Cisco UCS Performance Manager Planning Guide

First Published: October 2017

Release 2.5.1

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

Contents

About this guide

Cisco UCS Performance Manager Planning Guide provides the information needed to plan a deployment of Cisco UCS Performance Manager Express or 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.

Related publications

Title	Description
Cisco UCS Performance Manager Planning Guide	Provides general and specific information for preparing to deploy Cisco UCS Performance Manager.
Cisco UCS Performance Manager Installation Guide	Provides detailed information and procedures for installing Cisco UCS Performance Manager.
Cisco UCS Performance Manager Upgrade Guide	Provides detailed procedures for upgrading your existing Cisco UCS Performance Manager 2.x instance to a newer version.
Cisco UCS Performance Manager Migration Guide	Provides detailed information about, and where applicable, procedures for migrating data from Cisco UCS Performance Manager version 1.x into a version 2.x instance.
Cisco UCS Performance Manager Getting Started Guide	Provides instructions for configuring Cisco UCS Performance Manager to monitor your environment after installation.
Cisco UCS Performance Manager User Guide	Provides specific instructions for using Cisco UCS Performance Manager in the UCS environment.
Cisco UCS Performance Manager Administration Guide	Provides an overview of Cisco UCS Performance Manager architecture and features, as well as procedures and examples to help you use the system.
Cisco UCS Performance Manager Release Notes	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 Express and Cisco UCS Performance Manager—referred to "Cisco UCS Performance Manager" when the differences between them are not important—provide 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.

Cisco UCS Performance Manager is deployed into the distributed architecture of Control Center, an open-source, application service orchestrator based on *Docker*. Control Center and Cisco UCS Performance Manager are independent and unaware of each other, although Control Center is designed for the unique requirements of Cisco UCS Performance Manager. Control Center greatly simplifies the installation, deployment, and management of Cisco UCS Performance Manager.

This chapter describes the minimum requirements and packaging of Cisco UCS Performance Manager. The next chapter introduces Control Center, and the final chapter describes Cisco UCS Performance Manager deployment considerations.

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 to version 2.0.x, 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	16GB	900GB	200
3	8	32GB	150GB	100

Note To determine whether your environment requires a single-host or a multi-host deployment, please use the *Cisco UCS Performance Manager Deployment Calculator* (*http://zenoss.github.io/deployment-calculator/*).

The tool identifies the minimum requirements for your environment. Cisco strongly recommends using the results to size your deployment, and to include a margin of safety above the minimum requirements for the normal variance in resource usage that occur in deployments.

Packaging

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 7.3) 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.

Introduction to Control Center 2

This chapter introduces Control Center, an open-source application service orchestrator based on *Docker*.

Control Center is a platform-as-a-service framework that can manage any 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.

Features

Control Center includes the following key features:

- Intuitive HTML5 interface for deploying and managing applications
- 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
- Delegate host authentication to prevent unauthorized system access
- Storage monitoring and emergency shutdown of services to minimize the risk of data corruption
- Rolling restart of services to reduce downtime of multi-instance services

Terminology, internal services, and concepts

This section defines Control Center terminology, internal services that enable Control Center to function, and concepts that are used in this guide and other documentation.

application

One or more software services packaged in Docker Engine containers.

cluster

The collection of hosts in one or more Control Center resource pools.

delegate host

A host that runs the application services scheduled for the resource pool to which it belongs. A system can be configured as delegate or master.

Docker Engine

An open-source application for building, shipping, and running distributed applications.

Elasticsearch

(Control Center internal service) A distributed, real-time search and analytics engine. Control Center uses it to index log files and store service definitions.

Kibana

(Control Center internal service) A browser-based user interface that enables the display and search of Elasticsearch databases, including the log files that Control Center monitors.

Logstash

(Control Center internal service) A log file collector and aggregator that forwards parsed log file entries to Elasticsearch.

master host

The host that runs the application services scheduler, the Docker registry, the distributed file system, and other internal services, including the HTTP server for the Control Center browser interface and application browser interface. A system can be configured as delegate or master. Only one system in a Control Center cluster can be the master.

OpenTSDB

(Control Center internal service) A time series database that Control Center uses to store its service performance metrics.

resource pool

A collection of one or more hosts, each with its own compute, network, and storage resources. All of the hosts in a resource pool must have identical hardware resources, and must be located in the same data center and on the same subnet. If a resource pool host is a hypervisor guest system, all of the hosts in the resource pool must be guests of the same hypervisor host system.

service

A process and its supporting files that Control Center runs in a single container to provide specific functionality as part of an application.

serviced

The name of the Control Center service and a command-line client for interacting with the service.

tenant

An application that Control Center manages.

ZooKeeper (*Apache ZooKeeper*)

(Control Center internal service) A centralized service that Control Center uses for configuration maintenance, naming, distributed synchronization, and providing group services.

Docker fundamentals

This section summarizes *the architecture description provided by Docker* as customized for Control Center. For additional information, refer to the Docker site.

Docker provides convenient tools that make use of the *control groups 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. Control Center uses a private Docker registry for its own images and application images.

Docker containers

Docker containers have everything needed to run a service instance, and are created from images. Control Center launches each service instance in its own Docker container.

Docker storage

Docker and Control Center data are stored in a customized LVM thin pool that is created from one or more block devices or partitions, or from one or more LVM volume groups.

Control Center application data storage

Control Center uses a dedicated LVM thin pool on the master host to store application data and snapshots of application data.

- The distributed file system (DFS) of each tenant application that `serviced` manages is stored in separate virtual devices. The initial size of each tenant device is copied from the base device, which is created during the initial startup of `serviced`.
- Snapshots of tenant data, used as temporary restore points, are stored in separate virtual devices, outside of tenant virtual devices. The size of a snapshot depends on the size of the tenant device, and grows over time.

The Control Center master host requires high-performance, persistent storage. Storage can be local or remote.

- For local storage, solid-state disk (SSD) devices are recommended.
- For remote storage, storage-area network (SAN) systems are supported. High-performance SAN systems are recommended, as is assigning separate logical unit numbers (LUNs) for each mounted path.

The overall response times of master host storage affect the performance and stability of Control Center internal services and the applications it manages. For example, ZooKeeper (a key internal service) is sensitive to storage latency greater than 1000 milliseconds.

Note The physical devices associated with the application data thin pool must be persistent. If removable or re-connectable storage such as a SAN based on iSCSI is used, then the Device-Mapper Multipath feature of RHEL/CentOS must be configured and enabled.

Control Center includes the `serviced-storage` utility for creating and managing its thin pool. The `serviced-storage` utility can:

- use physical devices or partitions, or LVM volume groups, to create a new LVM thin pool for application data
- add space to a tenant device at any time
- identify and clean up orphaned snapshots
- create an LVM thin pool for Docker data

Networking

On startup, Docker creates the `docker0` virtual interface and selects an unused IP address and subnet (typically, 172.17.0.1/16) 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 through this virtual bridge.

Docker can only check directly connected routes, so the subnet it chooses for the virtual bridge might be inappropriate for your environment. The *Cisco UCS Performance Manager Administration Guide* includes procedures for configuring a different subnet for `docker0`.

The following list highlights potential communication conflicts:

- If you use a firewall utility, ensure that it does not conflict with Docker. The default configurations of firewall utilities such as *FirewallD* include rules that can conflict with Docker, and therefore Control Center. 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 must restart Docker.
- Even if you do not use a firewall utility, your firewall settings might still prevent communications over the Docker virtual bridge. This issue 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 172.17.42.1/16, then a command like the following example would ensure that the bridge works.

  Note Before modifying your `iptables` configuration, consult your networking specialist.

  ```
  iptables -A INPUT -d 172.17.0.0/16 -j ACCEPT
  ```

Additional requirements and considerations

Control Center requires a 16-bit, private IPv4 network for virtual IP addresses. The default network is 10.3/16, but during installation you can select any valid IPv4 16-bit address space.

Before installation, add DNS entries for the Control Center master host and all delegate hosts. Verify that all hosts in Control Center resource pools can

- Resolve the hostnames of all other delegate 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.

Control Center relies on Network File System (NFS) for its distributed file system implementation. Therefore, hosts in a Control Center cluster cannot run a general-purpose NFS server, and all hosts require NFS.

Security

In Cisco UCS Performance Manager appliances, the `firewalld` service is disabled. If desired, you may enable it, and then close unused ports. Likewise, SELinux is disabled and may be enabled.

Port information in this section applies only to Control Center. See the documentation for your application for additional port requirements.

During installation, Control Center has no knowledge of the port requirements of the applications it is to manage, so the installation procedure includes disabling the firewall. After both Control Center and an application are installed, you can close unused ports.

Control Center includes a virtual multiplexer (mux) that performs the following functions:

- Aggregates 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.)
- Along with the distributed file system, enables Control Center to quickly deploy services to any pool host.
- 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 requirements and considerations

- To install Control Center, you must log in as `root`, or as a user with superuser privileges.
- Access to the Control Center browser interface requires a login account on the Control Center master host. Pluggable Authentication Modules (PAM) is supported. By default, 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. The script does not modify the `/etc/sysconfig/limits.conf` file.
- Control Center supports *Security Enhanced Linux*.

Delegate host authentication

Control Center uses RSA key pairs to create the authentication tokens that are required for all delegate communications. When you add a host to a resource pool, the `serviced` instance on the master host creates a private key for the delegate and bundles it with its own public key. The `serviced` instance on the delegate host uses the bundle to sign messages with its unique tokens.

Key bundles are installed by using an SSH connection or a file.

- The command to add a host to a pool can initiate an SSH connection with the delegate and install the key bundle. This option is the most secure because no file is created. However, it requires either public key authentication or password authentication between the master and delegate hosts.
- When no SSH connection is requested, the command to add a host to a pool creates a file that contains the key bundle. You can move the key bundle file to the delegate host with any file transfer method, and then install it on the delegate.

3 Deployment considerations

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

- All Cisco UCS Performance Manager data is stored on the Control Center master host. Delegate 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. The *Cisco UCS Performance Manager Installation 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, a multi-host deployment includes a ZooKeeper cluster, which enhances Control Center reliability.

Supported operating systems and browsers

The following table identifies the supported combinations of client operating systems and web browsers.

Client OS	Supported Browsers
Windows 7 and 8.1	Internet Explorer 11 (Enterprise mode only; compatibility mode is not supported.)
	Internet Explorer 10*
Windows 10	Internet Explorer 11 (Enterprise mode only; compatibility mode is not supported.)
	Internet Explorer 10*
	Firefox 50 and later
	Chrome 54 and later
	Microsoft Edge
Windows Server 2012 R2	Firefox 30
	Chrome 36
Macintosh OS/X 10.9	Firefox 30 and above
	Chrome 36 and above
Ubuntu 14.04 LTS	Firefox 30 and above
	Chrome 37 and above
Red Hat Enterprise Linux 6.5, CentOS 6.5	Firefox 30 and above
	Chrome 37 and above

Compatibility matrix

The following tables provide information regarding the physical and virtual devices and software supported by Cisco UCS Performance Manager. The information has been segmented into different functional areas and is organized by vendor within each functional area.

Server support

The following table outlines server support for Cisco UCS Performance Manager.

Components	Supported Models	Supported Software
UCS B-Series Servers	All	UCS Manager Version 2.2 and 3.1 (1x)
UCS C-Series Servers	All	UCS Manager Version 2.2 and 3.1 (1x)
UCS Mini	All	UCS Manager Version 3.0 and 3.1 (1x)

* Support for Internet Explorer 10 will be withdrawn beginning with the next feature release of Cisco UCS Performance Manager.

Host Operating System support

Components	Supported Communication
Linux Servers The following distros are supported: ■ Ubuntu 12.04 LTS, 14.04 LTS, 15.04, 15.10 ■ RHEL 5, 6, 7 ■ CentOS 5, 6, 7 ■ SuSE LES (SLES) 11, 12	SNMP v1/v2/v3 or SSH
Windows Servers	■ SNMP v1/v2 or WinRM for Windows Server 2008 and 2008 R2. There is no SNMP v3 support. ■ WinRM for Windows 2012 R2. There is no SNMP support for Windows 2012. ■ WinRM for Windows 2016.

Network and Fabric support

The following table outlines the versions of Cisco network and fabric devices that are supported by this release.

Components	Supported Models	Supported Software
Cisco Nexus 1000 Series Distributed Virtual Switch	Nexus 1000v and 1010	NX-OS Version 4 and higher
Cisco Nexus 2000 Series Fabric Extenders	Nexus 2000 Series	NX-OS Version 4 and higher
Cisco Nexus 3000 Series Switches	Nexus 3000 Series	NX-OS Version 4 and higher
Cisco Nexus 5000 Series Switches	Nexus 5000 Series	NX-OS Version 4 and higher
Cisco Catalyst 6500 Series Switches and Virtual Switching Systems (VSS)	Catalyst 3560 and Catalyst 6500 Series	CatOS and Cisco IOS
Cisco Nexus 7000 Series Switches	Nexus 7000 Series	NX-OS Version 4 and higher
Cisco Nexus 9000 Series Switches	Nexus 9000 Series, Supported only in NX-OS mode	NX-OS Version 4 and higher
Cisco MDS 9000 Series Multilayer Switches	MDS 9000 Series	NX-OS Version 4 and higher

Hypervisor support

The following table outlines the versions of VMware vSphere that are supported by this release of Cisco UCS Performance Manager.

Software Components	Supported Versions
VMware vSphere Hypervisor (ESX/ESXi)	5.5, 6.0, 6.5
VMware vSphere vCenter Server	5.5, 6.0, 6.5

The following table outlines the versions of Microsoft Hyper-V that are supported by this release of Cisco UCS Performance Manager.

Software Components	Supported Versions	Windows Versions
Microsoft Hyper-V Hypervisor	Version 2.0	2008 R2 SP1
	Version 3.0	2012, 2012 R2

Storage support

The following table outlines storage support for NetApp and EMC.

Components	Supported Models	Supported Versions
NetApp FAS (Data-ONTAP 7-Mode or C-Mode)	NetApp FAS (Data-ONTAP 7-Mode or C-Mode)	Version 8.x
NetApp FAS (C-Mode)	NetApp FAS (C-Mode)	Version 9.0
EMC VMAX and VNX*	All models	SMI-S Provider V4.6.2.3 (SE V7.6-1808 2.8)**

* VNX File Mode is supported.
** SMI-S provider version 8.1 is not currently supported.