Cisco UCS Central Prerequisites

This chapter includes the following sections:

- System Requirements for Deploying Cisco UCS Central, page 1
- Supported Hypervisors for Deploying Cisco UCS Central, page 2
- Supported Web Browsers for the Cisco UCS Central GUI, page 3
- Information Required to Deploy Cisco UCS Central, page 3

System Requirements for Deploying Cisco UCS Central

Server Type

We recommend that you deploy Cisco UCS Central on a standalone rack server that is not managed by Cisco UCS Manager or integrated into a Cisco UCS domain. The server must have a high-speed data store, preferably one provisioned from a high-speed storage array.

Required TCP Ports

The following TCP ports must be open between Cisco UCS Manager and a registered Cisco UCS domain for the firmware management and backup functionality to work correctly:

- LOCKD_TCPPORT=32803
- MOUNTD_PORT=892
- RQUOTAD_PORT=875
- STATD_PORT=32805
- NFS_PORT="nfs"(2049)
- RPC_PORT="sunrpc"(111)

Server Requirements

The following table describes the minimum requirements for the standalone rack server on which you deploy Cisco UCS Central.

Table 1: System Requirements for Cisco UCS Central by Hypervisor

Requirement	ESX Minimum Requirement	Hyper-V Minimum Requirement
Disk space	60 GB	60 GB
RAM	4 GB	4 GB
VCPU cores	1 core	2 cores
Disk read speed	> 75 MBps >125 MBps is the recommended speed.	> 75 MBps >125 MBps is the recommended speed.

Note Performance of Cisco UCS Central is not guaranteed if you deploy it on a server that does not meet the minimum disk read speed requirement.

If the disk read speed on the server is lower than the required minimum during the deployment of Cisco UCS Central, the installer displays a warning message but you can complete the deployment. However, if the disk read speed is lower than the required minimum during operation, Cisco UCS Central raises a fault, as shown in the following table, depending upon how low the disk read speed is:

Disk Read Speed on Server	Fault Level
<75 MBps	Critical fault
75 to 100 MBps	Major fault
100 to 125 MBps	Minor fault
>125 MBps	N/A

Supported Hypervisors for Deploying Cisco UCS Central

The following table describes the support for hypervisors on which you can deploy Cisco UCS Central.

Table 2: Supported Hypervisors and Operating Systems

Hypervisors	Supported Versions
Microsoft Hyper-V	Windows 2008 R2 with SP1

Hypervisors	Supported Versions
VMware ESX	• ESX 4.0u2 • ESX 4.1u1 • ESX 5.0

Supported Web Browsers for the Cisco UCS Central GUI

Web browser support for the Cisco UCS Central GUI depends upon the operating system of the computer on which you plan to run Cisco UCS Central GUI.

Operating System	Supported Web Browsers
Microsoft Windows	• Internet Explorer 8 and above • Firefox 3.5 and above • Chrome 14 and above
Mac	• Firefox 3.5 and above • Chrome 14 and above • Safari 5 and above
Linux RHEL	• Firefox 3.5 and above • Chrome 14 and above

Information Required to Deploy Cisco UCS Central

When you deploy Cisco UCS Central, you need to provide the following information:

- Static IPv4 address for Cisco UCS Central
- IPv4 netmask
- Default gateway
- Password to be assigned to the Cisco UCS Central admin account
- Hostname for the virtual machine (VM)
- IPv4 address for the DNS server, if you plan to use one

- Name of the domain, if any, in which you plan to include Cisco UCS Central
- Shared secret, which is the password required when you register Cisco UCS domains with Cisco UCS Central

Guidelines for Cisco UCS Passwords

A password is required for each locally authenticated user account. A user with admin, aaa, or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

Cisco recommends that each user have a strong password. If you enable the password strength check for locally authenticated users, Cisco UCS Central rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.