Cisco UCS Director Shell Guide, Release 6.9

First Published: 2024-05-07

Last Modified: 2025-04-24

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 Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

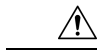
- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

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

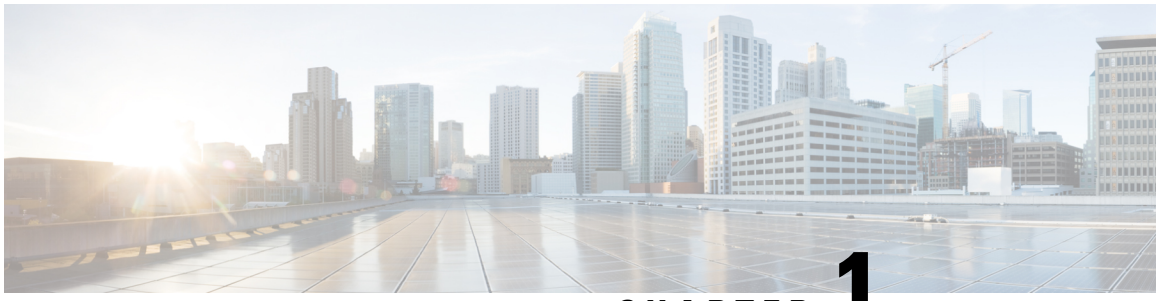
To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results 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 DevNet.
- 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

New and Changed Information for this Release

This chapter contains the following sections:

New and Changed Information

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New Features and Changed Behavior in Cisco UCS Director Shell, Release 6.9(2.0)

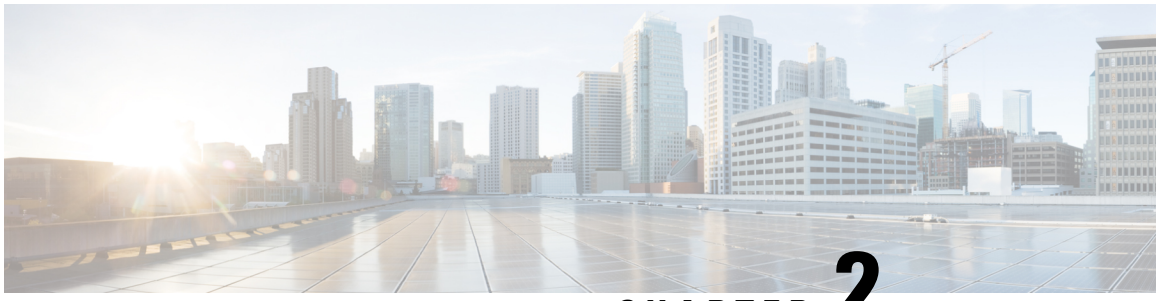
Feature	Description	Where Documented
Shelladmin options for ucsdadmin user	The root user access is disabled and ucsdadmin user access is enabled by default. The following shell admin options are introduced for the ucsdadmin user access: • Manage ucsdadmin Access • Login as ucsdadmin	Managing ucsdadmin Access
Configuring password policy	The new Shell admin option **Configure Password Policy** allows you to define a password policy that must be followed while setting passwords for shelladmin, ucsdadmin, and root users.	Configuring Password Policy

Table 2: New Features and Changed Behavior in Cisco UCS Director Shell, Release 6.9(1.0)

Feature	Description	Where Documented
Scale Setup Configuration	The new Shelladmin option **Configure Scale Setup** allows you to set up the scale configurations based on the VM counts for standalone node or primary and database node.	Configuring Scale Setup
NTP Authentication during time synchronization with NTP Server	The enhanced Shelladmin option **Time Sync** allows you to use NTP server with authentication.	NTP Authentication During Time Sync with NTP Server
Configuring DNS Server with DNSSEC Feature	The Shelladmin option **Configure DNS** allows you to configure a DNS server with DNSSEC feature that enhances DNS security and prevents potential attacks on the network.	Configuring DNS

Table 3: New Features and Changed Behavior in Cisco UCS Director Shell, Release 6.9

Feature	Description	Where Documented
Shell scripts enhancements	Shell options output updated to display additional details	Most of the sections in this guide are updated. • Configuring a Network Interface, on page 27 • Displaying Appliance Network Details, on page 28



CHAPTER 2

Overview

This chapter contains the following sections:

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

Cisco UCS Director Shell

The Cisco UCS Director Shell is a text-based menu that you access through a secure shell (SSH) application and Cisco UCS Director administrator credentials. With the Shell, you can execute commands to perform various system administration tasks, including:

- Patch updates
- Database backup and restore
- Certificate imports
- Services management

About Cisco UCS Director Shell Commands

This guide describes all of the commands available to you when logging in to the Cisco UCS Director shell. You can use these commands to perform the following administrative tasks:

- Quitting the shell
- Changing ShellAdmin password
- Displaying Service Status
- Stopping/starting all Cisco services
- Stopping/starting the database
- Backing up/restoring the appliance database
- Synching up time
- Pinging hostname/IP address
- Version (Cisco UCS Director appliance version)
- Generating self signed certificate and certificate signing request
- Importing CA/self-signed certificate
- Configuring network interface
- Displaying network details
- Enabling the database for a BMA Appliance
- Adding a BMA hostname/IP address to the appliance
- Troubleshooting by using Tail Inframgr logs
- Applying a patch to the appliance
- Shutting down of the Appliance
- Rebooting the Appliance
- Managing root Access
- Logging in as root
- Configuring Multi-node Setup
- Cleaning up Patch Files
- Collecting logs from a node
- Collecting diagnostics
- Enabling/Disabling HTTP access
- Resetting MariaDB user password
- Applying signed patch to the appliance
- Terminating active GUI session(s)
- Regenerating device connector REST API access key
- Granting/Denying client access to MariaDB port 3306
- Managing VMRC Tunneling Service

- Configuring scale setup
- Configuring DNS
- Managing ucsdadmin access
- Logging in as ucsdadmin
- Configuring password policy

For additional system administration information, refer to the Cisco UCS Director Administration Guide, Release 6.9.

Prerequisites

To successfully execute the commands described in this guide, you must meet the following prerequisites:

- Cisco UCS Director should be up and running (and reachable).

Note The information in this guide is based on Cisco UCS Director, release 4.0, and later releases.

Logging in to the Shell

The login procedure requires the use of a Secure Shell (SSH) client and the proper login credentials. After gaining access to Cisco UCS Director, you can perform a wide variety of system administration tasks.

Important We recommend you not to use Ctrl+C while executing the shelladmin options in the Secure Shell (SSH) client, because the user session will be terminated.

Note If you have not reset the default SSH password for shelladmin and ucsdadmin users during OVF/OVA deployment, you will be prompted to change your default password when you login to the Cisco UCS Director using SSH for the first time. Once you reset the default SSH password for the shelladmin and ucsdadmin users, you will be automatically logged out. After resetting the SSH password for the shelladmin and ucsdadmin users, you must login again and reset the default SSH password for the root user.

Before you begin

Obtain proper access to Cisco UCS Director and a secure shell (SSH) application.

Procedure

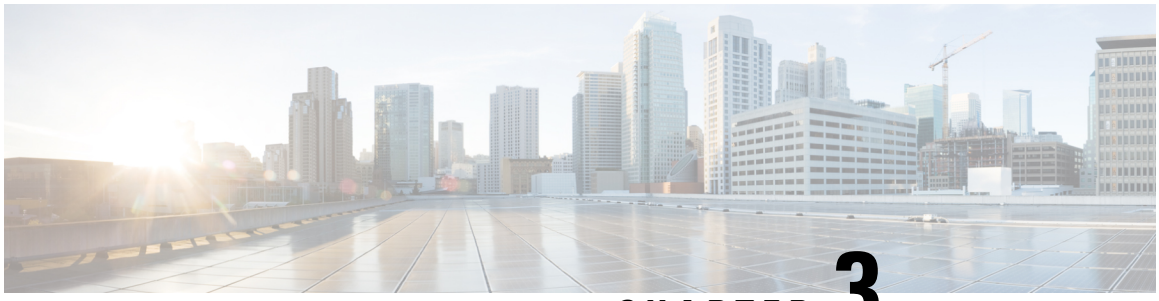
Step 1 Log in to Cisco UCS Director as shelladmin using your SSH terminal client.

Step 2 Press the **Enter** key.

The following services are available for selection:

```
                Cisco UCS Director Shell Menu
Node:Standalone | Version:6.8.0.0 Build:68012  | UpTime:  05:44:00 up 21 days,  3:03


0)  Quit
1)  Change shelladmin Password
2)  Display Services Status
3)  Stop Services
4)  Start Services
5)  Stop Database
6)  Start Database
7)  Backup Database
8)  Restore Database
9)  Time Sync
10) Ping Hostname/IP Address
11) Show Version
12) Generate Self-Signed Certificate and Certificate Signing Request
13) Import CA/Self-Signed Certificate
14) Configure Network Interface
15) Display Network Details
16) Enable Database for Cisco UCS Director Baremetal Agent
17) Add Cisco UCS Director Baremetal Agent Hostname/IP
18) Tail Inframgr Logs
19) Apply Patch
20) Shutdown Appliance
21) Reboot Appliance
22) Manage root Access
23) Login as root
24) Configure Multi Node Setup (Advanced Deployment)
25) Clean-up Patch Files
26) Collect logs from a Node
27) Collect Diagnostics
28) Enable/Disable HTTP
29) Reset MariaDB User password
30) Apply Signed Patch
31) Terminate active GUI session(s) for user
32) Regenerate Device Connector REST API Access Key
33) Grant/Deny client access to MariaDB port 3306
34) Manage VMRC Tunneling Service
35) Configure Scale Setup
36) Configure DNS
37) Manage ucsdadmin Access
38) Login as ucsdadmin
39) Configure Password Policy
```



CHAPTER 3

Using Shell Commands

This chapter contains the following sections:

General Administration

This section describes how to execute common administration tasks such as changing your password, stopping and starting services, generating log and report data, as well as other common system administration tasks.

Examining the Version Information

You can verify the Cisco UCS Director version and build number by choosing **`Show Version`**. This information is required for debugging purposes.

Procedure

Step 1 From the Cisco UCS Director Shell menu choose **Show Version** and press **Enter**.

Information similar to the following is displayed:

```
Cisco UCS Director Platform
-----------------
Version      : 6.9.x.x
Build Number : 22
Press return to continue ...
```

Step 2 Press **Enter** to complete the process.

Changing Your Password

You can change your Cisco UCS Director shell password by choosing **Change shelladmin password**.

Procedure

Step 1 From the **Cisco UCS Director Shell** menu, choose **Change shelladmin password** and press **Enter**. The following information is displayed:

```
Changing password for user shelladmin.
New password:
```

Step 2 Enter your new UNIX password and press the **Enter** key.

Step 3 Enter your new UNIX password once again and press the **Enter** key. The following information is displayed:

```
passwd: all authentication tokens updated successfully.
Press return to logout...
```

Synchronizing the System Time

You can synchronize the system time to the hardware time and the NTP server by choosing **Time Sync**.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Time Sync**.

Step 2 Press **Enter**.

The following information is displayed:

```
Time Sync......
System time is Thu Feb 11 17:41:18 UTC 2021
Hardware time is Thu 11 Feb 2021 05:41:19 PM UTC -0.569097 seconds
Do you want to sync systemtime [y/n]? y
System time reset to hardware clock
Do you want to sync to NTP [y/n]? y
NTP Server(s):
0.centos.pool.ntp.org
1.centos.pool.ntp.org
2.centos.pool.ntp.org
3.centos.pool.ntp.org
Enter NTP server to sync time with: xxx.xx.xx.xx
```

Step 3 Enter the NTP server hostname or IP address, and press **Enter** to synchronize to the NTP server.

The following information is displayed:

```
Enter NTP server to sync time with: xxx.xx.xx.xx
2021-02-11T17:41:50Z chronyd version 3.4 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER
+SIGND +ASYNCDNS +SECHASH +IPV6 +DEBUG)
2021-02-11T17:41:54Z System clock wrong by 199.380705 seconds (step)
2021-02-11T17:45:13Z chronyd exiting
Synchronized time with NTP server 'xxx.xx.xx.xx'
Added NTP server 'xxx.xx.xx.xx' to /etc/chrony.conf
Press return to continue ...
```

Once you have entered an NTP server hostname or IP address, it is added to the list of available NTP servers for future synchronization.

Step 4 Press the **Enter** key to complete the process.

NTP Authentication During Time Sync with NTP Server

The Cisco UCS Director provides a symmetric key-based authentication mechanism for time synchronization with the NTP server. This mechanism allows you to configure the auth key and its value during the initiation of the time sync process. The auth keys are generated by the **chrony** utility and stored in the **chrony.keys** file, where each key is referenced by its Key ID. The Cisco UCS Director verifies if the auth key and its value are valid and associated with the configured NTP server. If the auth key and its value are valid, the Cisco UCS Director confirms that the NTP authentication is successful, ensuring security by preventing chronyd from accepting modified, fake, or redirected packets.

You can use either NTP DNS name or IP address of the NTP server to proceed with the time sync process.

Before you begin

The chrony 4.0 or later version must be installed in the Cisco UCS Director and the NTP server.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Time Sync** and press **Enter**.
The following information is displayed:

```
Time Sync......
System time is Thu Feb 11 17:41:18 UTC 2021
```

```
Hardware time is Thu 11 Feb 2021 05:41:19 PM UTC -0.569097 seconds
Do you want to sync systemtime [y/n]?
```

Step 2 Enter **y** if you want to sync system time or enter **n** if you want to directly sync time to NTP server and press **Enter**.

Note
You can proceed to sync the time to the NTP server irrespective of the options **y** or **n** selected for the system time.

The following information is displayed:

```
Do you want to sync to NTP [y/n]?
```

Step 3 Enter **y** and press **Enter**.
The following information is displayed:

```
Enter NTP server to sync time with:
```

Step 4 Enter the host name or IP address of the NTP server to which the NTP client must have time synchronization.
The following information is displayed:

```
Do you want to authenticate with NTP server [y/n]?
```

Step 5 Enter **y** and press **Enter**.
The following information is displayed:

```
Enter NTP server auth key:
```

Note
If you enter **n** to sync the time with the NTP server without authentication, the following information is displayed:

```
Added NTP server xx.xxx.xx.xxx to /etc/chrony.conf
2024-09-25T10:17:27Z chronyd version 4.3 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER
+SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
2024-09-25T10:17:27Z Frequency -23.073 +/- 0.170 ppm read from /var/lib/chrony/drift
2024-09-25T10:17:27Z Using right/UTC timezone to obtain leap second data
2024-09-25T10:17:31Z System clock wrong by 0.000014 seconds (step)
2024-09-25T10:17:31Z chronyd exiting
Synchronized time from NTP server 'xx.xxx.xx.xxx' without Authentication
Press return to continue ...
```

Step 6 Enter the NTP server auth key and press **Enter**.
The following information is displayed:

```
Enter NTP server auth key value:
```

Note
The auth key and its value can be shared by the NTP server administrator.

Step 7 Enter the NTP server auth key value and press **Enter**.
The following information is displayed:

```
Authenticating with NTP server 'xx.xxx.xx.xxx'
Added NTP server 'xx.xxx.xx.xxx' key 'x' to /etc/chrony.conf
Added NTP server 'xx.xxx.xx.xxx' key 'x' to /etc/chrony.keys
2024-08-14T05:27:28Z chronyd version 4.3 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER
+SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
```

```
2024-08-14T05:27:28Z Frequency -22.133 +/- 0.300 ppm read from /var/lib/chrony/drift
2024-08-14T05:27:29Z Using right/UTC timezone to obtain leap second data
2024-08-14T05:27:33Z System clock wrong by -0.001261 seconds (step)
2024-08-14T05:27:33Z chronyd exiting
Synchronized time with NTP server 'xx.xxx.xx.xxx' with Authentication
Press return to continue ...
```

Note
If you enter NTP DNS name under **Enter NTP server to sync time with**, then the displayed response shows the DNS name instead of IP address.

Applying a Patch to Cisco UCS Director

Choose this option to apply a patch to the appliance.

Note The patch file (zip file) is provided by Cisco UCS Director. Before applying a patch:

- Review the patch release notes and the Readme file.
- Take a snapshot of your VM.
- Take a backup of your database prior to applying the patch. The **Apply Patch** option allows you to take a backup as part of the **Apply Patch** procedure; but the best practice is to take a backup immediately before using the **Apply Patch** option.
- Stop the appliance services.

Before you begin

- Download the patch file
- Place the file in a web server or FTP, SFTP, or SCP server
- Choose **Apply Patch** from the Cisco UCS Director Shell menu
- Provide patch URL (http://WebServer/TestPkg.zip)

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Apply Patch** and press Enter.

The following information is displayed:

```
Applying Patch...
Services will be stopped before upgrade. Do you want to stop the services? [y/n]:
```

Step 2 Enter **y**, and press **Enter**, the services are stopped.

```
Stopping services...
Stopping services... done
Do you want to take database backup before applying patch? [y/n]:
```

Step 3 If you entered **n**, enter the mode of transfer and press **Enter** and provide the required information, as follows:

- SFTP—Enter the SFTP server IP address, server login name and password, and the path to the location where you have stored the upgrade file.
- SCP—Enter the SCP server IP address, server login name and password, and the path to the location where you have stored the upgrade file.
- FTP—Enter the FTP server IP address, server login name and password, and the path to the location where you have stored the upgrade file. For example, **ftp***://username:password@hostname\IP_address/software_location_and_name*.
- HTTP—Enter the URL for the location where you stored the upgrade file.
- FILE—Enter the path to the local directory where you have stored the upgrade file.

```
n
User selected option not to take backup, proceeding with applying patch
Specify the Transfer mode [ftp sftp scp http file]: sftp
Server IP Address: xxx.xx.xxx.xxx
Server Username: xxxxx
Server Password:
SFTP Path to Patch Zip file: cucsd_patch_6_9_1_0_69306.zip
Apply the patch 'cucsd_patch_6_9_1_0_69306.zip'? [y/N]:
```

Note
Refer to the ReadMe file for information about the patches.

Note
Only from Release 6.5, the mode of transfer such as SFTP, SCP, HTTP, and File are supported. This step is applicable only from Release 6.5.

Step 4 If you entered **Y** and press **Enter** the backup process starts. Enter the transfer mode and press **Enter**, and provide the required information.

```
The backup process creates a <filename>.tar.gz file on the system running Cisco UCS Director.
You can copy the file to another server using ftp, sftp, or scp protocol.
Specify the Transfer mode [ftp sftp scp]: sftp
Specify the necessary login credentials
Server IP Address: xxx.xx.xxx.xxx
Server Username: xxxxx
Server Password:
Specify the sub-directory (from Home directory) to store the file.
Do you want to just use your home directory [y/n]? y
Taking backup of db_private_admin database..... done
Taking backup of confmgr_production database.... done
Creating database backup archive... done
Database backup archive: /tmp/database_backup.tar.gz
LOG_FILE=/var/log/ucsd/dba.log
File integrity check is successfull
Warning: Permanently added 'xxx.xx.xxx.xxx' (ECDSA) to the list of known hosts.
File has been copied successfully
Database backup done successfully, proceeding with applying patch
Enter patch file download protocol [sftp scp ftp http file]:sftp
   Server IP Address: xxx.xx.xxx.xxx
   Server Username: xxxx
   Server Password:
   Enter SFTP Path to Patch Zip file:
```

```
SFTP Path to Patch Zip file: cucsd_patch_6_9_1_0_69306.zip
Apply the patch 'cucsd_patch_6_9_1_0_69306.zip'? [y/n]:
```

Note
Refer to the ReadMe file for information about the patches.

Note
Only from Release 6.5, the mode of transfer such as SFTP, SCP, HTTP, and File are supported. Hence, for earlier versions, only FTP transfer mode details are displayed.

Step 5 If you are prompted to confirm that you want to apply the patch, enter **y**, then press **Enter**.

The following information is displayed:

```
y
Checking if the database is running... yes
Downloading the patch...
Successfully Connected to xxx.xx.xxx.xxx
Completed downloading the patch.
```

What to do next

After the patch is applied, start the services on the appliance using the **Start Services** option.

Applying a Signed Patch to Cisco UCS Director

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Apply Signed Patch** and press Enter.

The following information is displayed:

```
Applying Patch...
Services will be stopped before upgrade. Do you want to continue? [y/n]:
```

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Stopping services...
Do you want to take database backup before applying patch? [y/n]:
```

Step 3 If you entered **Y** and press **Enter** the backup process starts. Enter the transfer mode and press **Enter**.

```
The backup process creates a <filename>.tar.gz file on the system running Cisco UCS Director.
You can copy this file to another server using the ftp sftp scp mode.
Specify the transfer mode and login credentials
Specify the transfer mode [ftp sftp scp]:
   Specify the Transfer mode [ftp sftp scp]: sftp
   Specify the necessary login credentials
```

```
   Server IP Address: xxx.xx.xxx.xxx
   Server Username: root
   Server Password:
Specify the sub-directory (from Home directory) to store the file.
Do you want to just use your home directory [y/n]? y
Taking backup of db_private_admin database..........Done
Creating database backup archive... done
Database backup archive: /tmp/database_backup.tar.gz
LOG_FILE=/var/log/ucsd/dba.log
File integrity check is successfull
Warning: Permanently added 'xxx.xx.xxx.xxx' (ECDSA) to the list of known hosts.
File has been copied successfully
Database backup done successfully, proceeding with applying patch
Enter patch file download protocol [sftp scp ftp http file]:sftp
   Server IP Address: xxx.xx.xxx.xxx
   Server Username: xxxx
   Server Password:
   Enter SFTP Path to Patch Zip file:
Apply the patch '/opt/mytest123/cucsd_patch_6_9_1_0_69306_signed.zip? [y/n]:
```

Note
Refer to the ReadMe file for information about the patches.

Step 4 If you entered **n**, enter the desired patch file download protocol and press **Enter** and provide the required information, as follows:

- SFTP—Enter the SFTP server IP address, server login name and password, and the path to the location where you have stored the signed zip file.
- SCP—Enter the SCP server IP address, server login name and password, and the path to the location where you have stored the signed zip file.
- FTP—Enter the FTP server IP address, server login name and password, and the path to the location where you have stored the signed zip file. For example, **ftp***://username:password@hostname\IP_address/software_location_and_name*.
- HTTP—Enter the URL for the location where you stored the signed zip file.
- FILE—Enter the path to the local directory where you have stored the signed zip file.

```
n
User selected option not to take backup, proceeding with applying patch.
Enter patch file download protocol [ftp sftp scp http file]: scp
Server IP Address: xxx.xx.xxx.xxx
Server Username: root
Server Password:
Full Patch to Patch Zip File: /opt/mytest123/cucsd_patch_6_9_1_0_69306_signed.zip
Apply the patch '/opt/mytest123/cucsd_patch_6_9_1_0_69306_signed.zip? [y/n]:
```

Step 5 If you are prompted to confirm that you want to apply the patch, enter **y**, then press **Enter**.

The following information is displayed:

```
y
Checking if database is running ...yes
Downloading the patch...
Successfully Connected to xxx.xx.xxx.xxx
Completed downloading the patch.
Verifying patch signature...
Successfully verified the signature of patch file /opt/mytest123/cucsd_patch_6_9_1_0_69306_signed.zip
Proceeding with patch installation
```

Note

From this release, you can use the **Apply Signed Patch** option in the Shell menu to apply signed patch. If you want to upgrade to release 6.5, you should download the signed zip files, extract the files and follow the instructions available in the ReadMe file to manually verify the signature of the patch. Once the image is verified, you can apply the patch zip file using the **Apply Patch** option.

Shutting Down the Appliance

Choose this option to shut down a Cisco UCS Director appliance.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Shutdown Appliance** option and press **Enter**.

The following information is displayed.

```
Do you want to Shutdown appliance [y/n] ?:
```

Step 2 Enter **y** to shut down the appliance. The following information is displayed:

```
Shutting down the Cisco UCS Director Appliance....
```

Step 3 Press the **Enter** key to return to the main menu.

Rebooting an Appliance

Choose this option to reboot a Cisco UCS Director appliance.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Reboot Appliance** option and press the **Enter** key.

The following information displays:

```
Do you want to Reboot appliance [y/n] ?:
```

Step 2 Enter **y** to reboot the appliance. The following information is displayed:

```
Rebooting the Cisco UCS Director Appliance...
Broadcast message from root (pts/5) (Wed Sep 18 13:12:06 2013):

The system is going down for reboot NOW!
Rebooting successful
Press return to continue...
```

Step 3 Press the **Enter** key to return to the main menu.

Using a Multi-Node Setup

The multi-node setup is supported for Cisco UCS Director on VMware vSphere only. With a multi-node setup, you can scale Cisco UCS Director to support a larger number of VMs than is supported by a single installation of Cisco UCS Director. This setup has the following nodes:

- Database node—This node hosts the database service.
- Primary node—This node runs the software services and also acts as the front-end user interface node.

For more information about how to configure the primary node and database nodes, and how to assign system tasks, see the Cisco UCS Director Multi-Node Installation and Configuration Guide

Terminating Active GUI Sessions

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **`Terminate active GUI session(s) for user`** and press Enter.

The following information is displayed:

```
On a subsequent login, all active session(s) for the user will be terminated.
This utility is for terminating the GUI sessions after the specified maximum concurrent sessions for
 a user is reached.
Do you want to proceed [y/n]? :
```

Step 2 Enter **`y`** and press **`Enter`**.

The following information is displayed:

```
Specify the user name of the user session(s) that needs to be terminated :
```

Step 3 Enter the user name and press **`Enter`**.

```
Specify the user session(s) that need to be terminated [a) Oldest, b) All] a/b :
```

Step 4 Enter a or b based on the requirement and press **`Enter`**. On Subsequent login, the user GUI session(s) will be terminated, and you are allowed to log in.

Granting Client Access to MariaDB Port

Choose this option to allow the external clients to access the MariaDB port.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Grant/Deny client access to MariaDB port 3306** option and press **Enter**.

The following information displays:

```
Grant provide external clients access to MariaDB port 3306. Deny blocks external clients access to
MariaDB port 3306 for the granted ip address.

Source IP's configured
----------------------
xx.xxx.xxx.xx/0
----------------------

Grant/deny external clients access to MariaDB port 3306 [g/d]? :
```

Step 2 Enter **g** and press **Enter**.

The following information is displayed:

```
Enter the ip address you want to grant access to MariaDB port 3306 :
```

Step 3 Enter the IP address and press **Enter**.

The following information is displayed:

```
Enabling firewall rules for ip xx.xxx.xxx.xx
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Press return to continue...
```

Note
You can enter 0.0.0.0 (IP address) if you want to grant access to all the clients.

Step 4 Press **Enter** to return to complete the process.

Denying Client Access to MariaDB Port

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Grant/Deny client access to MariaDB port 3306** option and press **Enter**.

The following information displays:

```
Grant provide external clients access to MariaDB port 3306. Deny blocks external clients access to
MariaDB port 3306 for the granted ip address.

Source IP's configured
----------------------
```

```
xx.xxx.xxx.xx
----------------------

Grant/deny external clients access to MariaDB port 3306 [g/d]? :
```

Step 2 Enter **d** and press **Enter**.

The following information is displayed:

```
Enter the ip address you want to deny access to MariaDB port 3306 :
```

Step 3 Enter the IP address and press **Enter**.

The following information is displayed:

```
Successfully denied ipaddress xx.xxx.xxx.xx provided...
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Press return to continue...
```

Step 4 Press **Enter** to return to complete the process.

Regenerating Device Connector REST API Access Key

The device connector key is the authentication key that Cisco Intersight uses to connect to the Cisco UCS Director appliance. The Cisco UCS Director appliance has an unique device connector key to identify itself. Choose this option to generate the device connector key.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Regenerating Device Connector REST API Access Key** option and press the **Enter** key.

Step 2 Press the **Enter** key to return to the main menu.

Managing VMRC Tunneling Service

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Manage VMRC Tunneling Service**.

The following information is displayed:

```
VMRC Tunneling Service Menu
===========================
Options:
  1) Start VMRC Tunneling Service
  2) Status VMRC Tunneling Service
```

```
3) Stop VMRC Tunneling Service
4) Exit
```

Step 2 If you choose Start VMRC Tunneling Service option, a response similar to the following appears:

```
Type in option number and press <Enter> : 1
Starting VMRC Tunneling service...                [ OK ]
Press return to continue...
```

Note
When you try to start a VMRC Tunneling service that is already running, a message will be displayed regarding the service status.

Step 3 If you choose Status VMRC Tunneling Service option, a response similar to the following appears:

```
Type in option number and press <Enter> : 2
VMRC Tunneling Service RUNNING         13539
Press return to continue...
```

Step 4 If you choose Stop VMRC Tunneling Service option, a response similar to the following appears:

```
Type in option number and press <Enter> : 3
Stoping VMRC Tunneling Service [PID=13539]
Press return to continue...
```

Configuring Scale Setup

The **Configure Scale Setup** Shelladmin option streamlines the configuration process for the Cisco UCS Director's InfraMgr component, ensuring seamless scalability. By automatically allocating the necessary memory and configuring the database according to system requirements, this Shelladmin option eliminates the need for manual intervention, saving time and reducing the risk of errors. The Shelladmin option enables you to efficiently manage and scale your infrastructure for sustained performance and reliability.

The following procedure is an example of how to perform scale setup with the standalone node.

Before you begin

Configure the required amount of CPU, memory, and disk space of the Cisco UCS Director appliance in **VMware vCenter**. For more details about the guidelines on system requirements, see Cisco UCS Director Standalone Installation Guide for standalone node setup and Cisco UCS Director Multi-Node Installation and Configuration Guide for primary and database node setup.

Procedure

Step 1 From the **Cisco UCS Director Shell** menu, choose **`Configure Scale Setup`** and press **`Enter`**.

The following information is displayed:

```
Starting Scale Setup Configuration
Current node type: standalone
```

```
Note: Ensure the UCSD appliance meets the minimum CPU, memory, and disk space requirements as per
the Cisco UCS Director Standalone Installation Guide.

Have you allocated the above minimum system requirements for the current node type (standalone)?(y/n):
```

Step 2 Ensure that you have allocated the minimum system requirements for the current node type and press **Enter**.

The following information is displayed:

```
Proceeding with the setup...
Enter the number of VMs you want to set up (upto 5000):
```

Step 3 Enter the number of required VMs and press **Enter**. To know about the VM limit for each node, see the table below.

Node	VM Limit
Standalone	1–5000
Primary	1–50000
Database	1–50000

If the entered value is within the allowed limit, the following message is displayed:

```
Number of VMs is within the valid range: value
Updating memory allocation and database settings for standalone node...
Standalone node configuration updated successfully.
Restart the Database and UCSD services to make the changes effective.
Press return to continue ...
```

If the entered value exceeds the allowed limit, the following message is displayed:

```
ERROR: Number of VMs exceeds the limit for a standalone node (5000).
Enter the number of VMs you want to set up (upto 5000):
```

Step 4 Based on the current node, from the **Cisco UCS Director Shell** menu, perform the following for the changes to take effect:

- **Standalone node**—Stop Database, Start Database, Stop Services, and Start Services
- **Primary node**—Stop Services and Start Services
- **Database node**—Stop Database and Start Database

Upon successful scale setup configuration, the inframgr memory allocation and database configuration values are automatically updated in the **/opt/infra/bin/inframgr.env** and **/etc/my.cnf** files respectively.

Configuring DNS

DNSSEC (Domain Name System Security Extensions) is an important feature in AlmaLinux 9 OS for enhancing the security and integrity of DNS operations. In Cisco UCS Director 6.9(1.0), DNSSEC support is introduced to enhance the DNS security and ensure the integrity of DNS responses. The implementation involves configuring DNSSEC in the DNS settings, providing cryptographic validations for DNS queries and protecting your network against different potential attacks such as DNS spoofing and cache poisoning. By adding cryptographic signatures to the DNS records, the DNSSEC ensures that the responses to the DNS queries are

authentic and have not been tampered with during data transmission. This provides an additional layer of protection for your network against various types of attacks, where the attackers could redirect the users to the malicious websites by providing fraudulent DNS responses, ensuring that the DNS queries and responses are trustworthy and secure.

The Cisco UCS Director 6.9(1.0) allows the shelladmin to configure the DNS servers with or without DNSSEC support.

Procedure

Step 1 From the **Cisco UCS Director Shell** menu, choose **`Configure DNS`** and press **`Enter`**.

The following information is displayed:

```
Starting DNS Configuration.
Active connection found: ens192
Choose DNS configuration:
1) Configure DNS
2) Configure DNS with DNSSEC Enabled
3) Exit
Enter option (1, 2, or 3):
```

Step 2 Choose one of the following DNS configurations:

- Configure DNS
- Configure DNS with DNSSEC Enabled

Step 3 To configure a DNS server (without DNSSEC), enter **`1`** and press **`Enter`**.

The following information is displayed:

```
Option 1: Configure DNS selected.
Enter DNS Server 1 IP address (mandatory):
```

Step 4 Enter the IP address of the DNS server 1 which is mandatory and press **`Enter`**.

The following information is displayed:

```
Enter DNS Server 2 IP address (optional):
```

Step 5 (Optional) Enter the IP address of the DNS server 2 and press **`Enter`**.

The following information is displayed:

```
Connection 'ens192' successfully deactivated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/6
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/7)
DNS settings updated: DNS1=xx.xxx.xx.xxx, DNS2='None'
Press return to continue ...
```

Note
The above message shows that DNS2='None' as the IP address of DNS server 2 is not entered as it is optional. If the IP address of DNS server 2 is entered, the message shows as DNS2='IP address'.

Step 6 To configure a DNS server with DNSSEC, enter **`2`** and press **`Enter`**.

The following information is displayed:

```
Option 2: Configure DNS with DNSSEC Enabled selected.
Enter Domain Name:
```

Step 7 Enter the domain name.

The following information is displayed:

```
Enter DNS Master Server IP address:
```

Step 8 Enter the IP address of the DNS master server.

The following information is displayed:

```
Enter DNS Slave Server IP address:
```

Step 9 Enter the IP address of the DNS slave server.

The following information is displayed:

```
AD flag is present.
Current DNS query status: NOERROR
DNSSEC validation successful.
Connection 'ens192' successfully deactivated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/7)
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/8)
DNS settings updated with DNSSEC: Master=8.8.8.8, Slave=8.8.4.4
Press return to continue ...
```

Note
If the DNS server configuration with DNSSEC feature is not successful due to invalid domain name or Master/Slave IP addresses or some other reasons, the following error message is displayed:

```
AD flag is not present.
Current DNS query status: REFUSED
DNSSEC validation failed. AD flag or NOERROR status missing. Consider using the 'Configure DNS'
option.
```

Configuring Password Policy

The Cisco UCS Director Shell admin console allows you to configure a password policy for users such as shelladmin, ucsdadmin, and root. This configuration enforces strong password requirements to ensure the security of the Cisco UCS Director appliance.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **`Configure Password Policy`**, and press **`Enter`**.
The password policy criteria is displayed.

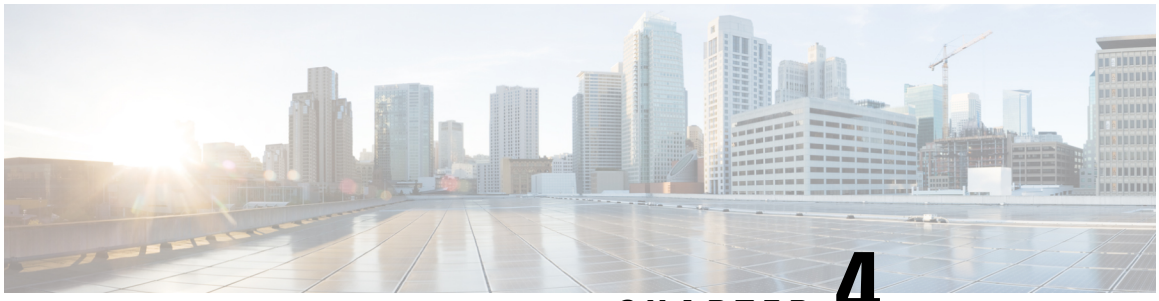
Criteria	Minimum Range	Maximum Range	Default Value
Minimum Password Length	6	80	8
Minimum Character Classes	0	4	4

Criteria	Minimum Range	Maximum Range	Default Value
Minimum Lowercase Letters	-5	0	-1
Minimum Uppercase Letters	-5	0	-1
Minimum Digits	-5	0	-2
Minimum Special Characters	-5	0	-1
Minimum Unique Characters from Old Password	0	5	2
Maximum Sequential Identical Characters Allowed	0	5	3
Maximum Retry Attempts	0	5	5
Number of Old Passwords Remembered	0	15	10
Enforce Policy for root	Yes/No		Yes

Step 2 Press **Enter** to keep the default values or enter a new value within the given range and press **Enter**.
The following information is displayed:

```
Password policy updated successfully in /etc/security/pwquality.conf and /etc/security/pwhistory.conf
Press return to continue ...
```

Note
When a shelladmin, ucsdadmin, or root user attempts to set a new password, the user must adhere to the configured password policy.



CHAPTER 4

Configuring Network Details

This chapter contains the following sections:

Configuring a Network Interface

You can configure a network interface for the Cisco UCS Director appliance by choosing **Configure Network Interface**.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Configure Network Interface** and press Enter.

```
After configuring the network interface, you must restart the Cisco UCS Director services for the
updated network configuration to be used.
Do you want to Configure DHCP/STATIC IP  [d/s] ? :
```

Step 2 Choose one of the following configuration selections:

- Choose **d** to configure a DHCP IP address.
- Choose **s** to configure a static IP address.

Step 3 To configure a static IP address, enter **s** and press **Enter**. The following information is displayed.

```
Configuring STATIC configuration..
Enter the ethernet interface that you want to configure [ens192/ens224]:
```

Step 4 Enter the Ethernet interface to configure (for example, ens192) and press **Enter**. The following information is displayed:

```
Do you want to configure IPv4 STATIC IP for ens192 [y/n]
```

Step 5 Enter **y** and press **Enter**. The following information is displayed:

```
IP Address: xxx.xx.xxx.xx
```

```
   Netmask: 255.255.255.192
   Gateway IP address: xxx.xx.xxx.x
   DNS Server1:
   DNS Server2:
Configuring Network with : INTERACE(ens192), IP(xxx.xx.xxx.xx), Netmask(255.255.255.192),
Gateway(xxx.xx.xxx.x),DNS Server1(), DNS Server2()
Do you want to continue [y/n]?
```

Step 6 Enter **n** to discontinue the configuration process. Press **Enter** to complete the process.

Step 7 To configure a DHCP IP address, enter **d** and press **Enter**. The following information is displayed.

```
Configuring DHCP configuration..
Enter the ethernet interface that you want to configure [ens192/ens224]:
```

Step 8 Enter the Ethernet interface to configure (for example, ens192) and press **Enter**. The following information is displayed:

```
Do you want to configure IPv4 [v4]:
```

Step 9 To configure IPv4, enter **v4** and press **Enter**. The following information is displayed:

```
Not in Static IP Mode
Do you want to configure DHCP [IPv4] for ens192 [y/n]?
```

Step 10 Enter **y** to configure DHCP [IPv4] for ens192 and press **Enter**. The following information is displayed:

```
Configuring DHCP IP for ens192
Successfully configured DHCP IP for ens192
```

Step 11 Press **Enter** to return to the main menu.

Displaying Appliance Network Details

You can display the Cisco UCS Director appliance network details by choosing the **Display Network Details** option.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Display Network Details** option and press **Enter**.

The following information is displayed:

```
Network details....
ens192
          Link encap:Ethernet HWaddr 00:50:56:97:1E:2D
          inet addr:xxx.x.x.xx Bcast:xxx.x.x.xxx Mask:255.255.255.0
          inet6 addr: fe80::230:56gg:fe97:1e2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:189818223 errors:14832 dropped:17343 overruns:0 frame:0
          TX packets:71520969 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:105749301003 (98.4 GiB) TX bytes:27590555706 (25.6 GiB)
          Interrupt:59 Base address:0x2000

lo        Link encap:Local Loopback
```

```
            inet addr:xxx.x.x.x  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:1821636581 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1821636581 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:327846827946 (305.3 GiB)  TX bytes:327846827946 (305.3 GiB)

Press return to continue ...
```

Step 2 Press **Enter** to complete the process.

Configuring DNS

DNSSEC (Domain Name System Security Extensions) is an important feature in AlmaLinux 9 OS for enhancing the security and integrity of DNS operations. In Cisco UCS Director 6.9(1.0), DNSSEC support is introduced to enhance the DNS security and ensure the integrity of DNS responses. The implementation involves configuring DNSSEC in the DNS settings, providing cryptographic validations for DNS queries and protecting your network against different potential attacks such as DNS spoofing and cache poisoning. By adding cryptographic signatures to the DNS records, the DNSSEC ensures that the responses to the DNS queries are authentic and have not been tampered with during data transmission. This provides an additional layer of protection for your network against various types of attacks, where the attackers could redirect the users to the malicious websites by providing fraudulent DNS responses, ensuring that the DNS queries and responses are trustworthy and secure.

The Cisco UCS Director 6.9(1.0) allows the shelladmin to configure the DNS servers with or without DNSSEC support.

Procedure

Step 1 From the **Cisco UCS Director Shell** menu, choose **Configure DNS** and press **Enter**.

The following information is displayed:

```
Starting DNS Configuration.
Active connection found: ens192
Choose DNS configuration:
1) Configure DNS
2) Configure DNS with DNSSEC Enabled
3) Exit
Enter option (1, 2, or 3):
```

Step 2 Choose one of the following DNS configurations:

- Configure DNS
- Configure DNS with DNSSEC Enabled

Step 3 To configure a DNS server (without DNSSEC), enter **1** and press **Enter**.

The following information is displayed:

```
Option 1: Configure DNS selected.
Enter DNS Server 1 IP address (mandatory):
```

Step 4 Enter the IP address of the DNS server 1 which is mandatory and press **Enter**.

The following information is displayed:

```
Enter DNS Server 2 IP address (optional):
```

Step 5 (Optional) Enter the IP address of the DNS server 2 and press **Enter**.

The following information is displayed:

```
Connection 'ens192' successfully deactivated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/6
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/7)
DNS settings updated: DNS1=xx.xxx.xx.xxx, DNS2='None'
Press return to continue ...
```

Note
The above message shows that DNS2='None' as the IP address of DNS server 2 is not entered as it is optional. If the IP address of DNS server 2 is entered, the message shows as DNS2='IP address'.

Step 6 To configure a DNS server with DNSSEC, enter **2** and press **Enter**.

The following information is displayed:

```
Option 2: Configure DNS with DNSSEC Enabled selected.
Enter Domain Name:
```

Step 7 Enter the domain name.

The following information is displayed:

```
Enter DNS Master Server IP address:
```

Step 8 Enter the IP address of the DNS master server.

The following information is displayed:

```
Enter DNS Slave Server IP address:
```

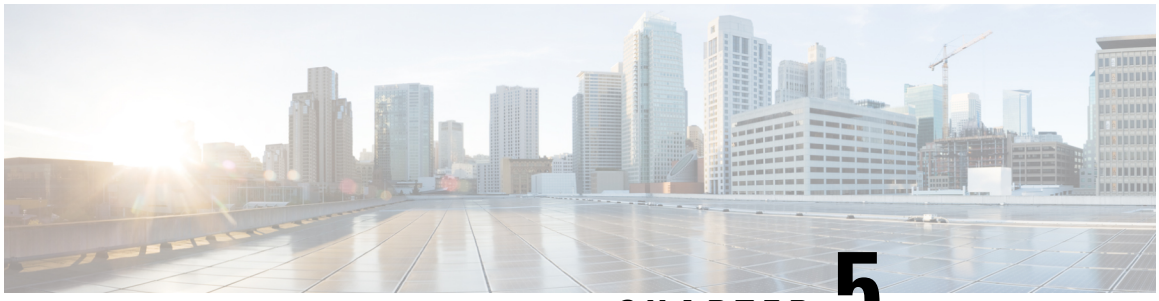
Step 9 Enter the IP address of the DNS slave server.

The following information is displayed:

```
AD flag is present.
Current DNS query status: NOERROR
DNSSEC validation successful.
Connection 'ens192' successfully deactivated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/7)
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/8)
DNS settings updated with DNSSEC: Master=8.8.8.8, Slave=8.8.4.4
Press return to continue ...
```

Note
If the DNS server configuration with DNSSEC feature is not successful due to invalid domain name or Master/Slave IP addresses or some other reasons, the following error message is displayed:

```
AD flag is not present.
Current DNS query status: REFUSED
DNSSEC validation failed. AD flag or NOERROR status missing. Consider using the 'Configure DNS'
option.
```



CHAPTER 5

Managing Cisco Services

This chapter contains the following sections:

Displaying the Status of Your Services

The Display Services option displays all executed services. The Display Services option also displays the status of any associated databases and disks.

- Broker - An ActiveMQ JMS broker used for inter-process communication using JMS messages. All infra services use the broker to communicate between them.
- Controller
- Eventmgr
- Client
- Idaccessmgr - Provides authentication service for Cisco UCS Director users (local, AD imported through LDAP). When you log in through the GUI, tomcat receives the login request and queries idaccessmgr to authenticate the user.
- Inframgr - The back-end server that proves APIs over JMS and REST. Tomcat (GUI) uses these back-end APIs.
- Websock - VNC proxy. Cisco UCS Director provides browser-based VNC access to the VM console. The websock service acts as a VNC proxy to the VM console.
- Tomcat - Hosts Cisco UCS Director GUI web app.
- Flashpolicyd

Note Ensure that all of the above services are up and operating. If a service is not executed on Cisco UCS Director, restart the service through the shell client.

Procedure

From the Cisco UCS Director Shell menu, choose the **Display Service Status** option and press **Enter**.

The following information is displayed.

```
Enter selection [0 to exit]: 2
Service         State      PID        %CPU %MEM    tELAPSED #Threads
-------------   -------    --------   -----------------------------------
broker          UP         14338       0.4  1.1       44:58 31
controller      UP         14517       0.3  1.3       44:11 74
eventmgr        UP         14738       2.0  3.5       43:24 96
idaccessmgr     UP         14939       1.7  3.2       43:17 96
inframgr        UP         15138      25.2 23.0       43:08 463
websock         UP         15231       0.0  0.0       43:02 1
connectormgr    UP         15383       1.4  2.4       42:54 52
tomcat          UP         15477       3.0  4.2       42:47 56
flashpolicyd    UP         15501       0.0  0.0       42:32 1
mariadbd        UP         13754      41.0 10.7       45:08 83

Database        IP Address           State      Client               Connections
-------------   ------------         --------   --------------       ------------
infradb         xxx.x.x.x            UP         xxx.x.x.x            66

Volume                    Mounted on      Size       Used       Available       %Use       Usage
----------------------    -------------   -------    --------   ---------       ------     -------------
/dev/mapper/almalinux-root   /              94G        14G        76G             16%        NORMAL
/dev/sda1                 /boot           976M       123M       787M            14%        NORMAL
infradb_vg-infradb_lv     /infradb        99G        5.2G       94G             6%         NORMAL

Press return to continue ...
```

Note
The corresponding status and process ID (PID) of each service is also displayed in the menu. In a multi-node setup, the status is also displayed for any inventory databases or monitoring databases.

Stopping Cisco Services

You can stop all Cisco services that are part of the Cisco UCS Director appliance by choosing **Stop Services**. You can verify that all services are stopped by choosing **Display Service Status**.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Stop Services**.

Step 2 Press **Enter**.

The following information displays:

```
Do you want to stop services [y/n]? : y
Stopping service broker...                  [ OK ]
```

```
Stopping service controller...              [ OK ]
Stopping service eventmgr...                [ OK ]
Stopping service client...                  [ OK ]
Stopping service idaccessmgr...             [ OK ]
Stopping service inframgr...                [ OK ]
Stopping service websock...                 [ OK ]
Stopping service tomcat...                  [ OK ]
Stopping service flashpolicyd...            [ OK ]
Press return to continue ...
```

Step 3 Press **Enter** to complete the procedure.

Starting Cisco Services

You can execute all services that are part of Cisco UCS Director by choosing **Start Services**.

After using this option, you can choose **Display Service Status** to verify that all services are executed.

Note Services started in the background are not displayed.

Procedure

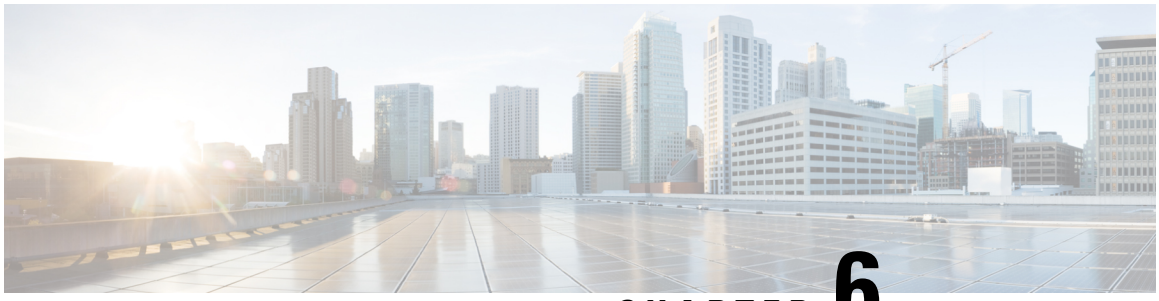
Step 1 From the Cisco UCS Director Shell menu, choose **Start Services**.

The following information is displayed:

```
Services are being started. Use "Display Services Status" option to check the status
Press return to continue ...
```

Step 2 Press **Enter** to complete the process.

Step 3 Choose **Display Service Status** to verify that the services are executed.



CHAPTER 6

Managing Databases

This chapter contains the following sections:

Working with Databases

This section describes how to enable, start and stop, as well as backup and restore a database.

Stopping the Database

You can halt the mariadb daemon (mariadbd) by choosing the **Stop Database** option. This option stops all of the following Cisco services:

- Broker
- Controller
- Eventmgr
- Client
- Idaccessmgr
- Inframgr
- Websock (VNC interface)
- Tomcat
- Flashpolicyd

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Stop Database** option.

The following information is displayed:

```
Do you want to stop database [y/n]? y
Stopping infra services...
Stopping services...
Stopping service broker...                  [DOWN]
Stopping service controller...              [DOWN]
Stopping service eventmgr...                [DOWN]
Stopping service idaccessmgr...             [DOWN]
Stopping service inframgr...                [DOWN]
Stopping service websock...                 [DOWN]
Stopping service connectormgr...            [DOWN]
Stopping service tomcat...                  [DOWN]
Stopping service flashpolicyd...            [DOWN]
Stopping services... done
Stopping database...
The database is stopped.
Database stopped
Press return to continue ...
```

Step 2 Choose **Display Service Status** option to verify that the Cisco services have been stopped on the database. The database status displays as down with no connections.

Starting the Database

You can start the mariadb daemon (mariadbd) by choosing the **Start Database** option.

Note This option starts the appliance database only.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Start Database** option.

Step 2 Press **Enter**.

The following information is displayed:

```
Starting database...
Checking if MariaDB database is running... ..................UP
Database started.
Press return to continue ...
```

Note
The Cisco services are not started automatically when you start the appliance database. Choose the **Start Services** option to start the Cisco services.

Step 3 Choose **Display Service Status** option to verify that the Cisco services have been started on the database. The database status displays as up and list the number of connections.

Backing Up the Database

You can backup the appliance database to an FTP, SFTP, or SCP server.

You need the following information in order to execute the task:

- FTP, SFTP, or SCP server's IP address (from where the database is backed up)
- Server's IP address (where the database is backed up)
- Server's login credentials

Note After the server credentials are provided, the entire database of the Cisco UCS Director appliance is backed up at the specified server location. You then can start the Cisco services by choosing the **Start Services** option.

Before you begin

Stop the Cisco services by using the Cisco UCS Director Shell **Stop Services** option.

Procedure

Step 1 If you have not already done so, stop the Cisco services by using the **Stop Services** option. Refer to the Shell documentation about using that option.

Step 2 From the Cisco UCS Director Shell menu, choose the **Backup Database** option and press **Enter**.

The following information is displayed:

```
Services will be stopped before Database Backup. Do you want to continue [y/n]?
```

Step 3 Enter y and press **Enter**.

The following information is displayed:

```
Stopping services...

Stopping services... done
Taking local Database backup...
The backup process creates a <filename>.tar.gz file on the system running Cisco UCS Director.
This file will be copied to another server using the ftp, sftp, or scp protocol.
Specify the transfer mode and login credentials.

   Specify the Transfer mode [ftp sftp scp]:
```

Step 4 Enter your mode of transfer and login credentials, and press **Enter**.

The following information is displayed:

```
Server IP Address:
```

Step 5 Enter Server IP address and press **Enter**.

The following information is displayed:

```
Server IP Address: xxx.xxx.xxx.xxx
Server Login:
```

Step 6 Enter your Server login name and press **Enter**.

Step 7 Enter your Server password and press **Enter**.

Note
For SFTP server, you can also store the backup files in the sub-directory. By default, the files are stored in the Home directory.

Note
For SCP, you need to provide the complete path to store the backup files.

Messages appear to confirm the progress of your backup.

Restoring the Database

Before restoring the database, stop the Cisco services. To stop the services, choose the **Stop Services** option. Provide the following information in order to execute the task:

- FTP, SFTP, or SCP server's IP address (from where the database is restored)
- Server's login credentials
- Restore filename
- Confirm to restore

Note After server credentials are provided, the entire database of the Cisco UCS Director appliance is restored from the specified server location. You can then start the Cisco services by choosing the **Start Services** option.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Restore Services** option and press **Enter**.

The following information is displayed:

```
Services will be stopped before Database Backup. Do you want to continue [y/n]?
```

Step 2 Enter y and press **Enter**.

The following information is displayed:

```
Stopping services... done
The restore process restores the database from a backed up <filename>.tar.gz file
on the system running Cisco UCS Director.
You can copy this file from another server using the ftp, sftp, or scp mode.

   Specify the Transfer mode [ftp sftp scp]:
```

Step 3 Enter your mode of transfer and login credentials, and press **Enter**.

The following information displays:

```
 Provide the necessary access credentials
Server IP Address:
```

Step 4 Enter your server IP address and press **Enter**.

The following information displays:

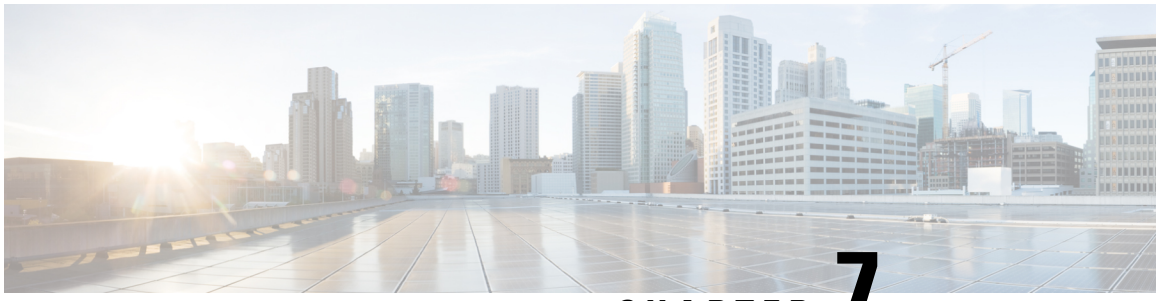
```
Server Login:
```

Step 5 Enter your server login and press **Enter**.

Step 6 Enter your server password and press the **Enter**.

Step 7 Follow the onscreen prompts to complete the process.

Step 8 Choose the **Start Services** option to restart the Cisco services.



CHAPTER 7

Managing Bare Metal Agent Details

This chapter contains the following sections:

Adding the Cisco UCS Director Bare Metal Agent Hostname and IP Address

Choose this option to add the Cisco UCS Director Bare Metal Agent appliance hostname and IP address entries into the Cisco UCS Director appliance's `/etc/hosts` file.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **`Add Cisco UCS Director Baremetal Agent`** option and press **`Enter`**.

The following information appears:

```
Adding Cisco UCS Director Baremetal Agent Hostname and IP Address entry to /etc/hosts
Enter Cisco UCS Director Baremetal Agent IP Address:xxx.x.x.x
Enter Cisco UCS Director Baremetal Agent Hostname:xxx.xx.x.x
Adding host entry xxx.x.xx.x to /etc/hosts
Entry xxx.x.xx.x does not exist
Backed up old file...
Added new entry xxx.x.xx.x
Added xxx.xx.x.x To /etc/hosts
Press return to continue ...
```

Step 2 Press **`Enter`** to complete the process.

Enabling the Database for Cisco UCS Director Bare Metal Agent

You can enable remote database access for the Cisco UCS Director Bare Metal Agent appliance by choosing the **Enabling the Database for BMA** option.

Note This option is required for configuration of the Cisco UCS Director appliance with the BMA appliance.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Enabling the Database for Cisco UCS Directory Baremetal Agent** option and press **Enter**.

The following information is displayed:

```
Do you want to enable 'remote database' access for Cisco UCS Director Baremetal Agent [y/n]? y
   Cisco UCS Director Baremetal Agent Hostname/IP Address: xxx.xxx.x.xxx
```

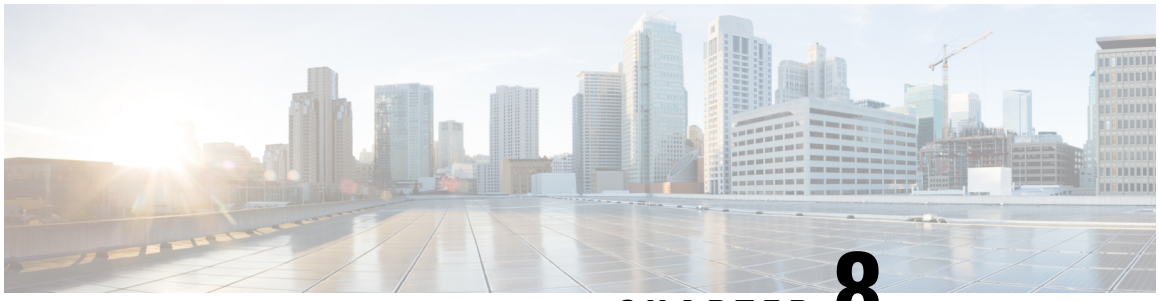
Step 2 Choose **y** and press **Enter**.

The following information is displayed:

```
Cisco UCS Director Baremetal Agent Hostname/IP Address: xxx.xxx.xx.xx
Enabling 'remote database' access for xxx.xxx.xx.xx
Enabling remote database access to xxx.xxx.xx.xx
Loading class `com.mariadb.jdbc.Driver'. This is deprecated. The new driver class is
`com.mariadb.cj.jdbc.Driver'. The driver is automatically registered via the SPI and manual loading
 of the driver class is generally unnecessary.
About to enable remote access to database - please be catious that this is only supported for Cisco
 UCS Director Baremetal Agent
About to enable remote access to database (xxx.xxx.xx.xx) please be catious that this is only supported
 for Cisco UCS Director
Baremetal Agent
 INFO (DBEnableRemoteAccess.java:195) About to enable remote access to database (xxx.xxx.xx.xx) please
 be catious that this is
only supported for Cisco UCS Director Baremetal Agent
Remote DB access enabled
 INFO (DBEnableRemoteAccess.java:213) About to enable remote access to datbase - please be catious
that this is only supported
for Cisco UCS Director Baremetal Agent
flushPrivileges - About to enable remote access to database - please be catious that this is only
supported for Cisco UCS
Director Baremetal Agent
 INFO (DBEnableRemoteAccess.java:119) flushPrivileges - About to enable remote access to database -
 please be catious that
this is only supported for Cisco UCS Director Baremetal Agent
Enabled 'Remote' database access
 INFO (DBEnableRemoteAccess.java:219) Enabled 'Remote' database access
Successfully added credential for ipAddress xxx.xxx.xx.xx
flushPrivileges - About to enable remote access to database - please be catious that this is only
supported for Cisco UCS
Director Baremetal Agent
 INFO (DBEnableRemoteAccess.java:119) flushPrivileges - About to enable remote access to database -
 please be catious that
this is only supported for Cisco UCS Director Baremetal Agent
Enabled 'Remote' database access for: xxx.xxx.xx.xx
```

```
 INFO (DBEnableRemoteAccess.java:679) Enabled 'Remote' database access for: xxx.xxx.xx.xx
Completed remote database access...
Press return to continue ...
```

Step 3 Press **Enter** to return to the main menu.



CHAPTER 8

Managing Certificates

This chapter contains the following sections:

Managing SSL Certificates

This section describes how to generate a Self-Signed certificate and Certificate Signing Request (CSR) that can be used to obtain SSL certificates from a Certificate Authority such as VeriSign, Digicert, and so on It also provides instructions to import the generated Self-Signed certificate or CA certificate in Cisco UCS Director.

Generating Self-Signed Certificates and Certificate Signing Requests

When you generate a self-signed certificate, a new self-signed certificate in PEM format and a Certificate Signing Request (CSR) file are created in the `/opt/certs/` directory. When generating a self-signed certificate, clicking enter will select the default option. For example, if you do not specify a domain name, the shell admin by default chooses the domain name of the appliance that is configured.

You can generate a self-signed certificate and a CSR using the **`Generate Self-Signed Certificate and Certificate Signing Request`** option.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **`Generate Self-Signed Certificate and Certificate Signing Request`** and press **`Enter`**.

The following information is displayed:

```
Do you want to use the domain localdom [y/n]?
```

Step 2 Enter **`y`** and press **`Enter`**.

By default the shell menu selects the domain name of the local appliance that is configured.

The following information is displayed:

```
Enter number of days the generated certificate will be valid for.
It should be between 1825 days (5 years) and 5475 days (15 years).
Enter number of days the certificate will be valid:
```

Step 3 Enter the number of days that you want the self-signed certificate to be valid for and press **Enter**. It is recommened to enter the number of days between 1825 days (5 years) and 5475 days (15 years).

The following information is displayed:

```
Generating a 2048 bit RSA private key
writing new private key to '/opt/certs/localdom.key'
------
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
------
Country Name (2 letter code) [xx]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
```

Step 4 Enter the country name, state or province name, locality name, organization name, organizational unit name, common name, and email address, and press **Enter**.

The following information is displayed:

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Step 5 (Optional) Enter a challenge password and an optional company name, and press **Enter**.

The following information is displayed:

```
Writing new CSR (Certificate Signing Request) to /opt/certs/localdom.csr.
Use the CSR to obtain a certificate in PEM format from a CA (Certificate Authority).
Signature ok
subject=/C=AU/ST=Some-State/O=Internet Pty Ltd
Getting Private key
Writing new self-signed certificate in PEM format to /opt/certs/localdom.pem.
Press return to continue ...
```

Importing Certification Authority or Self-Signed Certificates

You can either import the generated self-signed certificate or import a certificate generated by another system or third party by copying .pem and .key (private key) files to the `/opt/certs/` directory. The shell admin will automatically discover the .pem and .key files for the given domain in the `/opt/certs/` directory. The .pem file provided is exported into PKCS12 format, and then converted to JKS format. The JKS file can be imported into Tomcat.

You can import a CA signed certificate, self-signed certificate, or a certificate bundle (with multiple certificates, if it involves multiple signing authority) using the **Import CA/Self-Signed Certificate** option.

Note Before importing a root chain CA certificate using the Shell menu, you must combine the primary, intermediate, and root certificates into a single .pem file.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Import CA/Self-Signed Certificate** option and press **Enter**.

The following information is displayed:

```
Do you want to use the domain localdom [y/n]?
```

Step 2 Enter **y** and press **Enter**.

By default the shell menu selects the domain name of the local appliance that is configured.

The following information is displayed:

```
Enter the path for the CA/self-signed certificate (PEM) for localdom (e.g.,
/root/Downloads/localdom.pem):
```

Step 3 Enter the path to the CA signed certificate, self-signed certificate, or a certificate bundle (with multiple certificates, if it involves multiple signing authority), and press **Enter**.

The following information is displayed:

```
Enter private key [/opt/certs/localdom.key]:
```

Step 4 Enter the path to the private key and press **Enter**.

The following information is displayed:

```
Enter keystore password:
```

Step 5 Enter the Java KeyStore (JKS) password and press **Enter**.

Information similar to the following is displayed

```
Verifying /opt/certs/localdom.pem ...

The certificate /opt/certs/localdom.pem is valid.
```

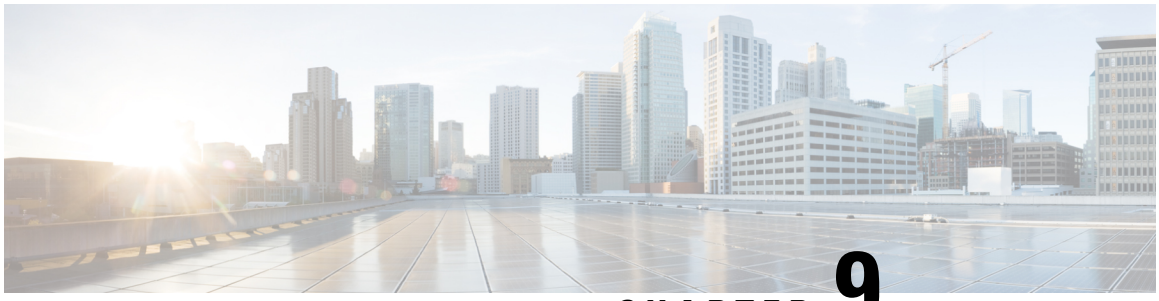
```
Exporting /opt/certs/localdom.pem to PKCS12 format....

Converting PKCS12 to JKS format...

Importing /opt/certs/keystore.jks into tomcat for secured access to UCSD UI using HTTPS.

Certificate /opt/certs/keystore.jks imported to tomcat succesfully.

Press return to continue ...
```



CHAPTER 9

Managing Root Access

This chapter contains the following sections:

Accessing root Privileges

This section describes how to access root. Tasks that require root privileges include moving directories or files into other directories, providing or revoking user privileges, general system repairs, and occasionally installing applications.

Important From the Cisco UCS Director release 6.9(2.0), root user access is disabled by default to prevent the use of root privileges for regular management operations. Instead, 'ucsdadmin' user account is enabled by default to enhance security. Therefore, it is recommended to access the Cisco UCS Director using the 'ucsdadmin' account. For more information on ucsdadmin options, see Managing ucsdadmin Access.

To provide administrative privileges, the following Shell admin options are introduced:

- **Manage ucsdadmin Access**
- **Login as ucsdadmin**

Configuring root Access

You can enable root privileges by choosing **`Manage root Access`**.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **`Manage root Access`** and press **`Enter`**.

The following information is displayed:

```
Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **c** and press **Enter**.

The following information is displayed:

```
Warning: If the root user account is disabled, it will be enabled during the password reset process.
Do you want to Configure/Set root Privilege/Password [y/n]?
```

Step 3 Enter **y** and press **Enter**.

The following information is displayed:

```
Changing password for user root.
New password:
```

Step 4 Enter a new password and press **Enter**.

The following information is displayed:

```
Retype new password:
```

Note
If the password is invalid, a warning message is displayed along with the password policy.

Step 5 Enter the password again for confirmation and press **Enter**.

The following information is displayed:

```
passswd: all authentication tokens updated successfully.
         root passwd changed successfully and the root account has been enabled.
         Press return to continue...
```

Step 6 Press **Enter** to complete the process.

Enabling root Access

You can enable root privileges by choosing **Manage root Access**.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Manage root Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **e** and press **Enter**.

The following information is displayed:

```
WARNING: Enabling the root user increases the potential risk of system compromise.
Proceed with caution, and consider disabling the root user when it is no longer necessary.
```

Step 3 Enter **y** and press **Enter**.

The following information is displayed:

```
Enabling root access...
Unlocking password for user root.
passwd: Success
root access enabled successfully
Press return to continue...
```

Step 4 Press **Enter** to return to complete the process.

Disabling Root Access

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Manage Root Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **d** and press **Enter**.

The following information is displayed:

```
Warning: All active terminal sessions of the root user will be terminated.
Do you want to Disable Root Access [y/n]?
```

Step 3 Enter **y** and press **Enter**.

The following information is displayed:

```
Disabling root access...
         Locking password for user root.
         passwd: Success
         Root access disabled successfully
         All active root sessions have been terminated.
         Press return to continue...
```

Step 4 Press **Enter** to return to the main menu.

Logging in as root

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Login As root** option and press **Enter**.

The following information is displayed:

```
Do you want to  Login As root [y/n]? :
```

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Logging in as root
         password:
```

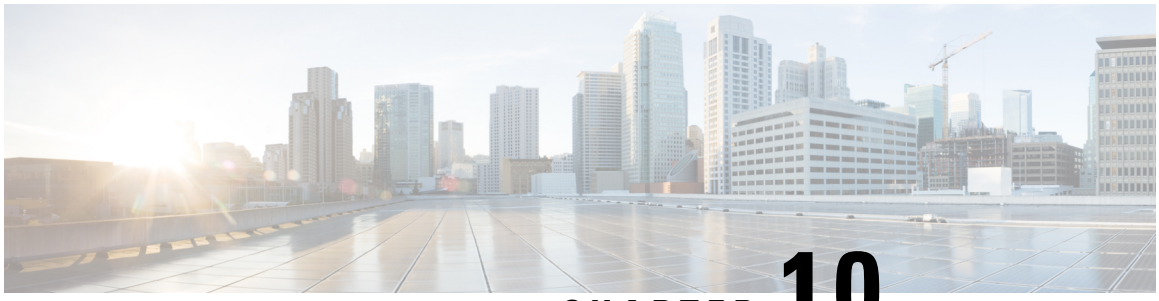
Step 3 Enter your root password and press **Enter**.
The following information is displayed:

```
[root@localhost shelladmin]#
```

Step 4 Perform the required actions.

Step 5 (Optional) Enter **exit** if you want to exit from the Shell session.
The following information is displayed:

```
exit
Press return to continue ...
```



CHAPTER 10

Managing ucsdadmin Access

This chapter contains the following sections:

Logging in as ucsdadmin User

Note As the 'root' user access is disabled and 'ucsdadmin' user access is enabled by default, you must log in as ucsdadmin user with **ucsdadmin** as the password.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Login as ucsdadmin** and press **Enter**.

The following information is displayed:

```
Do you want to Login As ucsdadmin [y/n]?
```

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Logging in as ucsdadmin
Password:
```

Step 3 Enter the password, and press **Enter**.

Note
When you first log into Cisco UCS Director using the default password **ucsdadmin**, you will be prompted to change the password in accordance with the password policy.

The Cisco UCS Director Shell options are displayed.

Enabling ucsdadmin Access

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Manage ucsdadmin Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (ucsdadmin privilege) [e/d/c]:
```

Step 2 Enter **e**, and press **Enter**.

The following information is displayed:

```
Do you want to Enable ucsdadmin Access [y/n]?
```

Step 3 Enter **y**, and press **Enter**.

The following information is displayed:

```
Enabling ucsdadmin access...
Unlocking password for user ucsdadmin.
passwd: Success
ucsdadmin access enabled successfully
Press return to continue ...
```

Step 4 Press **Enter** to complete the process.

Disabling ucsdadmin Access

Note As the 'root' user access is disabled and 'ucsdadmin' user access is enabled by default to enhance security, it is not recommended to disable the **ucsdadmin** access.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Manage ucsdadmin Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (ucsdadmin privilege) [e/d/c]:
```

Step 2 Enter **d**, and press **Enter**.

The following information is displayed:

```
Warning: All active terminal sessions of the ucsdadmin user will be terminated.
Do you want to Disable ucsdadmin Access [y/n]?
```

Step 3 Enter **y**, and press **Enter**.

The following information is displayed:

```
Disabling ucsdadmin access...
Locking password for user ucsdadmin.
passwd: Success
ucsdadmin access disabled successfully
All active ucsdadmin sessions have been terminated.
Press return to continue ...
```

Step 4 Press **Enter** to complete the process.

Configuring ucsdadmin Access

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Manage ucsdadmin Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (ucsdadmin privilege) [e/d/c]:
```

Step 2 Enter **c**, and press **Enter**.

The following information is displayed:

```
Warning: If the ucsdadmin user account is disabled, it will be enabled during the password reset
process.
Do you want to Configure/Set ucsdadmin Privilege/Password [y/n]?
```

Step 3 Enter **y**, and press **Enter**.

The following information is displayed:

```
Changing password for user ucsdadmin.
New password:
```

Step 4 Enter the password, and press **Enter**.

The following information is displayed:

```
Retype new password:
```

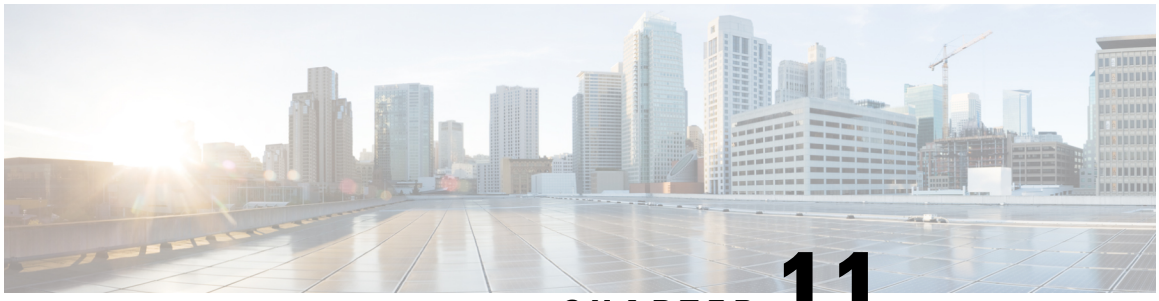
Note
If the password is invalid, a warning message is displayed along with the password policy.

Step 5 Enter the password again for confirmation and press **Enter**.

The following information is displayed:

```
passwd: all authentication tokens updated successfully.
ucsdadmin password changed successfully and ucsdadmin account has been enabled.
Press return to continue ...
```

Step 6 Press **Enter** to complete the process.



CHAPTER 11

Troubleshooting

This chapter contains the following sections:

Backing up the Monitoring Database in a Multi-Node Setup

Problem—You are unable to back up the monitoring database in a multi-node setup.

Recommended Solution—Edit the `dbMonitoringBackupRestore.sh` script.

Procedure

Step 1 Edit the `/opt/infra/dbMonitoringBackupRestore.sh` script using vi.

Step 2 Remove the `CHARGEBACK_HISTORY_ENTRY` table name from the script.

Pinging the Hostname and IP Address

You can ping a hostname or IP address to test your connectivity by choosing the **Ping Hostname/IP address** option.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Ping Hostname/IP address** option and press **Enter**.

Step 2 Enter your IP address and press **Enter**.

The following information is displayed:

```
 Enter IP Address : xxx.xxx.xxx.xxx
PING xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx) 56(84) bytes of data.
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=64 time=9.90 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=64 time=0.254 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=4 ttl=64 time=0.198 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=5 ttl=64 time=0.267 ms

--- xxx.xxx.xxx.xxx ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.198/2.187/9.901/3.857 ms
Press return to continue ...
```

Step 3 Press **Enter** to exit out of the operation.

Viewing Tail Inframgr Logs

This Shell lets enables you to see inframgr (Infrastructure Manager) log data, which are generated behind the scenes by use of the Unix tail command. When you are debugging, you can trace problems by using this log data. You use the **Tail Inframgr Logs** option to immediately tail the most recent inframgr logs. The results are displayed on your screen directly after you select this option.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Tail Inframgr Logs** option and press **Enter**.

Following are a few sample lines, typical of the results displayed immediately after use of the **Tail Inframgr Logs** option:

```
2014-07-20 23:17:43,500 [pool-23-thread-17]
INFO  getBestAgent(SystemTaskExecutor.java:308)
- No Agent available for remoting SnapMirrorHistoryStatusSchedulerTask
2014-07-20 23:17:43,502 [pool-23-thread-17]
INFO  updateStatus(SystemTaskStatusProvider.java:181)
- Task: task.SnapMirrorHistoryStatusSchedulerTask changed state to OK
2014-07-20 23:17:43,562 [pool-23-thread-17]
INFO  executeLocally(SystemTaskExecutor.java:133)
- Executing task locally: SnapMirrorHistoryStatusSchedulerTask
2014-07-20 23:17:43,562 [pool-23-thread-17]
INFO  getClusterLeaf(ClusterPersistenceUtil.java:81)
- Leaf name LocalHost
2014-07-20 23:17:43,571 [pool-23-thread-17]
```

Step 2 To exit from the log file display, type **Ctrl+C**, then press **Enter**.

Cleaning Up Patch Files

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Clean-up Patch Files** option and press the **Enter** key.

The following information is displayed:

```
Do you want to delete an old patch file/directory [y/n]?
```

Step 2 Enter **y** and press **Enter** to delete the patch files.

The following information is displayed:

```
1) cucsd_patch_6_6_0_0_66450
2) cucsd_patch_6_6_0_0_66460
3) cucsd_patch_6_6_0_0_66470
4) cucsd_patch_6_6_0_0_66480
5) infra-12-07-2017-21-17-30
6) infra-12-07-2017-21-17-40
7) Exit
Select an option to delete a patch file/directory:
```

Step 3 Choose the required option to delete the patch file or directory and press **Enter**.

The following information is displayed:

```
Select an option to delete a patch file/directory: 4
Are you sure you want to delete: cucsd_patch_6_6_0_0_66480 [y/n]?
```

Step 4 If you are prompted to confirm that you want to delete the patch file or directory, enter **y** and then press **Enter**.

The following information is displayed:

```
Directory Deleted
Press return to continue...
```

Step 5 Press the **Enter** key to return to the main menu.

Collecting Logs from a Node

The Collect Logs from a Node option lets you collect logs from the local node or from a remote node.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Collect Logs from a Node Status** and press **Enter**.

The following list of services appears:

```
 ********************************************************************
            This wizard helps to do Logs from UCSD Appliance
********************************************************************
 Logs Collection  Option #

 Exit         --> Select '0'
 Current Node --> Select '1'
 Remote Node  --> Select '2'

Enter an option [0 1 2]:
```

Step 2 Enter the logs collection option and press **Enter**.

- If you choose to collect logs from the current node, a response similar to the following appears:

```
Collecting all feature logs....
============================================================
                    Collection of Logs
============================================================
Moving logs from /opt/infra/broker to common/logs
Moving logs from /opt/infra/client to common/logs
Moving logs from /opt/infra/controller to common/logs
Moving logs from /opt/infra/eventmgr to common/logs
Moving logs from /opt/infra/idaccessmgr to common/logs
Moving logs from /opt/infra/inframgr to common/logs
Moving logs from /opt/infra/web_cloudmgr to common/logs

Logs archive path:  /opt/infra/common/logs-07-31-2014-08-36-48.tar
You can also view individual feature logs under /opt/infra/common/logs

Logs collection done for current node
Do you want to collect logs from another node?  [y/n]: Collect Logs from a Node
```

Note
To collect logs from another node, the best practice is to return to the Shell menu, select the Collect Logs from a Node option again, and choose the **Remote Node** option.

- If you choose to collect logs from a remote node, a response similar to the following appears:

```
Please enter the remote server IP/Hostname from where we collect logs:
```

Follow the onscreen instructions to provide the address of the remote log, establish a secure connection, and provide the required login credentials for that remote node.

Collecting Diagnostics

The Collect Diagnostics option helps to collect logs from a Multi-Node setup and a Standalone setup for debugging purposes.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Collect Diagnostics**.

The following information is displayed:

```
Diagnostics Menu
==================
Options:
  0) Exit
  1) Collect essential diagnostics
  2) Collect basic diagnostics
  3) Collect full diagnostics
  4) Collect inframgr thread dump
  5) Collect inframgr heap dump
  6) Display Disk Speed

Enter option number [0 1 2 3 4 5 6]:
```

Note
In a multi-node setup, only Collect essential diagnostics option is supported in inventory and monitoring nodes.

Step 2 If you choose Collect essential diagnostics option, a response similar to the following appears:

```
Type in option number and press <Enter> : 1
Collecting essential diagnostics...
Collecting system info...
Collecting 'inframgr' service diags (config files, logs files, etc) ...
Collecting 'tomcat' diags (config files, logs files, etc) ...
Creating diagnostics archive /opt/infra/diags/standalone_diags_essential_02-07-2018-08-20-36.tgz....
 done
Press return to continue ...
```

Step 3 If you choose Collect basic diagnostics option, a response similar to the following appears:

```
Type in option number and press <Enter> : 2
Collecting basic diagnostics...
Collecting system info...
Collecting 'broker' service diags (config files, logs files, etc) ...
Collecting 'controller' service diags (config files, logs files, etc) ...
Collecting 'eventmgr' service diags (config files, logs files, etc) ...
Collecting 'idaccessmgr' service diags (config files, logs files, etc) ...
Collecting 'inframgr' service diags (config files, logs files, etc) ...
Collecting 'tomcat' diags (config files, logs files, etc) ...
Collecting system/OS diags...
Collecting SAR data as text...
Collecting output of essential commands...
Creating diagnostics archive /opt/infra/diags/standalone_diags_base_02-07-2018-08-22-28.tgz....
done
Press return to continue ...
```

Step 4 If you choose Collect full diagnostics option, a response similar to the following appears:

```
Type in option number and press <Enter> : 3
Pre-requisites:
1. Download JDK installer jdk-8u131-linux-x64.tar.gz from oracle.com JDK archive
2. Copy the jdk-8u131-linux-x64.tar.gz under /opt/bin.
3. Install the JDK by running the following commands.
        cd /opt/bin
        tar -xzvf jdk-8u131-linux-x64.tar.gz

Enter JDK path if it's already installed (e.g. /opt/bin/jdk1.8.0_131): /root/java/jdk1.8.0_131
```

Note
If you receive a 'Permission denied' error while copying the `tar.gz` file, execute the following command:

```
sudo chmod 775 /opt/bin
```

Step 5 Enter the JDK path and press **Enter**. The following information is displayed.:

```
Collecting full diagnostics. This operation may take several minutes to complete

 .
Collecting system info...
Collecting 'broker' service diags (config files, logs files, etc) ...
Collecting 'controller' service diags (config files, logs files, etc) ...
Collecting 'eventmgr' service diags (config files, logs files, etc) ...
Collecting 'idaccessmgr' service diags (config files, logs files, etc) ...
Collecting 'inframgr' service diags (config files, logs files, etc) ...
Collecting 'tomcat' diags (config files, logs files, etc) ...
Collecting system/OS diags...
Collecting SAR data as text...
Collecting output of essential commands...
Collecting inframgr (PID=11890) thread dump...
Collecting inframgr (PID=11890) memory dump. This operation may take several minutes to complete.
Dumping heap to /opt/infra/diags/02-07-2018-08-24-40/inframgr.hprof ...
Heap dump file created

Creating diagnostics archive
/opt/infra/diags/standalone_diags_full_02-07-2018-08-24-40.tgz.............................. done
Press return to continue ...
```

Step 6 If you choose Collect inframgr thread dump option, a response similar to the following appears:

```
Type in option number and press <Enter> : 4
Pre-requisites:
1. Download JDK installer jdk-8u131-linux-x64.tar.gz from oracle.com JDK archive.
2. Copy the jdk-8u131-linux-x64.tar.gz under /opt/bin.
3. Install the JDK by running the following commands.
        cd /opt/bin
        tar -xzvf jdk-8u131-linux-x64.tar.gz

Enter JDK path if it's already installed (e.g. /opt/bin/jdk1.8.0_131): /root/java/jdk1.8.0_131
```

Step 7 Enter the JDK path and press **Enter**. The following information is displayed.:

```
Collecting inframgr-tdump diagnostics. This operation may take several minutes to complete.....
done
Creating diagnostics archive
```

```
/opt/infra/diags/standalone_diags_inframgr-tdump_02-07-2018-08-30-43.tgz.... done
Press return to continue ...
```

Step 8 If you choose Collect inframgr heap dump option, a response similar to the following appears:

```
Type in option number and press <Enter> : 5
Pre-requisites:
1. Download JDK installer jdk-8u131-linux-x64.tar.gz from oracle.com JDK archive.
2. Copy the jdk-8u131-linux-x64.tar.gz under /opt/bin.
3. Install the JDK by running the following commands.
        cd /opt/bin
        tar -xzvf jdk-8u131-linux-x64.tar.gz

Enter JDK path if it's already installed (e.g. /opt/bin/jdk1.8.0_131): /root/java/jdk1.8.0_131
```

Step 9 Enter the JDK path and press **Enter**. The following information is displayed.:

```
Collecting inframgr-hdump diagnostics. This operation may take several minutes to complete.......
done
Creating diagnostics archive
/opt/infra/diags/standalone_diags_inframgr-hdump_02-07-2018-08-28-29.tgz.............................
 done
Press return to continue ...
```

Step 10 If you choose Display Disk Speed option, a response similar to the following appears:

```
Type in option number and press <Enter> : 6
Results of the disk speed check are more accurate if UCS Director services and database services
are not running. If these services are running when you initiate the disk speed check, it could
affect the disk I/O bandwidth for these services and impact system performance. We recommend you
stop these services using the shelladmin option while running this utility.
Do you want to continue [y/n]? :
```

Note
Display Disk Speed option allows you to check the read/write speed of a database disk in the Cisco UCS Director appliance. In a dual-node setup, Display Disk Speed option is not applicable for a primary node, as the primary node does not run the database services.

Step 11 Enter **y** and press **Enter**. The following information is displayed.:

```
Checking Disk
Read Bandwidth  : 240.864MB/s
Write Bandwidth : 241.246MB/s
Press return to continue ...
```

Using Diagnostics Information

User or TAC engineer can collect the basic diagnostics data using **Collect basic diagnostics** option in the shelladmin while reporting any issue. The diagnostics bundle contains the following diagnostics data that is used for troubleshooting the reported issues.

- Summary file—Contains important and high level summary.

- Diag file—Contains information such as version history with timestamp, average CPU utilization, infra services status, database status, and database size.
- SummaryReport file—Contains summary report.
- DiagOutput file—Contains detailed report.
- UcsdExceptions file—Contains all exceptions found in the inframgr/logfile.txt.* and number of occurrences of each exception.
- infra-env Directory—Contains the infra services configuration (<service>.env) files.
- commands Directory—Contains the output of various system commands.
- var-log-ucsd zip file—Contains the log files such as install.log, bootup.log, and services.log.

Troubleshooting VMware Console Display Issues

Problem—The VMware console does not display after an abrupt shutdown of the Cisco UCS Director VM from VMware vCenter.

Possible Cause—Occasionally after Cisco UCS Director VM is powered on, the VMware console prompt gets stuck after the process restart and does not return to the shelladmin.

Recommended Solution—After the VM is powered on, press **Alt-F1** to refresh the VMware console.

Procedure

In the Cisco UCS Director VM prompt after the VM is powered on, press **Alt-F1**.

The VMware console screen is refreshed.

Enabling HTTP Access

By default, HTTPS access mode is enabled during initial OVF installation and Cisco UCS Director upgrade. When HTTP is enabled, you can log in to Cisco UCS Director, using both HTTP and HTTPS modes. When HTTPS is enabled, you can log in to the Cisco UCS Director only using HTTPS mode. Even when you try to log in to Cisco UCS Director using HTTP mode, you will be redirected to HTTPS user interface only.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Enable/Disable HTTP** option and press **Enter**.

The following information is displayed:

```
HTTPS is currently enabled. Do you want to enable HTTP [y/n]? :
```

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Cisco UCS Director Services will be restarted to enable the HTTP configuration. Do you want to continue
 [y/n]?
```

Step 3 Enter **y** and press **Enter**. The Cisco services are restarted.

Resetting MariaDB User Password in a Multi-Node Setup

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Reset MariaDB User password** option and press **Enter**.

The following information is displayed:

```
This utility will restart the services after changing MariaDB user password, do you want to continue?
 [y/n]:
```

Note
In a multi-node setup, ensure that the infra services are stopped in the primary and service nodes before executing the Reset MariaDB User password option in DB nodes.

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Stopping the infra services...
The infra services are stopped.
Do you want to change the password for MariaDB 'admin' user? [y/n]:
```

Step 3 Enter **y** and press **Enter**.

The following information is displayed:

```
Current Password (Type in current password or press enter key to use password from the existing
credentials file):
```

This option is applicable only for the primary and service nodes in a multi-node setup.

Step 4 Enter **y** and press **Enter**.

The following information is displayed:

```
Do you want to generate random password for MariaDB 'admin' user? [y/n]:
```

Step 5 Enter **n** and press **Enter**.

The following information is displayed:

```
Specify the new password for MariaDB 'admin' user:
```

Step 6 Enter a new MariaDB admin password and press **Enter**.

Note
Special characters such as *, \, ', and $ are not allowed for MariaDB admin user passwords.

Step 7 Enter your new MariaDB admin password and press **Enter**.

The following information is displayed:

```
MariaDB user password is updated.
Checking if the database is running...yes.
Stopping the database...
The database is stopped.
Starting the database...
The database is started.
Copying credential files to BMA appliance...
Trying to get session to xxx.xxx.xxx.xxx ....
Trying to connect...
Successfully connected
Uloaded file:/opt/certs/MariaDB/dbkeys.key
Trying to get session to xxx.xxx.xxx.xxx...
Trying to connect...
Successfully connected
Uploaded file:/opt/certs/MariaDB/dbcreds.properties
Starting the infra services...
Press return to continue...
```

Note
If a BMA appliance is associated with a Cisco UCS Director, the dbkeys and dbcreds files are copied to a specific location in the BMA appliance to establish successful connectivity to the Cisco UCS Director. After resetting the MariaDB user password, you should restart the BMA services either from the Cisco UCS Director user interface or from the BMA appliance.

Note
In a multi-node set up, if you want to reset the MariaDB user password, you should execute the Reset MariaDB User password option in all the nodes in the following sequence inventory, monitoring, primary, and service nodes.

Resetting MariaDB User Password in a Standalone Setup

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose the **Reset MariaDB User password** option and press **Enter**.

The following information is displayed:

```
This utility will restart the services after changing MariaDB user password, do you want to continue?
 [y/n]:
```

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Stopping the infra services...
```

```
The infra services are stopped.
Do you want to change the password for MariaDB 'admin' user? [y/n]:
```

Step 3 Enter **y** and press **Enter**.

The following information is displayed:

```
Do you want to generate random password for MariaDB 'admin' user? [y/n]:
```

Step 4 Enter **y** and press **Enter**.

The following information is displayed:

```
Generating Random Password....... done
Do you want to change the password for MariaDB 'root' user? [y/n]:
```

Step 5 If you entered **n**, enter the new password for MariaDB admin user and press **Enter**.

Note
Special characters such as *, \, ', and $ are not allowed for MariaDB admin user passwords.

The following information is displayed:

```
Specify the new password for MariaDB 'admin' user:
Confirm the new password for MariaDB 'admin' user:
Password update takes few minutes. Please wait..... done
```

Step 6 Enter **y** and press **Enter**.

The following information is displayed:

```
Do you want to generate random password for MariaDB 'root' user? [y/n]:
```

Step 7 Enter **y** and press **Enter**.

The following information is displayed:

```
Generating Random Password....... done
MariaDB user password is updated.
Checking if the database is running... yes.
Stopping the database...
.............
The database is stopped.
Starting the database...
Checking if MariaDB database is running... .UP
The database is started.

Starting the infra services...
```

Step 8 If you entered **n**, enter the new password for MariaDB root user and press **Enter**.

Note
Special characters such as *, \, ', and $ are not allowed for root user passwords.

The following information is displayed:

```
Specify the new password for MariaDB 'root' user:
Confirm the new password for MariaDB 'root' user:
Password update takes few minutes. Please wait..................... done
```

```
MariaDB user password is updated.
Checking if the database is running... yes.
Stopping the database...
..
The database is stopped.
Starting the database...
Checking if MariaDB database is running... UP
The database is started.

Starting the infra services...
```

Note
After resetting the MariaDB user password, you should restart the BMA services either from the Cisco UCS Director user interface or from the BMA appliance.

Generating Device ID

You can generate a device ID for a cloned Cisco UCS Director appliance by choosing **Configure Network Interface** option.

Procedure

Step 1 From the Cisco UCS Director Shell menu, choose **Configure Network Interface** and press Enter.

The following information is displayed:

```
Cisco UCS Director's VM UUID change detected. It is recommended to generate a new GUID for this UCS
 Director instance. Proceed [y/n]?
```

Note
This option is displayed only when a Cisco UCS Director is cloned. You must generate a new GUID. The GUID is used to claim a device in Cisco Intersight. For more information about how to claim a device, see the Cisco UCS Director Administration Guide.

Step 2 Enter **y** to assign a new, unique, and unclaimed device ID to the cloned Cisco UCS Director, and press **Enter**. The following information is displayed.

```
Generation of Cisco UCS Director GUID is successful.

After configuring the network interface, you must restart the  Cisco UCS Director services for the
updated network configuration to be used.

Do you want to Configure DHCP/STATIC IP  [D/S] ? :
```

Note
Enter **n** only if you want Cisco Intersight to call the cloned Cisco UCS Director rather than the original Cisco UCS Director.

Note
To configure a network interface for the Cisco UCS Director appliance, see Configuring a Network Interface.