname.

Note Cisco recommends using only the **Configure Network and DNS** option to change connection properties or the hostname, and always rebooting after making changes.

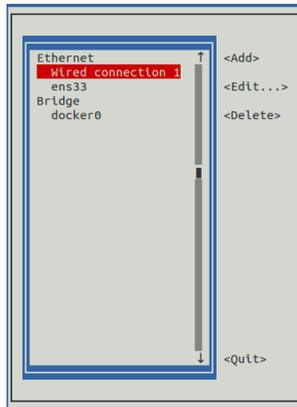
Edit a connection

The default configuration for network connections is DHCP. To configure static IPv4 addressing, perform this procedure.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.
 - b Press the **Tab** key to select the **Run** button.
 - c Press the **Enter** key.

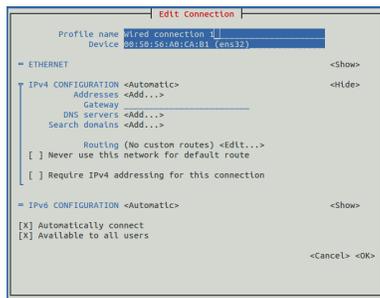


- 4 On the **NetworkManager TUI** menu, select **Edit a connection**, and then press the **Return** key. The TUI displays the connections that are available on this host.

Figure 47: Example: Available connections

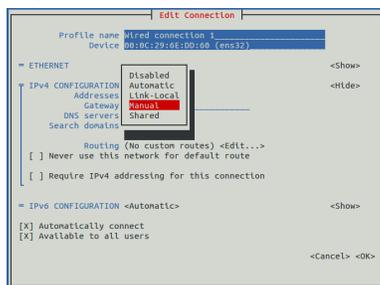
- 5 Use the down-arrow key to select **Wired Connection 1**, and then press the **Return** key.

Note Do not use the TUI to edit the `docker0` connection. For more information, see [Configuring the Docker virtual bridge](#) on page 132.

Figure 48: Example: Edit Connection screen

Use the **Tab** key and the arrow keys to navigate among options in the **Edit Connection** screen, and use the **Return** key to toggle an option or to display a menu of options.

- 6 Optional: If the **IPv4 CONFIGURATION** area is not visible, select its display option (**<Show>**), and then press the **Return** key.
- 7 In the **IPv4 CONFIGURATION** area, select **<Automatic>**, and then press the **Return** key.

Figure 49: Example: IPv4 Configuration options

- 8 In the submenu, use the down-arrow key to select **Manual**, and then press the **Return** key.

Note For static networking, the option next to **IPv4 CONFIGURATION** must be **Manual**. If it is **Automatic**, the host uses an address from a DHCP server.

- 9 Enter an IPv4 address in CIDR notation.

- a Use the **Tab** key or the down arrow key to select the **<Add...>** option next to **Addresses**, and then press the **Return** key.
 - b In the **Addresses** field, enter an IPv4 address, followed by the solidus character (/) and then the prefix length.
For more information, see [CIDR prefix lengths for commonly-used netmasks](#) on page 133.
 - c Press the **Return** key.
- 10 Configure the **Gateway** and **DNS servers** fields with IPv4 addresses.
 - 11 Use the **Tab** key or the down arrow key to select the **<OK>** option at the bottom of the **Edit Connection** screen, and then press the **Return** key.
 - 12 In the available connections screen, use the **Tab** key to select the **<Quit>** option, and then press the **Return** key.
 - 13 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

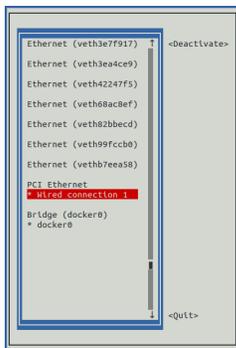
Activate a connection

The **Activate a connection** submenu provides options for activating and deactivating network connections.

Note Do not deactivate the `docker0` connection.

On selection, the **Activate a connection** submenu displays the available connections. The asterisk character (*) at the beginning of a connection name indicates that the connection is active.

Figure 50: Example: Available connections



Use the arrow keys to select a connection, and then use the **Tab** key to navigate the options at the right side of the list. Use the **Return** key to choose an option.

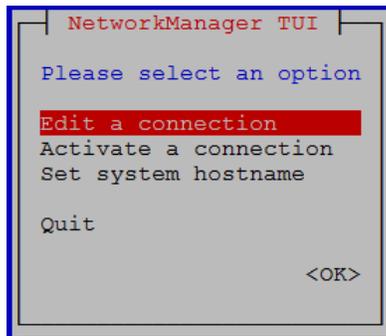
Note Always reboot after activating or deactivating a connection.

Set system hostname

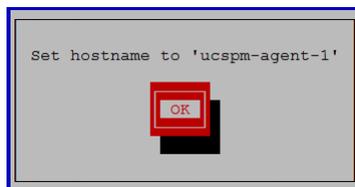
The default hostname of a Control Center host is `ucspm`. To change the hostname, perform this procedure.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Select the **NetworkManager TUI** menu.
 - a In the **Appliance Administration** menu, select the **Configure Network and DNS** option.

- b Press the **Tab** key to select the **Run** button.
- c Press the **Enter** key.



- 4 Display the hostname entry field.
 - a In the **NetworkManager TUI** menu, use the down-arrow key to select **Set system hostname**.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.
- 5 In the **Hostname** field, enter the new hostname.
You may enter either a hostname or a fully-qualified domain name.
- 6 Press the **Tab** key twice to select the **OK** button, and then press the **Enter** key.

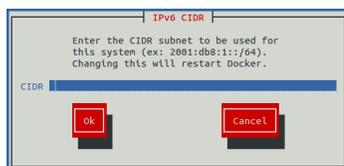


- 7 In the confirmation dialog, press the **Return** key.
- 8 Reboot the operating system.
 - a In the **Appliance Administration** menu, use the down-arrow key to select the **Reboot / Poweroff System** option.
 - b Press the **Tab** key to select the **OK** button.
 - c Press the **Enter** key.

Configure IPv6 Network CIDR

The version of Docker included in the Cisco UCS Performance Manager virtual appliance needs to know at startup the address prefix of the IPv6 network it will use. To enable monitoring of devices that use IPv6, perform this procedure on the Control Center master host, and all agent hosts.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, select the **Configure IPv6 Network CIDR** option.



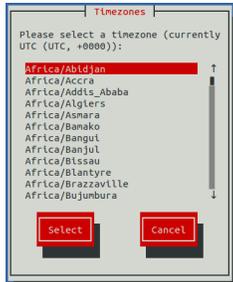
- 4 In the **IPv6 CIDR** screen, enter the address prefix of your IPv6 network in the **CIDR** field.
- 5 Use the **Tab** key to select the **Ok** button, and then press the **Return** key.

The Docker daemon restarts, and the **Appliance Administration** disappears briefly before returning. This is normal.

Configure Timezone

The default timezone of the Cisco UCS Performance Manager virtual appliance is UTC. This procedure changes the timezone setting of a single host. All hosts in a multi-host must use the same timezone.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, select the **Configure Timezone** option.



- 4 Use the **Down Arrow** key to select the desired timezone.
- 5 Press the **Tab** key to highlight **Select**, and then press the **Return** key.

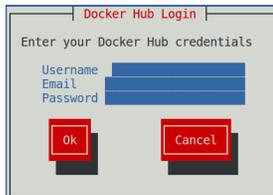
Note Always reboot after changing the timezone.

Change Docker Hub Credentials

To perform this procedure, you need the username, email address, and password of a Docker Hub user account that is authorized to pull Cisco UCS Performance Manager images. The information is provided by Cisco Support when necessary.

The Control Center master host can obtain software updates over the internet from the *Docker Hub* registry. This option obtains a JSON web token from Docker Hub and stores it at `/root/.docker/config.json`.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, select the **Change Docker Hub Credentials** option.



- 4 Enter the username, email address, and password of the authorized user account in the fields. Use the **Tab** key to advance to the next field.
- 5 Press the **Tab** key to highlight **OK**, and then press the **Return** key.

Change Root Password

This option invokes the `passwd` command to change the password of the `root` user account.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, select the **Change Root Password** option.
The **Appliance Administration** menu disappears, and the system prompts for a new password:

```
Changing password for user root.
New password:
```

- 4 **Note** Passwords must include a minimum of eight characters, with at least one character from three of the following character classes: uppercase letter, lowercase letter, digit, and special.

Enter a new password, and then press the **Return** key.

- 5 Enter the password again, and then press the **Return** key.
The **Appliance Administration** menu reappears.

Change ccuser Password

This option invokes the `passwd` command to change the password of the `ccuser` user account.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, select the **Change Root Password** option.
The **Appliance Administration** menu disappears, and the system prompts for a new password:

```
Changing password for user ccuser.
New password:
```

- 4 **Note** Passwords must include a minimum of eight characters, with at least one character from three of the following character classes: uppercase letter, lowercase letter, digit, and special.

Enter a new password, and then press the **Return** key.

- 5 Enter the password again, and then press the **Return** key.
The **Appliance Administration** menu reappears.

Update System

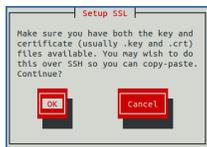
This option updates the Control Center and Cisco UCS Performance Manager software on a host. For more information, refer to the upgrade appendix for your hypervisor.

Change SSL settings

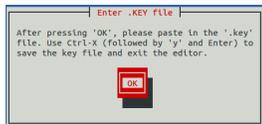
To perform this step, you need to be able to display the contents of the SSL certificate and key files that you want to install on the Control Center master host, and you need a copy of the root certificate file (`rootCA.pem`). In addition, Cisco recommends logging in to the master host through SSH, rather than the hypervisor console, so that you can copy and paste content.

This option allows you to provide new content for SSL certificate and key files.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Use the **Down Arrow** key to select **Change SSL settings**, and then press the **Return** key.



- 4 When you are ready to add the contents of your SSL certificate and key files to the Control Center master host, press the **Return** key.



- 5 Press the **Return** key.
The **Appliance Administration** menu is replaced with the nano text editor.
- 6 Enter the contents of your SSL key file, and then save the file and exit the editor.
 - a Press **Ctrl-O**.
 - b Press **Ctrl-X**.
 - c Press the **y** key, and then press the **Return** key.



- 7 Press the **Return** key.
The **Appliance Administration** menu is replaced with the nano text editor.
- 8 Enter the contents of your SSL certificate file, and then save the file and exit the editor.
 - a Press **Ctrl-O**.
 - b Press **Ctrl-X**.
 - c Press the **y** key, and then press the **Return** key.



- 9 Restart the Control Center daemon (`serviced`) now or later.
Restarting `serviced` pauses Cisco UCS Performance Manager services briefly.
 - To restart `serviced` now, press the **Return** key.
 - To restart `serviced` later, press the **Tab** key to select **No**, and then press the **Return** key.
- 10 Install the root certificate into browser clients.
The procedures for installing a root certificate into a browser client varies by browser and client operating system. For more information, refer to your browser documentation or articles such as [this one](#).

Root Shell

This option starts a command-line session as the `root` user.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as [PuTTY](#).
- 2 Log in as the `root` user.
- 3 Use the **Down Arrow** key to select **Root Shell**, and then press the **Return** key.

The menu is replaced by a command prompt similar to the following example:

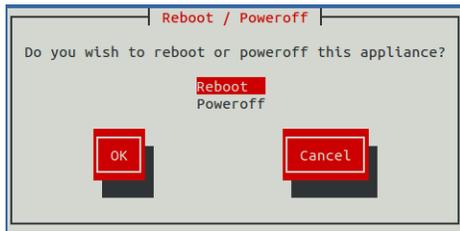
```
[root@ucspm ~]#
```

To return to the **Appliance Administration** menu, enter the `exit` command.

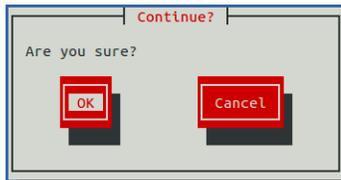
Reboot / Poweroff System

This option reboots or shuts down and turns off a Control Center host.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 In the **Appliance Administration** menu, select the **Reboot / Poweroff System** option.



- 4 Use the **Down Arrow** key to select **Reboot** or **Poweroff System**.
- 5 Press the **Tab** key to highlight **OK**, and then press the **Return** key.



- 6 Use the **Tab** key to select **OK** or **Cancel**, and then press the **Return** key. The system reboots or shuts down and powers off.

D

Networking and security

This appendix describes important networking and security aspects of Cisco UCS Performance Manager appliances. The appliances use the CentOS 7.2 operating system.

Networking requirements

On startup, Docker creates the `docker0` virtual interface and selects an unused IP address and subnet (typically, 172.17.42.1/16) to assign to the interface. The virtual interface is used as a virtual Ethernet bridge, and automatically forwards packets among real and virtual interfaces attached to it. The host and all of its containers communicate among one another through this virtual bridge.

Docker can only check directly-connected routes, so the subnet it chooses for the virtual bridge may be inappropriate for your environment. For example, if you are using the `docker0` subnet for nameservers in your environment, then DNS resolution within containers will fail. To configure a different subnet, see [Configuring the Docker virtual bridge](#) on page 132.

The `firewalld` utility includes rules that can conflict with Docker, and therefore, Control Center and Cisco UCS Performance Manager. The following interactions illustrate the conflicts:

- The `firewalld` daemon removes the `DOCKER` chain from `iptables` when it starts or restarts.
- Under `systemd`, `firewalld` is started before Docker. However, if you start or restart `firewalld` while Docker is running, you need to restart Docker.

By default, `firewalld` is disabled. If you wish to enable it, please ensure that it does not conflict with Docker.

If you are not using a firewall utility, your firewall settings may still prevent communications over the Docker virtual bridge. This occurs when `iptables` INPUT rules restrict most traffic. To ensure that the bridge works properly, append an INPUT rule to your `iptables` configuration that allows traffic on the bridge subnet. For example, if `docker0` is bound to 172.17.42.1/24, then the following, non-specific command ensures that the bridge works:

```
iptables -A INPUT -d 172.17.42.1/24 -j ACCEPT
```

Note The preceding command is only an example. Please consult your networking specialist before modifying your `iptables` configuration.

Additional requirements

Control Center requires a 16-bit, private IPv4 network for virtual IP addresses. The default network is 10.3/16. If the default network is already in use in your environment, you may substitute any valid IPv4 16-bit address space. To

do so, edit the Control Center configuration file, `/etc/default/serviced`, and provide a new value for the `SERVICED_VIRTUAL_ADDRESS_SUBNET` variable.

Note *RFC 1918* restricts private networks to the 10/8, 172.16/12, and 192.168/16 address spaces. However, Control Center accepts any valid, 16-bit, IPv4 address space for its private network.

This release of Control Center relies on Network File System (NFS) for its distributed file system implementation. For this reason, hosts in a Control Center cluster may not run a general-purpose NFS server, and all hosts require NFS.

All hosts in Control Center resource pools must:

- be able to resolve the hostnames of all other resource pool hosts to IPv4 addresses (for example, if the public IP address of your host is 192.0.2.1, then the `hostname -i` command should return 192.0.2.1)
- respond with an IPv4 address other than `127.x.x.x` when `ping Hostname` is invoked
- return a unique result from the `hostid` command

Security considerations

In Cisco UCS Performance Manager appliances, the `firewalld` service is disabled. If desired, you may enable it, and then close unused ports.

Control Center includes a virtual multiplexer (mux), to aggregate the UDP and TCP traffic among the services it manages. The aggregation is opaque to services, and mux traffic is encrypted when it travels among containers on remote hosts. (Traffic among containers on the same host is not encrypted.) The mux, along with the distributed file system, enables Control Center to deploy services to any pool host, rapidly. The mux also reduces the number of open ports required on a Control Center host to a predictable set.

The following table identifies the ports that Control Center requires for its operations. All of the ports except 4979 are configurable. All traffic is TCP.

Note Control Center relies on the system clock to synchronize its actions, and indirectly, NTP, to synchronize clocks among multiple hosts. In the default configuration of `ntpd`, the firewalls of master and resource pool hosts must support an incoming UDP connection on port 123.

Table 1: Port requirements among Control Center hosts

Port	Protocol	Application
22	TCP	SSH
443, 50443	TCP	HTTPS
2049	TCP	NFS
2181	TCP	ZooKeeper
2888, 3888	TCP	ZooKeeper (multi-host deployments only)
4979	TCP	Control Center RPC endpoint
5000	TCP	Docker registry
5042, 5043	TCP	Logstash
8443	TCP	Elasticsearch
22250	TCP	Control Center virtual multiplexer

Additional considerations

- To gain access to the Control Center browser interface, users must have login accounts on the Control Center master host. (Pluggable Authentication Modules (PAM) is supported.) By default, the users must be members of the `wheel` group. The default group may be changed by setting the `SERVICED_ADMIN_GROUP` variable, and the replacement group does not need superuser privileges.
- The `serviced` startup script sets the hard and soft open files limit to 1048576, but does not modify the `/etc/sysconfig/limits.conf` file.
- Control Center does not support *Security Enhanced Linux* in enforcing mode, so it is disabled in Cisco UCS Performance Manager appliances.

Configuring the Docker virtual bridge

To perform this task, you need an unused, 24-bit IPv4 address block.

Perform this procedure to change the subnet of the Docker virtual bridge. This procedure is valid for Cisco UCS Performance Manager release 2.0.1 and later releases.

- 1 Gain access to the Control Center host, through the console interface of your hypervisor, or through a remote shell utility such as *PuTTY*.
- 2 Log in as the `root` user.
- 3 Change directory to the location of the primary Docker configuration file.

```
cd /etc/systemd/system/docker.service.d
```

- 4 Create a backup copy of the primary configuration file.

```
cp docker.conf docker-conf.bak
```

- 5 Open `docker.conf` with a text editor.
- 6 On the last line, replace the value of the `--dns` flag with the IPv4 address of your unused subnet. Do not use CIDR notation for this value. The last line specifies the value of the `ExecStart` directive.
- 7 On the last line, set the `--bip` flag.
The value of the flag is the IPv4 address of your subnet, in CIDR notation. The routing prefix does not need to be larger than 24 bits. The flag is present in release 2.0.2 and later. The flag is usually placed after the `--dns` flag.

- If the flag is absent, add it.
- If the flag is present, replace the existing IP address with the IP address of your unused subnet. Do not remove the routing prefix.

- 8 Save the file, and then close the text editor.

The following example shows valid settings of the `--dns` and `--bip` flags for the `ExecStart` directive in a primary Docker configuration file.

Note In this example, the value of the `ExecStart` variable is formatted to fit the available space. In the configuration file, the variable and value are on the same line.

```
ExecStart=/usr/bin/docker daemon -H fd:// $OPTIONS -s devicemapper \
--storage-opt dm.basesize=45G \
--storage-opt dm.thinpooldev=/dev/mapper/docker-docker--pool \
--dns=172.17.0.1 --bip=172.17.0.1/24 \
--exec-opt native.cgroupdriver=cgroupfs
```

CIDR prefix lengths for commonly-used netmasks

Subnet mask	CIDR prefix length
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29



Tuning considerations

This appendix describes how to tune the service definitions of key Cisco UCS Performance Manager services, for both single-host and multi-host deployments. For more information about tuning your system, contact your Cisco representative.

Single-host deployment tuning options

In single-host deployments, all Cisco UCS Performance Manager services run on the same host. So, adjusting the values of the `RAMCommit` parameter in the Cisco UCS Performance Manager service definition is not as important as it is in multi-host deployments. Nonetheless, the following list identifies both the services to modify to support 500 UCS servers, and their new values:

- RegionServer, 4GB
- mariadb-event, 2GB
- memcached, 2GB
- CentralQuery, 2GB
- Zope, 2GB
- zenhub, 4GB
- zenmodeler, 2GB
- zenucsevents, 2GB
- zenvsphere, 4GB

In addition, the following adjustments are recommended:

- For big UCS servers, reduce `configsipsize` from 25 to 5 or less in `zenucsevents.conf` (in the `zenucsevents` service).
- For large vCenters (10,000 VMs), reduce `configsipsize` from 25 to 1 in `zenvsphere.conf` (in the `zenvsphere` service).

Multi-host deployment tuning options

For multi-host deployments, adjust the values of the `RAMCommit` parameter in the Cisco UCS Performance Manager service definition for the services in the following list. The list identifies both the services to modify and their new values:

- RegionServer, 8GB
- reader, 4GB
- mariadb-model, 4GB

- mariadb-events, 4GB
- memcached, 4GB
- Zope, 4GB
- zenucsevents, 3GB
- zenvsphere, 6GB
- zenpython, 3GB
- zenmodeler, 3GB
- zenhub, 15GB
- CentralQuery, 4GB
- MetricConsumer, 2GB

In addition, adjust the zenhub service to use 6 workers and 3 invalidation workers.

Using Zenoss Toolbox

This appendix describes how to install and use Zenoss Toolbox.

Zenoss Toolbox tools

The Zenoss Toolbox tools examine key Cisco UCS Performance Manager components for common issues affecting data integrity. Cisco recommends running the following tools, in order, before upgrading Cisco UCS Performance Manager:

- 1 The `zodbscan` tool quickly scans the Zope Object Database (ZODB) to provide a preliminary indication of the health of the database, and to determine whether the database needs to be compressed with `zenossdbpack` before upgrading.
- 2 The `findposkeyerror` tool checks objects and their relationships, and provides options for fixing errors.
- 3 The `zenrelationscan` tool checks only ZenRelations between objects.
- 4 The `zencatalogscan` tool checks ZODB object catalogs, which speed up web interface access.

The tools are run inside a Zope container, and the log files for each command are found in `$ZENHOME/log/toolbox`.

Downloading Zenoss Toolbox with internet access

This procedure describes how to download Zenoss Toolbox to a Control Center master host that has internet access.

- 1 Log in to the Control Center master host as `root`, or as a user with superuser privileges.
- 2 Create a temporary directory, and change the current working directory to the temporary directory. The directory must be local (not mounted).

```
mkdir /tmp/toolbox && cd /tmp/toolbox
```

- 3 Download Zenoss Toolbox.

```
myUrl=https://github.com/zenoss/zenoss.toolbox/archive/master.zip  
curl -sL --insecure -o master.zip $myUrl
```

- 4 Change the directory and file permissions.

The directory and file must be readable, writable, and executable by all users.

```
chmod -R 777 /tmp/toolbox
```

Downloading Zenoss Toolbox without internet access

This procedure downloads Zenoss Toolbox to a Control Center master host that does not have internet access.

- 1 Log in to a system that has internet access.
- 2 Start a web browser, and then navigate to [the Zenoss Toolbox releases page](#).
- 3 Download the latest version of the Zenoss Toolbox source code ZIP file. The name of the file is `zenoss.toolbox-Version.zip`.
- 4 Use your operating system to rename the file to `master.zip`.
- 5 Use a file transfer utility such as [WinSCP](#) to copy the file to the Control Center master host.
- 6 Log in to the Control Center master host as `root`, or as a user with superuser privileges.
- 7 Create a temporary directory, and change the current working directory to the temporary directory. The directory must be local (not mounted).

```
mkdir /tmp/toolbox && cd /tmp/toolbox
```

- 8 Copy the Zenoss Toolbox ZIP file to the temporary directory.

Replace *Path-to-File* with the location of the `master.zip` file.

```
cp Path-to-File/master.zip /tmp/toolbox
```

- 9 Change the directory and file permissions. The directory and file must be readable, writable, and executable by all users.

```
chmod -R 777 /tmp/toolbox
```

Installing Zenoss Toolbox

This procedure describes how to install Zenoss Toolbox for use in Control Center Zope containers.

- 1 Log in to the Control Center master host as `root`, or as a user with superuser privileges.
- 2 Start a shell as the `zenoss` user in a Zope container.
 - a Change directory to the temporary location of the Zenoss Toolbox `master.zip` file.

```
cd /tmp/toolbox
```

- b Start an interactive shell in a Zope container and save a snapshot named `InstallZenossToolbox`.

```
mySnap=InstallZenossToolbox
serviced service shell -i -s $mySnap zope bash
```

- c Switch user to `zenoss`.

```
su - zenoss
```

- 3 Install Zenoss Toolbox, and then exit the container.

- a Install Zenoss Toolbox.

```
easy_install /mnt/pwd/master.zip
```

- b Exit the zenoss user account.

```
exit
```

- c Exit the Zope container.

```
exit
```

- 4 Commit the named snapshot.

```
serviced snapshot commit $mySnap
```

- 5 Restart the Zope service.

```
serviced service restart zope
```

Running Zenoss Toolbox tools

- 1 Log in to the Control Center master host as a user with serviced CLI privileges.
- 2 Start an interactive session in a Zope container.

```
serviced service attach zope/0
```

- 3 Switch user to zenoss.

```
su - zenoss
```

- 4 Run the Zenoss Toolbox tools, in order.
For more information about the tools, see [Zenoss Toolbox tools](#) on page 136.
- 5 Exit the zenoss user account.

```
exit
```

- 6 Exit the Zope container.

```
exit
```