Cisco UCS Director Installation Guide for VMware vSphere and Microsoft Hyper-V, Release 6.9

First Published: 2024-05-07

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

Preface

Audience

This guide is intended primarily for data center administrators who use and who have responsibilities and expertise in one or more of the following:

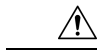
- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.



Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

Documentation Feedback

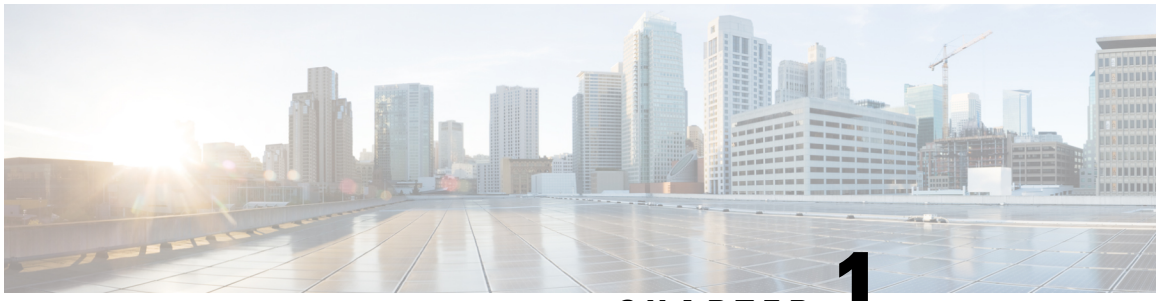
To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

Overview

Cisco UCS Director

Cisco UCS Director is a complete, highly secure, end-to-end management, orchestration, and automation solution for a wide array of Cisco and non-Cisco data infrastructure components, and for the industry's leading converged infrastructure solutions based on the Cisco UCS and Cisco Nexus platforms. For a complete list of supported infrastructure components and solutions, see the Cisco UCS Director Compatibility Matrix.

Cisco UCS Director is a 64-bit appliance that uses the following standard templates:

- Open Virtualization Format (OVF) and Open Virtual Appliance (OVA) for VMware vSphere
- Virtual Hard Disk (VHD) for Microsoft Hyper-V

Management through Cisco UCS Director

Cisco UCS Director extends the unification of computing and networking layers through Cisco UCS to provide you with comprehensive visibility and management of your data center infrastructure components. You can use Cisco UCS Director to configure, administer, and monitor supported Cisco and non-Cisco components. The tasks you can perform include the following:

- Create, clone, and deploy service profiles and templates for all Cisco UCS servers and compute applications.
- Monitor organizational usage, trends, and capacity across a converged infrastructure on a continuous basis. For example, you can view heat maps that show virtual machine (VM) utilization across all your data centers.
- Deploy and add capacity to converged infrastructures in a consistent, repeatable manner.
- Manage, monitor, and report on data center components, such as Cisco UCS domains or Cisco Nexus network devices.
- Extend virtual service catalogs to include services for your physical infrastructure.

- Manage secure multi-tenant environments to accommodate virtualized workloads that run with non-virtualized workloads.

Automation and Orchestration with Cisco UCS Director

Cisco UCS Director enables you to build workflows that provide automation services, and to publish the workflows and extend their services to your users on demand. You can collaborate with other experts in your company to quickly and easily create policies. You can build Cisco UCS Director workflows to automate simple or complex provisioning and configuration processes.

Once built and validated, these workflows perform the same way every time, no matter who runs the workflows. An experienced data center administrator can run them, or you can implement role-based access control to enable your users and customers to run the workflows on a self-service basis, as needed.

With Cisco UCS Director, you can automate a wide array of tasks and use cases across a wide variety of supported Cisco and non-Cisco hardware and software data center components. A few examples of the use cases that you can automate include, but are not limited to:

- VM provisioning and lifecycle management
- Network resource configuration and lifecycle management
- Storage resource configuration and lifecycle management
- Tenant onboarding and infrastructure configuration
- Application infrastructure provisioning
- Self-service catalogs and VM provisioning
- Bare metal server provisioning, including installation of an operating system

Features and Benefits

The features and benefits of Cisco UCS Director are as follows:

Feature	Benefit
Central management	• Provides a single interface for administrators to provision, monitor, and manage the system across physical, virtual, and bare metal environments • Provides unified dashboards, reports, and heat maps, which reduce troubleshooting and performance bottlenecks
Self-service catalog	• Allows end users to order and deploy new infrastructure instances conforming to IT-prescribed policies and governance
Adaptive provisioning	• Provides a real-time available capability, internal policies, and application workload requirements to optimize the availability of your resources
Dynamic capacity management	• Provides continuous monitoring of infrastructure resources to improve capacity planning, utilization, and management • Identifies underutilized and overutilized resources

Feature	Benefit
Multiple hypervisor support	• Supports VMware ESX, ESXi, Microsoft Hyper-V, and Red Hat hypervisors
Computing management	• Provisions, monitors, and manages physical, virtual, and bare metal servers, as well as blades • Allows end users to implement virtual machine life-cycle management and business continuance through snapshots • Allows administrators to access server utilization trend analysis
Network management	• Provides policy-based provisioning of physical and virtual switches and dynamic network topologies • Allows administrators to configure VLANs, virtual network interface cards (vNICs), port groups and port profiles, IP and Dynamic Host Control Protocol (DHCP) allocation, and access control lists (ACLs) across network devices
Storage management	• Provides policy-based provisioning and management of filers, virtual filers (vFilers), logical unit numbers (LUNs), and volumes • Provides unified dashboards that allow administrators comprehensive visibility into organizational usage, trends, and capacity analysis details.

Physical and Virtual Management Features

Physical Server Management	Virtual Computing Management
• Discover and collect configurations and changes • Monitor and manage physical servers • Perform policy-based server provisioning • Manage blade power • Manage server life cycle • Perform server use trending and capacity analysis • Perform bare metal provisioning using preboot execution environment (PXE) boot management	• Discover, collect, and monitor virtual computing environments • Perform policy-based provisioning and dynamic resource allocation • Manage the host server load and power • Manage VM life cycle and snapshots • Perform analysis to assess VM capacity, sprawl, and host utilization

Physical Storage Management	Virtual Storage Management
• Discover, collect, and monitor storage filers • Perform policy-based provisioning of vFilers • Provision and map volumes • Create and map Logical Unit Number (LUN) and iGroup instances • Perform SAN zone management • Monitor and manage network-attached storage (NAS) and SAN-based storage • Implement storage best practices and recommendation	• Discover, collect, and monitor storage of vFilers and storage pools • Perform policy-based storage provisioning for thick and thin clients • Create new datastores and map them to virtual device contexts (VDCs) • Add and resize disks to VMs • Monitor and manage organizational storage use • Perform virtual storage trend and capacity analysis
Physical Network Management	**Virtual Network Management**
• Discover, collect, and monitor physical network elements • Provision VLANs across multiple switches • Configure Access Control Lists (ACLs) on network devices • Configure storage network s • Implement dynamic network topologies	• Add networks to VMs • Perform policy-based provisioning with IP and DHCP allocation • Configure and connect Virtual Network Interface Cards (vNICs) to VLANs and private VLANs • Create port groups and port profiles for VMs • Monitor organizational use of virtual networks

Cisco UCS Director Installation Guidelines

Before you install Cisco UCS Director, be aware of the following:

Cisco UCS Director VM Disks

During Cisco UCS Director installation, on either VMware vSphere or Microsoft Hyper-V, the installer creates two hard disks.

- Primary disk—Contains the Cisco UCS Director appliance and operating system. Post-installation, the primary disk is named Hard Disk 1.
- Secondary disk—Contains the Cisco UCS Director database. Post-installation, the secondary disk is named Hard Disk 2.

Both disks are automatically created during the installation with the same disk format and parameters.

Cisco UCS Director OVF and VHD Zip Files

Note Cisco UCS Director OVF and VHD zip files are created using zip 3.x in AlmaLinux9.x. For Linux systems, you can extract the zip files with unzip 6.x or higher or with the latest version of the 7-Zip archiving tool. For Windows systems, you can extract the zip files with the native Extract All in Windows Explorer for Windows and Windows Server or with the latest versions of archiving tools such as 7-Zip or WinRAR.

About Licenses

You must obtain a license to use , as follows:

1. Before you install , generate the license key and claim a certificate (Product Access Key).
2. Register the Product Access Key (PAK) on the Cisco software license site, as described in Fulfilling the Product Access Key, on page 5.
3. After you install , update the license in as described in Updating the License, on page 23.
4. After the license has been validated, you can start to use .

Fulfilling the Product Access Key

Before you begin

You need the PAK number.

Step 1 Navigate to the Cisco Software License website.

Step 2 If you are directed to the Product License Registration page, you can take the training or click **Continue to Product License Registration**.

Step 3 On the Product License Registration page, click **Get New Licenses from a PAK or Token**.

Step 4 In the **Enter a Single PAK or TOKEN to Fulfill** field, enter the PAK number.

Step 5 Click **Fulfill Single PAK/TOKEN**.

Step 6 Complete the additional fields in **License Information** to register your PAK:

Name	Description
Organization Name	The organization name.
Site Contact Name	The site contact name.
Street Address	The street address of the organization.
City or Town	The city or town.
State or Province	The state or province.
Zip or Postal Code	The zip code or postal code.

Name	Description
Country	The country name.

Step 7 Click **Issue Key**.

The features for your license appear, and you receive an email with the Digital License Agreement and a zipped license file.

Digitally Signed Images

images are delivered in digitally signed zip files. These signed zip files are wrapped in a container zip file that includes the following:

- Digitally signed zip file—Contains the installation image
- Verification program—Verifies the certificate chain and signature. During certificate chain validation, the program verifies the authenticity of the end-entity certificate using Cisco's SubCA and root CA certificates. Then, the authenticated end-entity certificate is used to verify the signature.
- Digital signature file—Contains the signature that you can verify before installation.
- Certificate file—Enables you to verify the digital signature. This Cisco-signed x.509 end-entity certificate contains a public key that can be used to verify the signature. This certificate is chained to the Cisco root posted on http://www.cisco.com/security/pki/certs/crcam2.cer.
- ReadMe file—Provides the information and instructions required to verify the digitally signed zip file.

Verify the image offline. Once the image is verified, you can begin the installation of .

Requirements for Verifying Digitally Signed Images

Before you verify a digitally signed image, ensure that you have the following on your local machine:

- Connectivity to https://www.cisco.com during the verification process
- Python 3.4.0 or later
- OpenSSL

Verifying a Digitally Signed Image

Before you begin

Download the image from Cisco.com.

Step 1 Unzip the file you downloaded from Cisco.com and verify that it contains the following files:

- ReadMe file

- Digitally signed zip file, for example `CUCSD_6_9_0_0_69115_VMWARE_GA.zip or CUCSD_6_9_0_0_69115_HYPERV_GA.zip`
- Certificate file, for example `UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`
- Digital signature generated for the image, for example `CUCSD_6_9_0_0_69115_VMWARE_GA.zip.signature` or `CUCSD_6_9_0_0_69115_HYPERV_GA.zip.signature`
- Signature verification program, for example `cisco_x509_verify_release.py3`

Step 2 Review the instructions in the ReadMe file.

Note If there are any differences between these instructions and those in the ReadMe, follow the ones in the ReadMe.

Step 3 Run the signature verification program from the directory where you have unzipped the downloaded content.

Example: Signature Verification for VMware OVA Installation

```
python3 cisco_x509_verify_release.py3 -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer -i
CUCSD_6_9_0_0_69115_VMWARE_GA.zip -s  CUCSD_6_9_0_0_69115_VMWARE_GA.zip.signature -v dgst -sha512
```

Example: Signature Verification for Hyper-V VHD Installation

Step 4 Review the output and ensure that the verification has succeeded.

Example: Expected Output for VMware OVA Installation

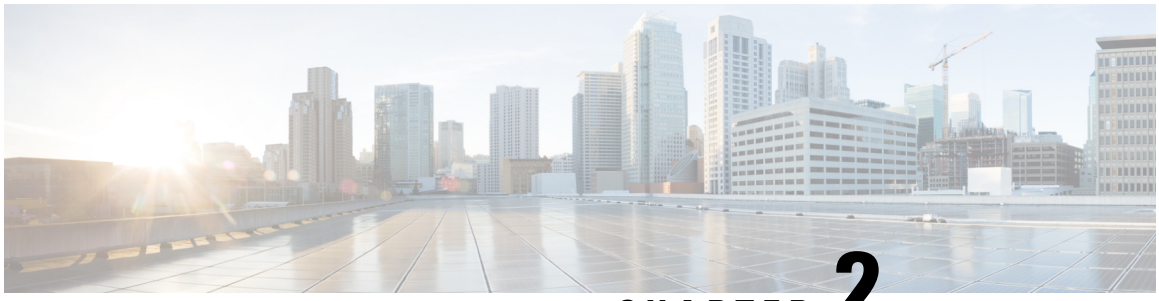
```
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer.
Successfully verified the signature of CUCSD_6_9_0_0_69115_VMWARE_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

Example: Expected Output for Hyper-V VHD Installation

```
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer.
Successfully verified the signature of CUCSD_6_9_0_0_69115_HYPERV_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

What to do next

Install or upgrade .



CHAPTER 2

Installing Cisco UCS Director on VMware vSphere

for VMware vSphere

Note The appliance and boot-up logs are located in the `/var/log/ucsd` directory.

- `install.log` contains the one time appliance installation logs.
- `bootup.log` contains the appliance boot-up sequence information, such as startup messages for the database and infrastructure services.

Default Root and Shelladmin Passwords

During installation, Cisco UCS Director uses default passwords for the following accounts:

- Root user for the Almalinux operating system of the Cisco UCS Director VM. The default password is cisco123.
- Shelladmin user for the Cisco UCS Director Shell menu. The default password is changeme.

Once the installation is completed ,the first time you log in to Cisco UCS Director, you are prompted to reset the default root and Shelladmin passwords.

The new root and Shelladmin password must meet the password requirements. It cannot be a dictionary word or be all lowercase.

Prerequisites for VMware vSphere

Before you install Cisco UCS Director for VMware vSphere, complete the following steps:

- Install VMware vSphere or vCenter.
- Configure a VMware vSphere or vCenter user account with system administrator privileges for Cisco UCS Director.

  You need administrator privileges to connect to and install Cisco UCS Director on VMware vCenter. Cisco UCS Director requires a user account with system administrator privileges to discover, manage and automate VMware vCenter configuration from Cisco UCS Director. These operations include creating, deleting and modifying VMs, ESXi hosts and clusters, datastores and datastore clusters, standard and DV switches, and virtual network port groups.
- Download the Cisco UCS Director software from the Download Software area on Cisco.com.
- Extract the Cisco UCS Director OVF file from the digitally signed zip file to your local disk. See Digitally Signed Images, on page 6.

Minimum System Requirements for a Single-Node Setup

The following tables detail the minimum resource requirements for a single-node setup of . Cisco recommends a single-node setup for installations of up to 5000 VMs.

For optimal performance, the entire memory and CPU allocations specified in the table below should be reserved. Failure to follow these specifications could affect performance. For example, 4 vCPU cores with 3000 MHz and 16G of memory must be reserved for the VM.

The minimum memory required for the **inframgr** service is automatically set during deployment. To enable the **inframgr** service to use more than the minimum required memory, edit the `inframgr.env` file available in the following location:

`/opt/infra/bin/`

In this file, update the MEMORY_MAX parameter to the value you want. To activate the changes, restart the **inframgr** service.

The default memory settings are MEMORY_MIN=8192m and MEMORY_MAX=8192m.

For information about minimum system requirements for a multi-node setup, see the Cisco UCS Director Multi-Node Installation and Configuration Guide.

Table 1: Minimum system requirements for a single-node installation (up to 5,000 VMs)

Element	Minimum Supported Requirement
vCPU	4
Allocated Memory	16 GB
Reserved Memory	16 GB
Disk Space	100 GB

Element	Minimum Supported Requirement
Disk Write I/O Bandwidth	4 MBps
Disk Read I/O Bandwidth	4 MBps
Memory Allocated for **inframgr**	8 GB

Restart the database and all services after making these changes to the `/etc/my.cnf`.

Up to 2,000 VMs

If you plan to manage up to 2,000 VMs, the environment must meet at least the minimum system requirements in the following table.

Table 2: Minimum System Requirements for up to 2,000 VMs

Element	Minimum Supported Requirement
vCPU	4
Memory	16 GB
Primary Disk (Hard Disk 1)	100 GB
Secondary Disk (Hard Disk 2)	100 GB
Disk Read I/O Bandwidth	4 MBps
Disk Write I/O Bandwidth	4 MBps

Up to 5,000 VMs

If you plan to manage no more than 5,000 VMs, the environment must meet at least the minimum system requirements and recommended configurations in the following tables.

Table 3: Minimum System Requirements for up to 5,000 VMs

Element	Minimum Supported Requirement
vCPU	8
Memory	20 GB
Primary Disk (Hard Disk 1)	100 GB
Secondary Disk (Hard Disk 2)	100 GB
Disk Write I/O Bandwidth	4 MBps
Disk Read I/O Bandwidth	4 MBps

You must also edit the **MEMORY_MIN** and **MEMORY_MAX** settings in `/opt/infra/bin/inframgr.env` as follows:

MEMORY_MIN=8192m

MEMORY_MAX=8192m

Restart the inframgr service after making the memory size changes.

Edit the following parameters in the `/etc/my.cnf` file.

Table 4: Minimum Database Configuration

Element	Minimum Supported Configuration
thread_cache_size	100
max_connections	1000
innodb_lock_wait_timeout	100
query_cache_size	128 MB
innodb_buffer_pool_size	2048 MB
max_connect_errors	10000
connect_timeout	20
innodb_read_io_threads	64
innodb_write_io_threads	64

Restart the database and all services after making these changes to the `/etc/my.cnf`.

Installing on VMware vSphere

Note We recommend that you use VMware vCenter for OVF deployment. VMware vCenter versions ESXi 8.0 U1 and ESXi 8.0 U2 are supported. OVF deployment wizards support only IPv4 addresses.

Before you begin

You need administrator privileges to connect to VMware vCenter. Cisco UCS Director requires a user account with system administrator privileges to discover, manage and automate VMware vCenter configuration from Cisco UCS Director. These operations include creating, deleting and modifying VMs, ESXi hosts and clusters, datastores and datastore clusters, standard and DV switches, and virtual network port groups.

Note If you do not want to use DHCP, you need the following information: IPv4 address, subnet mask, and default gateway.

Step 1 In the **Navigation** pane, choose the **Data Center** where you want to deploy Cisco UCS Director.

Step 2 Choose **Datacenter** > **Deploy OVF Template**.

Step 3 In the **Source** pane, do one of the following to choose your OVA source location:

- Choose files , navigate to the location where you downloaded the OVF, choose the OVA file, and click **Open**.
- Replace *FQDN* (Fully Qualified Domain Name) with the path to the URL on your local area network where the OVA file is stored, including the IP address or domain name, and click **Next**.

Step 4 In the **Name and Location** pane, do the following:

a) In the **Name** field, edit the VM name.

b) From the Inventory Location area, choose the inventory location where is being deployed, and click **Next**.

Note If you chose a Data Center in Step 2, option b might not be available.

c) Click **Next**.

Step 5 In the **Compute Resource** pane, choose the required host, and click **Next**.

Step 6 The**Review Details** pane, will display template details ,verify and click **Next**.

Step 7 On the **Select Storage** , choose the storage location for the VM.

Step 8 In the **Disk Format** pane, choose one of the following options and click **Next**:

- **Thick Provisioned (Lazy Zeroed)** format—To allocate storage immediately in thick format. This is the recommended format. All performance data is verified with this format.
- **Thick Provisioned (Eager Zeroed)** format—To allocate storage in thick format. It might take longer to create disks using this option.
- **Thin Provisioned** format—To allocate storage on demand as data is written to disk.

Important We recommend that you do not choose the **Thin Provisioned** format.

Step 9 In the **NetworkMapping** pane, choose the network and click **Next**

Step 10 In the **Properties** pane, enter the following information and click **Next**:

- **Management IP Address**—The management IP address to be used for ens192. If your network uses DHCP, leave the default value of 0.0.0.0.
- **Management IP Subnet Mask**—The management IP subnet mask to be used for ens192. If your network uses DHCP, leave the default value of 0.0.0.0.
- **Gateway IP Address**—The Gateway IP Address to be used for ens192. If your network uses DHCP, leave the default value of 0.0.0.0.
- **Ucsd Root Password**
- **ShellAdmin Password**

Note While deploying the OVA in a **Customise template** window,if no default passwords are populated for root and shelladmin, please enter the default password **`cisco123`** for **root** and **`changeme`** for **shelladmin**.

Step 11 In the **Ready to Complete** pane, do the following:

a) Verify the options that you chose in the previous panes.

b) Click **Finish**to start the deployment process.

Step 12 After the appliance has booted up, copy and paste the management IP address (from the IP address that is shown) into a supported web browser to access the **Login** page.

Step 13 On the **Login** page, enter `admin` as the username and `admin` for the login password.

Step 14 Agree to the **License Agreement** and click the submit button.

Step 15 Generate a **Self-Signed Certificate** by entering the Local domain, day, and password.

Note It will take 30 seconds to restart the Tomcat service.

Step 16 On the **Login** page, enter **admin** as the **username** and **admin** for the **login** password to change the password for the admin user.

For information about upgrading from Cisco UCSD 6.7.4.3/6.8.x.x to Cisco UCSD 6.9, follow the migration process under the Cisco UCS Director Upgrade Guide.

Reserving System Resources

For optimal performance, we recommend reserving extra system resources for beyond the minimum system requirements listed in Minimum System Requirements for a Single-Node Setup, on page 10.

Note For more information about how to reserve system resources, see the VMWare documentation.

Step 1 Log in to VMware vCenter.

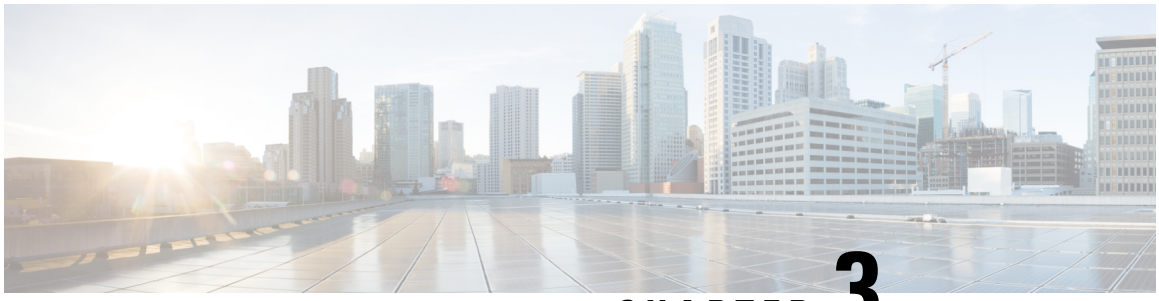
Step 2 Choose the VM for .

Step 3 Shut down the VM.

Step 4 In VMware vCenter, click the **Resource Allocation** tab to view the current resource allocations, and click **Edit.**

Step 5 In the **Virtual Machine Properties** pane, edit resource allocations by choosing a resource and entering the new values.

Step 6 Verify that the new resource allocations have been made.



CHAPTER 3

Installing Cisco UCS Director on Microsoft Hyper-V

for Microsoft Hyper-V

can be deployed in a Hyper-V environment.

Note

- We recommend to deploy on the Hyper-V managed host, rather than the SCVMM console.
- The appliance and bootup logs are located in the `/var/log/ucsd` directory. `install.log` contains the one time appliance installation logs. `bootup.log` contains the appliance boot-up sequence information, such as startup messages for the database and infrastructure services.

Prerequisites

Before you install Cisco UCS Director for Microsoft Hyper-V, complete the following steps:

- Install Microsoft System Center Virtual Machine Manager (SCVMM).

  If you only have a Hyper-V environment, must be deployed on a Hyper-V host.
- Configure an SCVMM user account with administrator privileges for Cisco UCS Director.
- Download the Cisco UCS Director software from the Download Software area on Cisco.com.
- Extract the Cisco UCS Director VHD and db files from the digitally signed zip file to your local disk. See Digitally Signed Images, on page 6.

Minimum System Requirements for a Single Node Setup on Microsoft Hyper-V

The minimum system requirements depend upon how many VMs you plan to manage. We recommend deploying a VM on a local datastore with a minimum of 25 Mbps I/O speed, or on an external datastore with a minimum of 50 Mbps I/O speed.

Note

- For optimal performance, reserve additional CPU and memory resources. We recommend that you reserve the following resources in addition to the minimum system requirements listed in the tables below: CPU resources of more than or equal to 3000MHz, and memory reservation of more than or equal to 1 GB. You should add more vCPUs if the VM's CPU usage is consistently high.
- The minimum memory required for the inframgr service is automatically set during deployment. However, if you want to modify the memory for the inframgr service, edit the inframgr.env file available in the following location:

  /opt/infra/bin/inframgr.env

  In this file, update the "MEMORY_MAX" parameter to the value you want. After changing this parameter, restart the service for the changes to take effect. The default memory settings are MEMORY_MIN=6144 m and MEMORY_MAX=6144 m.

For information about minimum system requirements for a multi-node setup, see Cisco UCS Director Multi-Node Installation and Configuration Guide.

Up to 2,000 VMs

If you plan to manage up to 2,000 VMs, the environment must meet at least the minimum system requirements in the following table.

Table 5: Minimum System Requirements for up to 2,000 VMs

Element	Minimum Supported Requirement
vCPU	4
Memory	16 GB
Primary Disk (Hard Disk 1)	100 GB
Secondary Disk (Hard Disk 2)	100 GB
Disk Read I/O Bandwidth	4 MBps
Disk Write I/O Bandwidth	4 MBps

Up to 5,000 VMs

If you plan to manage no more than 5,000 VMs, the environment must meet at least the minimum system requirements and recommended configurations in the following tables.

Table 6: Minimum System Requirements for up to 5,000 VMs

Element	Minimum Supported Requirement
vCPU	8
Memory	20 GB
Primary Disk (Hard Disk 1)	100 GB
Secondary Disk (Hard Disk 2)	100 GB
Disk Read I/O Bandwidth	4 MBps
Disk Write I/O Bandwidth	4 MBps

You must also edit the **MEMORY_MIN** and **MEMORY_MAX** setting in `/opt/infra/bin/inframgr.env` as follows:

MEMORY_MIN=8192m

MEMORY_MAX=8192m

Edit the following parameters in the `/etc/my.cnf` file.

Table 7: Minimum Database Configuration

Element	Minimum Supported Configuration
thread_cache_size	100
max_connections	1000
innodb_lock_wait_timeout	100
query_cache_size	128 MB
innodb_buffer_pool_size	2 GB
max_connect_errors	10000
connect_timeout	20
innodb_read_io_threads	64
innodb_write_io_threads	64

Note After updating and saving the `/etc/my.cnf` file, you need to restart the database.

Installing on Microsoft Hyper-V

Before you begin

- System administrator privileges for Hyper-V are required.
- Microsoft Windows 2019 with Hyper-V Role or Windows 2022 with Hyper-V Role are required to deploy this release of Cisco UCS Director.

Step 1 Log into the Hyper-V host.

Step 2 Choose **Start** > **Administrative Tools** to open **Hyper-V Manager.**

Step 3 In the **Hyper-V Manager** dialog box, choose **Action** > **New Virtual Machine**.

Step 4 In the **Before You Begin** pane, click **Next**.

Step 5 In the **Name and Location** pane, do the following:

a) In the **Name** field, edit the default VM name.
b) Check the **Store the virtual machine in a different location** checkbox and specify the alternate location.
c) Click **Next**.

Step 6 In the **Select Generation** pane, choose **Generation2**.

With **Generation2**, this virtual machine provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.

Step 7 In the **Assign Memory** pane, enter the amount of memory to allocate to this VM (16 GB minimum) and click **Next**.

Step 8 In the **Configure Networking** pane, click **Next** to accept the default option in the **Connection** field.

The default option is **Not Connected**.

Step 9 In the **Connect Virtual Hard Disk** pane, choose **Attach a virtual disk later** and click **Next**.

Step 10 In the **Completing the New Virtual Machine Wizard** pane, verify the settings and click **Finish**.

Step 11 In the **Navigation** pane, right-click the new VM and choose **Settings**.

Step 12 In the Security pane, deselect the **Enable Secure Boot** checkbox.

Step 13 In the **Navigation** pane, choose **IDE Controller 0**.

Step 14 In the **IDE Controller** pane, choose **Hard Drive** and click **Add**.

Note You need to add two hard drives since we have two VHD files separately for OS and application, and for database.

Step 15 In the **Hard Drive** pane, choose the downloaded .vhd file and click **OK.**

Step 16 Inspect the virtual hard drive properties.

Step 17 In the **Navigation** pane, choose **Memory.**

Step 18 In the **Memory** pane, enter the recommended value (minimum 16 GB).

Step 19 In the **Navigation** pane, choose **Processor**.

Step 20 In the **Processor** pane, enter the recommended value (4 vCPU).

Step 21 Remove the network adapter that was created when you created the new VM.

Step 22 In the **Navigation** pane, choose **Add Hardware**.

Step 23 In the **Add Hardware** pane, choose **Network Adapter** and click **OK**.

Step 24 In the **Navigation** pane, choose the network adapter.

Step 25 In the **Network Adapter** pane, in the **Network** field, choose your network and click **OK**.

Step 26 Verify that you have allocated sufficient vCPU and Memory resources. For the minimum resource requirements, see Minimum System Requirements for a Single Node Setup on Microsoft Hyper-V, on page 16.

Step 27 Power on the VM.

Optionally you can configure network properties from the shelladmin.

By default, this version of Microsoft Hyper-V uses DHCP for address allocation. If you want to use a static IP address instead of DHCP, you can change this configuration through ShellAdmin.

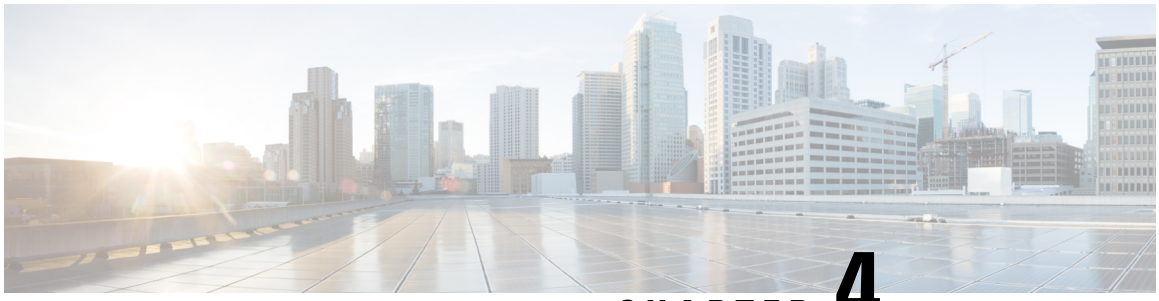
Step 28 After the appliance has booted up, copy and paste the IP address that is displayed into a supported web browser to access the **Login** page.

Step 29 At the login prompt, enter `admin` for username and `admin` for the password to log into .

Note We recommend that you change the default admin password after this initial login.

What to do next

Update your license.



CHAPTER 4

Restarting Cisco UCS Director

This chapter contains the following sections:

Restarting

If you see errors after installing , log in to the Secure Shell (SSH) client and verify whether services are running or not.

Step 1 Log in to the VM console with the shelladmin user credentials:

If this is the first time you have logged into the ShellAdmin after deployment, you will be prompted to change the default password.

Step 2 To display the status of all services, choose `Display services status`.

If this option is not available, you can use SSH to restart the services.

Step 3 Verify that the following services appear:

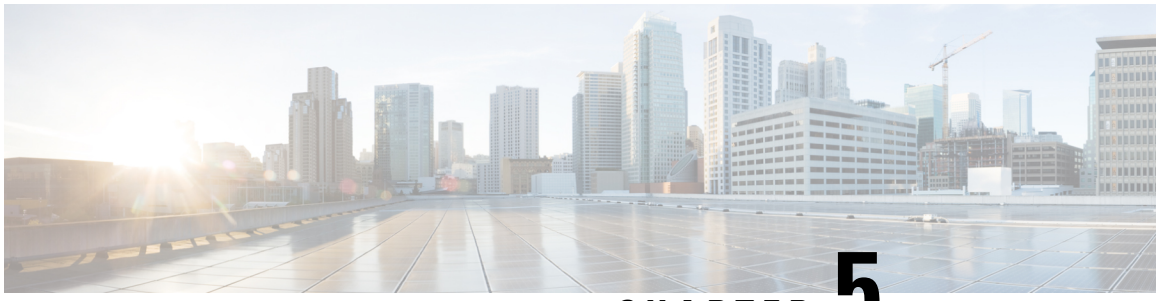
```
 1. broker
 2. controller
 3. eventmgr
 4. idaccessmgr
 5. inframgr
 6. websock
 7. connectormgr
 8. tomcat
 9. flashpolicy
10. mariadbd
```

Note Services that start in the background do not appear in the window.

Step 4 Choose `Stop services`.

Step 5 To verify that all services are stopped, choose `Display services status`.

Step 6 To restart services, choose `Start services`.



CHAPTER 5

Post-Installation Configuration

Changing the Admin Password

You are prompted to change the default admin user password after you log into for the first time. On subsequent login, you can follow these steps to change the admin user password.

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Click the row with the administration user for which you want to change the default password.

Step 4 From the **More Actions** drop-down list, choose **Change Password**.

Step 5 On the **Change Password** screen, enter the old password and then the new password and confirm it.

Step 6 Click **Save**.

Updating the License

Before you begin

If you received a zipped license file by an email, extract and save the license (.lic) file to your local machine.

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **License Keys**.

Step 3 Click **Update License**.

Step 4 On the **Update License** screen, do the following:

a) Drop the `.lic` file from your local system or click **Select a File** and navigate to the location where you stored the `.lic` file.

To enter license text instead of file upload, check the **Enter License Text** checkbox and enter the license text in the **License Text** field.

b) Click **Submit**.

The license file is processed, and a message appears confirming the successful update.

Configuring the Network Interface in ShellAdmin

This procedure is optional.

Step 1 Log in to the VM console with the shelladmin user credentials:

If this is the first time you have logged into the ShellAdmin after deployment, you will be prompted to change the default password.

Step 2 Choose `Configure Network Interface`.

Step 3 At the `Do you want to Configure DHCP/STATIC IP [D/S]` prompt, enter one of the following choices:

- If DHCP is enabled, enter **D** (IP addresses are assigned automatically)
- To configure static IP, enter **S**, and then choose the interface you want to configure at the next prompt followed by the option to select IPv4. This is followed by the confirmation of the interface selected and the version of IP for which you select **Y** to continue. Then enter the following details:
  - IP address
  - Netmask
  - Gateway
  - DNS Server 1
  - DNS Server 2

Step 4 Confirm when prompted.

Changing the Maximum Packet Size

The default maximum packet (query) size for the database queries is 4 MB. If one or more of your pods requires a larger size, we recommend that you increase the configuration of the maximum packet size to 100 MB. For example, the import of large open automation modules typically require a larger packet size.

Note For a multi-node setup, perform this configuration on the inventory database and monitoring database nodes.

Step 1 In the shelladmin, choose `Login as Root` to log in to .

Step 2 Navigate to the `/etc` folder.

Step 3 Open the `my.cnf` file and locate the `max_allowed_packet` parameter.

Step 4 Change the value of the `max_allowed_packet` parameter to **`max_allowed_packet=100M`**

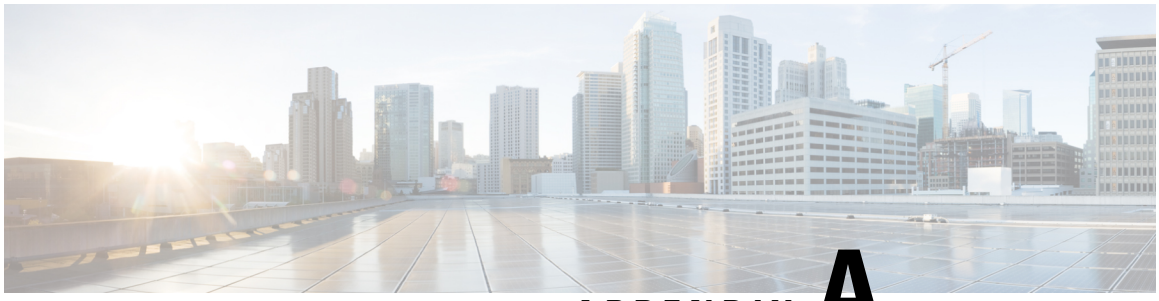
Step 5 Save the `my.cnf` file.

Step 6 In the shelladmin, stop and restart the services on every node, as follows:

a) Choose `Stop services`.

b) To verify that all services are stopped, choose `Display services status`.

c) After all services have stopped on the node, choose `Start services`.



APPENDIX A

Ports

This appendix contains the following sections:

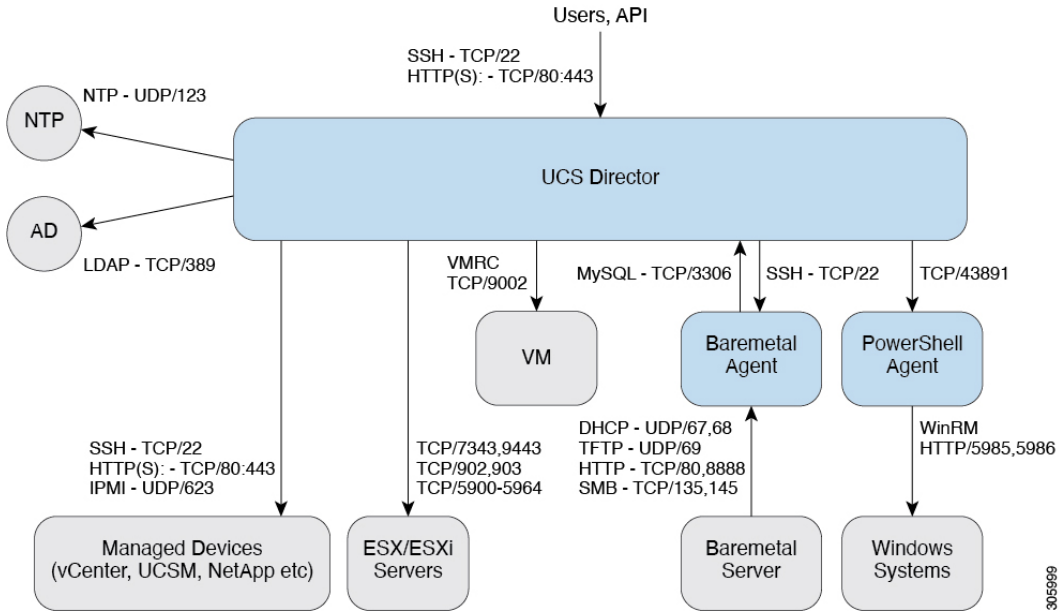
Cisco UCS Director TCP and UDP Port Usage

This section provides a list of the TCP and UDP ports that Cisco UCS Director uses for connections and communications with external applications or devices. The port usage depends upon whether you have deployed Cisco UCS Director on VMware vSphere or Microsoft Hyper-V.

Cisco UCS Director TCP and UDP Port Usage on VMware vSphere

The following figure shows the network ports used for communication between the Cisco UCS Director appliance and managed devices, ESX servers, Bare Metal Agent, PowerShell Agent, NTP, and Active Directory for an installation on VMware vSphere.

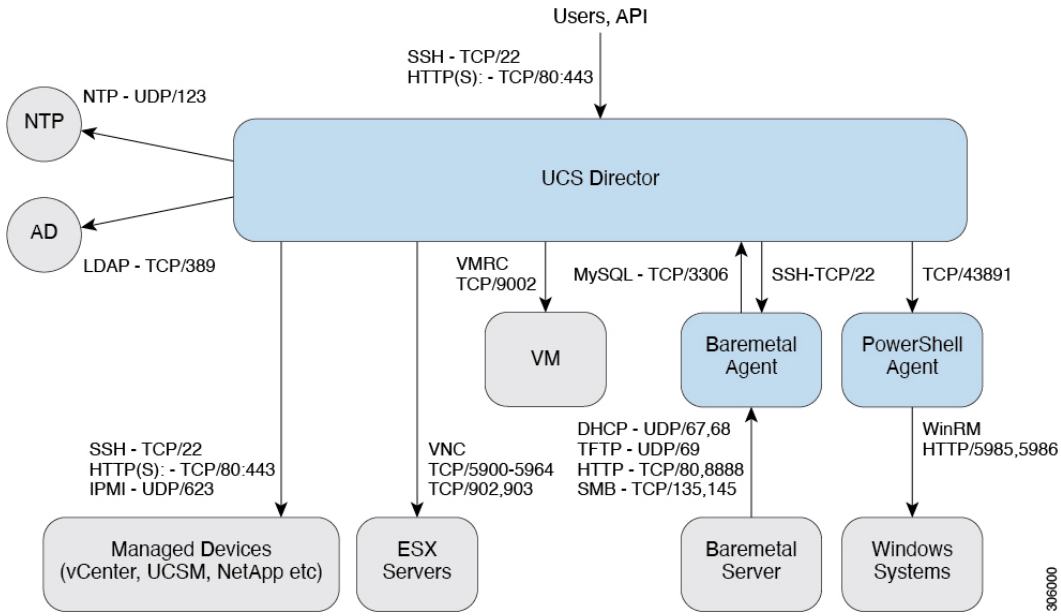
Figure 1: Cisco UCS Director TCP and UDP Port Usage



Cisco UCS Director TCP and UDP Port Usage on Microsoft Hyper-V

The following figure shows the network ports used for communication between the Cisco UCS Director appliance and managed devices, ESX servers, Bare Metal Agent, PowerShell Agent, NTP, and Active Directory for an installation on Microsoft Hyper-V.

Figure 2: Cisco UCS Director TCP and UDP Port Usage



Port List

Default Port	Protocol	Description
22	TCP	SSH
80	TCP/UDP	HTTP
69	TFTP	TFTP for Cisco UCS Director Bare Metal Agent
443	UDP	HTTPS
27000/7279/8082 (Mgmt)	TCP	Citrix licensing
2598/1494/2112/2513	TCP	Virtual Desktop Agent for Desktops
67/68	UDP	DHCP
389/636 3268/3269	TCP/UDP TCP	Active Directory
53	TCP/UDP	DNS
123	TCP/UDP	NTP
3306	TCP/UDP	MariaDB
8787/5900-5964	TCP	+ VNC Connectivity
3389	TCP/UDP	+ RDP Connectivity
80/443/8080	TCP/UDP	+ NetApp Connectivity
80/443	UDP	+ Cisco UCS Manager Connectivity
80/443	UDP	+ vCenter Connectivity
3389	TCP/UDP	RDP
135/445	TCP	SMB/RPC
88	TCP/UDP	Kerberos
137	TCP/UDP	NetBIOS Name (nbname)
138	TCP/UDP	NetBIOS datagram (nbdatagram)
139	TCP	NetBIOS session (nbsession)
80/443	UDP	Desktop Delivery Controller <--> vCenter
8080 through ICA	TCP	Desktop Delivery Controller <--> Virtual Desktops
1494/2598/2512/2513	TCP	Users (Citrix Recvr) <--> Virtual Desktops

Default Port	Protocol	Description
389/636 (LDAP Ports)	TCP/UDP	Desktop Delivery Controller <--> Active Directory
389/636, 3268/3269, 53	TCP/UDP	Virtual Desktops <--> Active Directory + DNS
5985/5986	TCP	PowerShell Agent <-> Xendesktop through WinRM
43891	TCP/UDP	<--> PowerShell Agent
80/8081	TCP	XenApp
902	TCP	VMwareESXi host management and VM customization and to execute VIX tasks
903	TCP	VMwareESXi host management and VM customization and to execute VIX tasks (for Vmware vCenter releases prior to 5.0)
9002	TCP	VMRC Connectivity

Multi-Node Port Requirements

The ports listed in Cisco UCS Director TCP and UDP Port Usage, on page 27 are applicable for both single and multi-node setups.

For a multi-node setup, the following port must be opened between the nodes:

- From the primary nodes to database nodes: port 3306