



Cisco UCS Director Shell Guide, Release 6.7

First Published: 2019-01-09

Last Modified: 2020-11-13

Americas Headquarters

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

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface vii

Audience vii

Conventions vii

Related Documentation ix

Documentation Feedback ix

Communications, Services, and Additional Information ix

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information 1

CHAPTER 2

Overview 3

Cisco UCS Director 3

Cisco UCS Director Shell 4

About Cisco UCS Director Shell Commands 4

Prerequisites 6

Logging in to the Shell 6

CHAPTER 3

Using Shell Commands 9

General Administration 9

Examining the Version Information 9

Changing Your Password 10

Synchronizing the System Time 10

Applying a Patch to Cisco UCS Director 11

Applying a Signed Patch to Cisco UCS Director 13

Shutting Down the Appliance 14

Rebooting an Appliance 14

Using a Multi-Node Setup 15

Terminating Active GUI Sessions 15

Granting Client Access to MySQL Port 16

Denying Client Access to MySQL Port 17

Regenerating Device Connector REST API Access Key 17

Managing VMRC Tunneling Service 18

CHAPTER 4 **Configuring Network Details 19**

 Configuring a Network Interface 19

 Displaying Appliance Network Details 20

CHAPTER 5 **Managing Cisco Services 21**

 Displaying the Status of Your Services 21

 Stopping Cisco Services 23

 Starting Cisco Services 23

CHAPTER 6 **Managing Databases 25**

 Working with Databases 25

 Stopping the Database 25

 Starting the Database 26

 Backing Up the Database 26

 Restoring the Database 28

CHAPTER 7 **Managing Bare Metal Agent Details 31**

 Adding the Cisco UCS Director Bare Metal Agent Hostname and IP Address 31

 Enabling the Database for Cisco UCS Director Bare Metal Agent 31

CHAPTER 8 **Managing Certificates 33**

 Managing SSL Certificates 33

 Generating Self-Signed Certificates and Certificate Signing Requests 33

 Importing Certification Authority or Self-Signed Certificates 34

CHAPTER 9 **Managing Root Access 37**

Accessing Root Privileges	37
Configuring Root Access	37
Enabling Root Access	38
Disabling Root Access	38
Logging in as Root	39

CHAPTER 10**Troubleshooting 41**

Backing up the Monitoring Database in a Multi-Node Setup	41
Pinging the Hostname and IP Address	41
Viewing Tail Inframgr Logs	42
Cleaning Up Patch Files	43
Collecting Logs from a Node	43
Collecting Diagnostics	45
Using Diagnostics Information	47
Troubleshooting VMware Console Display Issues	48
Enabling HTTP Access	48
Resetting MYSQL User Password in a Multi-Node Setup	49
Resetting MYSQL User Password in a Standalone Setup	50
Generating Device ID	51



Preface

- [Audience, on page vii](#)
- [Conventions, on page vii](#)
- [Related Documentation, on page ix](#)
- [Documentation Feedback, on page ix](#)
- [Communications, Services, and Additional Information, on page ix](#)

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 <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <i>this font</i> .
System output	Terminal sessions and information that the system displays appear in <i>this font</i> .

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



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



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



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



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



Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

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

Cisco UCS Documentation Roadmaps

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

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

**Note**

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

Documentation Feedback

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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



CHAPTER 1

New and Changed Information for this Release

This chapter contains the following sections:

- [New and Changed Information, on page 1](#)

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 6.7

Feature	Description	Where Documented
Shell options output updated to display additional details	The Generate Self-Signed Certificate and Certificate Signing Request option allows you to generate the self-signed SSL certificate. Starting with this release, Cisco UCS Director requires a self-signed SSL certificate. When you install Cisco UCS Director Release 6.7, the system checks if there is a self-signed certificate available or not. If there is no certificate available, when the administrator user logs in to the user interface, the systems prompts the user to generate the self-signed certificate.	Generating Self-Signed Certificates and Certificate Signing Requests
	The Configure Network Interface option allows you to generate a device ID for a cloned Cisco UCS Director appliance.	Generating Device ID, on page 51

Table 2: New Features and Changed Behavior in Cisco UCS Director Shell, Release 6.7.4.2

Feature	Description	Where Documented
Manage VMRC Tunneling Service option	Manage VMRC Tunneling Service option is newly added.	Managing VMRC Tunneling Service, on page 18



CHAPTER 2

Overview

This chapter contains the following sections:

- [Cisco UCS Director, on page 3](#)
- [Cisco UCS Director Shell, on page 4](#)
- [About Cisco UCS Director Shell Commands, on page 4](#)
- [Prerequisites, on page 6](#)
- [Logging in to the Shell, on page 6](#)

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) 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:

- Stopping/starting all Cisco services
- Display Service Status
- Stopping/starting the MySQL database
- Backing up/restoring the appliance database
- Changing ShellAdmin password
- Syncing up time
- Configuring network interface
- Enabling the database for a BMA Appliance
- Adding a BMA hostname/IP address to the appliance
- Displaying network details
- Pinging hostname/IP address
- Version (Cisco UCS Director appliance version)
- Importing CA (JKS) file
- Importing CA Cert (PEM) file for Virtual Network Computing (VNC)
- Shutdown of the Appliance
- Rebooting the Appliance
- Manage Root Access
- Troubleshooting by using Tail Inframgr logs
- Applying a patch to the appliance
- Login as Root
- Configuring Multi-node Setup
- Clean Up Patch Files
- Migrating from Single to Multi-Node
- Enabling HTTP access
- Configuring the defaulty UI
- Resetting MySql user password
- Applying signed patch to the appliance
- Terminating active GUI session(s)
- Quitting the shell

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

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.

Before you begin

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

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:6.6.0.0 Build:203 | UpTime: 05:44:00 up 121 days, 3:

```

01

```

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 MySQL 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 MySQL port 3306
 - 34) Quit
-



CHAPTER 3

Using Shell Commands

This chapter contains the following sections:

- [General Administration](#), on page 9
- [Examining the Version Information](#), on page 9
- [Changing Your Password](#), on page 10
- [Synchronizing the System Time](#), on page 10
- [Applying a Patch to Cisco UCS Director](#), on page 11
- [Applying a Signed Patch to Cisco UCS Director](#), on page 13
- [Shutting Down the Appliance](#), on page 14
- [Rebooting an Appliance](#), on page 14
- [Using a Multi-Node Setup](#), on page 15
- [Terminating Active GUI Sessions](#), on page 15
- [Granting Client Access to MySQL Port](#), on page 16
- [Denying Client Access to MySQL Port](#), on page 17
- [Regenerating Device Connector REST API Access Key](#), on page 17
- [Managing VMRC Tunneling Service](#), on page 18

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.

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      : 5.4.0.0
```

```
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**.

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 UNIX 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 continue...
```

Synchronizing the System Time

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

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 Tue Oct 27 11:26:44 UTC 2015
Hardware time is Tue Oct 27 11:26:44 2015 -0.345445 seconds
Do you want to sync systemtime [y/n]? n
Do you want to sync to NTP [y/n]? y
Enter NTP server to sync time with: 10.64.58.50
```

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

The following information is displayed:

```
ntpd (pid 2893) is running...
Shutting down ntpd: [ OK ]
27 Oct 11:17:25 ntpdate[1476]: step time server 10.64.58.50 offset -605.971324 sec
Synchronized time with NTP server '10.64.58.50'
Added NTP server '10.64.58.50' to /etc/ntp.conf
Starting ntpd: [ OK ]
synchronised to NTP server (10.64.58.50) at stratum 3
time correct to within 8145 ms
```

```
polling server every 64 s
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.

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>)

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 continue? [y/N]:
```

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

```
y
Stopping services...
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 [SFTP/SCP/FTP/HTTP/FILE]: SFTP
Server IP Address: XXX.XX.XXX.XXX
Server Username: XXXXX
Server Password:
SFTP Path to Patch Zip file: cucsd_patch_6_5_0_0_61705.zip
Apply the patch 'cucsd_patch_6_5_0_0_61705.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.

```
Y
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 SFTP/SCP/FTP/HTTP/FILE mode.
Specify the Transfer mode [SFTP/SCP/FTP/HTTP/FILE]: SFTP
Server IP Address: XXX.XX.XXX.XXX
Server Username: XXXXX
Server Password:
SFTP Path to Patch Zip file: cucsd_patch_6_5_0_0_61705.zip
Apply the patch 'cucsd_patch_6_5_0_0_61705.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

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]:
```

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 [SFTP/SCP/FTP/HTTP/FILE]: SCP
Server IP Address: 172.29.109.134
Server Username: root
Server Password:
Full Patch to Patch Zip File: /opt/mytest123/cucsd_patch_6_5_0_0_65341_signed.zip
Apply the patch '/opt/mytest123/cucsd_patch_6_5_0_0_65341_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 172.29.109.134
Completed downloading the patch.
Verifying patch signature...
Successfully verified the signature of patch file /opt/mytest123/cucsd_patch_6_5_0_0_65341_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.

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

The following information displays:

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

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

```
Broadcast message from root (pts/0) (Thu Sep 15 13:34:33 2013)
```

```
The system is shutting down NOW!
```

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.

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:

- One primary node
- One or more service nodes
- One monitoring database
- One inventory database



Note For a multi-node setup, you have to install the license on the primary node only.

A multi-node setup improves scalability by offloading the processing of system tasks, such as inventory data collection, from the primary node to one or more service nodes. You can assign certain systems tasks to one or more service nodes. The number of nodes determines how the processing of system tasks is scaled.

Node pools group service nodes and enable you to assign system tasks to more than one service node. If one service node is busy when a system task needs to be run, Cisco UCS Director uses a round-robin assignment to determine which service node should process the system task. If all, service nodes are busy, you can have the primary node run the system task.

For more information about how to configure the primary node and service nodes, and how to assign system tasks, see the [Cisco UCS Director Multi-Node Installation and Configuration Guide](#)

Terminating Active GUI Sessions

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 MySQL Port

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

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

The following information displays:

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

```
Source IP's configured
-----
10.197.110.92
-----
```

```
Do you want to grant/deny external clients access to MySQL 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 MySQL port 3306 :
```

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

The following information is displayed:

```
Enabling firewall rules for ip 10.197.110.92
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 MySQL Port

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

The following information displays:

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

```
Source IP's configured
-----
10.197.110.92
-----
```

```
Do you want to grant/deny external clients access to MySQL 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 MySQL port 3306 :
```

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

The following information is displayed:

```
Successfully denied ipaddress 10.197.110.92 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 a unique device connector key to identify itself. Choose this option to generate the device connector key.

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

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
Stopping VMRC Tunneling Service [PID=13539]
Press return to continue...
```



CHAPTER 4

Configuring Network Details

This chapter contains the following sections:

- [Configuring a Network Interface, on page 19](#)
- [Displaying Appliance Network Details, on page 20](#)

Configuring a Network Interface

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

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

```
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 configure E.g. eth0 or eth1:
```

Step 4 Enter the Ethernet interface to configure (for example, eth1) and press **Enter**. The following information is displayed:

```
Configuring STATIC IP for eth1...  
IP Address: 209.165.200.224  
Netmask: 255.255.255.0  
Gateway: 209.187.108.1  
DNS Server1: 198.51.100.1  
DNS Server2: 203.0.113.1  
Configuring Network with : INTERFACE(eth1), IP(209.165.200.224), Netmask(255.255.255.0),  
Gateway(209.187.108.1),  
DNS Server1(198.51.100.1), DNS Serverx 2(203.0.113.1)  
  
Do you want to continue [y/n]? :
```

Step 5 Enter **n** to discontinue the configuration process. Press **Enter** to complete the process.

Step 6 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 configure E.g. eth0 or eth1:
```

Step 7 Enter the Ethernet interface to configure (for example, eth0) and press **Enter**. The following information is displayed:

```
Select the IP version you want to configure [a) IPv4, b) IPv6] a/b :
```

Step 8 To configure IPv4, enter **a** and press **Enter**. The following information is displayed:

```
Static IP Mode enabled
Interface is configured with static IP. Moving to DHCP configuration may result in connectivity loss
for shelladmin. Do you want to configure DHCP [IPv4] for eth0 [y/n]? : y
Configuring DHCP [IPv4] for eth0....
Configuring DHCP IP for eth0
Successfully configured DHCP IP for eth0
```

Step 9 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.

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....
eth0      Link encap:Ethernet HWaddr 00:50:56:97:1E:2D
          inet addr:192.0.2.23 Bcast:192.0.2.255 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:127.0.0.1 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.



CHAPTER 5

Managing Cisco Services

This chapter contains the following sections:

- [Displaying the Status of Your Services, on page 21](#)
- [Stopping Cisco Services, on page 23](#)
- [Starting Cisco Services, on page 23](#)

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 provides 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.

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

The following list of services appears:

```
Cisco UCS Director Shell Menu
Node:Standalone | Version:6.6.0.0 Build:203 | UpTime: 05:44:00 up 121 days, 3:
```

01

```
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 MySQL 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 MySQL port 3306
34) Quit
```

```
SELECT> 2
```

Service	State	PID	%CPU	%MEM	tELAPSED	#Threads
broker	UP	12358	0.5	0.8	06:11	32
controller	UP	12385	1.7	1.3	06:06	45
eventmgr	UP	12391	29.4	6.0	06:02	41
client	UP	12398	28.8	5.9	05:57	40
idaccessmgr	UP	12404	30.7	6.0	05:52	41
inframgr	UP	12415	69.1	24.4	05:47	121
websock	UP	12588	0.0	0.0	05:42	1
tomcat	UP	12461	12.8	11.6	05:37	34
flashpolicyd	UP	12227	0.0	0.0	05:36	1

Database	IP Address	State	Client	Connections
infra	127.0.0.1	UP	localhost	17

Disk	Size	Used	Available	%Use	Usage
------	------	------	-----------	------	-------


```

-----
/dev/sda1    477M      111M      341M      25%      NORMAL
/dev/sdb     50G       28G       20G       59%      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**.

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.

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, on page 25](#)
- [Stopping the Database, on page 25](#)
- [Starting the Database, on page 26](#)
- [Backing Up the Database, on page 26](#)
- [Restoring the Database, on page 28](#)

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 mysql daemon (mysqld) 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

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 database...
Database stopped.
  Stopping broker [PID=13113]/[Child=13115]
  Stopping controller [PID=13139]/[Child=13142]
  Stopping eventmgr [PID=13146]/[Child=13149]
  Stopping client [PID=13153]/[Child=13156]
13167
13173]
  Stopping idaccessmgr [PID=13163]/[Child=]
  Stopping inframgr [PID=13170]/[Child=]
  Tomcat is running with [PID=13216]. Stopping it and its child process
  Flashpolicyd is not running
Stopping websock[PID=13342]
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 mysql daemon (mysqld) by choosing the **Start Database** option.



Note This option starts the appliance database only.

- 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...
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.

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:

```
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 FTP/SFTP/SCP protocol.
Specify the transfer mode and login credentials
```

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.

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

Step 2 Press **Enter**.

The following information displays:

```
Restore database.....
Restore will recover file from an FTP/SFTP server or can copy the backup file through SCP mode to
another server.
Provide the necessary mode of transfer and access credentials
Please provide transfer mode[FTP/SFTP/SCP]:
```

Step 3 Enter your mode of transfer 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, on page 31](#)
- [Enabling the Database for Cisco UCS Director Bare Metal Agent, on page 31](#)

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.

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:192.0.2.1
Enter Cisco UCS Director Baremetal Agent Hostname:192.44.2.1
Adding host entry 192.3.55.1 to /etc/hosts
Entry 192.3.55.1 does not exist
Backed up old file...
Added new entry 192.3.55.1
Added 192.44.2.1 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.

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: 192.168.0.241
```

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

The following information is displayed:

```
Cisco UCS Director Baremetal Agent Hostname/IP Address: 192.0.2.0
Enabling 'remote database' access for 192.0.2.0
Enabling remote database access to 192.0.2.0
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 (192.0.2.0) 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 (192.0.2.0) 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 192.0.2.01
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: 192.0.2.0
INFO (DBEnableRemoteAccess.java:679) Enabled 'Remote' database access for: 192.0.2.0
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, on page 33](#)
- [Generating Self-Signed Certificates and Certificate Signing Requests, on page 33](#)
- [Importing Certification Authority or Self-Signed Certificates, on page 34](#)

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.

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:

```
Domain Name [localdom]:
```

Step 2 Enter the domain name and press **Enter**.

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

The following information is displayed:

How many days is self-signed certificate valid for [Choose value which is greater than 5 years and less than 15 years]? [1825]:

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

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) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My 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 []:
```

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 Widgits 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.

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:

```
Domain Name [localdom]:
```

Step 2 Enter the domain name 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 CA/self-signed certificate [/opt/certs/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.
```

```
Do you want to import the certificate file:///opt/certs/localdom.pem into WebProxy for secured access to VM console through VNC [y/n]?:
```

Step 6 Enter **y** and press **Enter** to import the certificate file into WebProxy for secured access to the VM console through VNC.

The following information is displayed:

```
Certificate file:///opt/certs/localdom.pem imported to WebProxy succesfully.  
Press return to continue ...
```



CHAPTER 9

Managing Root Access

This chapter contains the following sections:

- [Accessing Root Privileges, on page 37](#)
- [Configuring Root Access, on page 37](#)
- [Enabling Root Access, on page 38](#)
- [Disabling Root Access, on page 38](#)
- [Logging in as Root, on page 39](#)

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.



Note Compiling software as root is not recommended for security reasons.

Configuring Root Access

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

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:

```
Do you want to Configure/Set Root Privilege/Password [y/n]? :
```

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

The following information is displayed:

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

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

The following information is displayed:

```
Retype new UNIX password:
```

Step 5 Enter your new UNIX password and press **Enter**.

The following information displays:

```
passwd: all authentication tokens updated successfully.
Root passwd changed successfully
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**.

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

The following information displays:

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

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

The following information is displayed:

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

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

Choose this option to disable root privileges.

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

The following information displays:


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

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

The following information displays:

```
Do you want to Disable Root Access [y/n]? :
```

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

The following information is displayed:

```
disabling root access...
  Locking password for user root.
  Passwd: Success
  Root access disabled successfully
  Press return to continue...
```

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

Logging in as Root

You can log in as root by choosing the **Login As Root** option.

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:

```
Logging as root
Password:
[root@localhost shelladmin]#
```

Step 4 Enter your password and press **Enter**.

Step 5 Enter **exit** to return to the shelladmin.

Information similar to the following is displayed:

```
[root@localhost shelladmin]# cd /opt
[root@localhost opt]# exit
exit
Successful login
Press return to continue ...
```



CHAPTER 10

Troubleshooting

This chapter contains the following sections:

- [Backing up the Monitoring Database in a Multi-Node Setup, on page 41](#)
- [Pinging the Hostname and IP Address, on page 41](#)
- [Viewing Tail Inframgr Logs, on page 42](#)
- [Cleaning Up Patch Files, on page 43](#)
- [Collecting Logs from a Node, on page 43](#)
- [Collecting Diagnostics, on page 45](#)
- [Using Diagnostics Information, on page 47](#)
- [Troubleshooting VMware Console Display Issues, on page 48](#)
- [Enabling HTTP Access, on page 48](#)
- [Resetting MYSQL User Password in a Multi-Node Setup, on page 49](#)
- [Resetting MYSQL User Password in a Standalone Setup, on page 50](#)
- [Generating Device ID, on page 51](#)

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.

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.

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 : 209.165.200.224
PING 209.165.200.224 (209.165.200.224) 56(84) bytes of data.
64 bytes from 209.165.200.224: icmp_seq=1 ttl=64 time=9.90 ms
64 bytes from 209.165.200.224: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 209.165.200.224: icmp_seq=3 ttl=64 time=0.254 ms
64 bytes from 209.165.200.224: icmp_seq=4 ttl=64 time=0.198 ms
64 bytes from 209.165.200.224: icmp_seq=5 ttl=64 time=0.267 ms

--- 209.165.200.224 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.

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

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.

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

The following list of services appears:

```

                Cisco UCS Director Shell Menu
Node:Standalone | Version:6.6.0.0 Build:203 | UpTime: 05:44:00 up 121 days, 3:
01

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 MySQL 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 MySQL port 3306
- 34) Quit

Step 2 Enter the Logs Collection option.

- 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.

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

The following information is displayed:

```
Diagnostics Menu
=====
Options:
 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
 7) Exit
```

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
```

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 -xvzf 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.

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.

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 MYSQL User Password in a Multi-Node Setup

Step 1 From the Cisco UCS Director Shell menu, choose the **Reset MYSQL User password** option and press **Enter**. The following information is displayed:

```
This utility will restart the services after changing MYSQL 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 MySQL 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 MYSQL '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 MYSQL 'admin' user? [y/n]:
```

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

The following information is displayed:

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

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

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

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

The following information is displayed:

```
MYSQL 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
Uploaded file:/opt/certs/mysql/dbkeys.key
Trying to get session to xxx.xxx.xxx.xxx...
Trying to connect...
Successfully connected
Uploaded file:/opt/certs/mysql/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 MySQL 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 MySQL user password, you should execute the Reset MySQL User password option in all the nodes in the following sequence inventory, monitoring, primary, and service nodes.

Resetting MySQL User Password in a Standalone Setup

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

The following information is displayed:

```

This utility will restart the services after changing MySQL 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 MySQL 'admin' user? [y/n]:

```

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

The following information is displayed:

```

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

```

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

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

The following information is displayed:

```
Specify the new password for MySQL 'admin' user:
Confirm the new password for MySQL '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 MySQL 'root' user? [y/n]:
```

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

The following information is displayed:

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

Starting the infra services...
```

Step 8 If you entered **n**, enter the new password for MySQL 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 MySQL 'root' user:
Confirm the new password for MySQL 'root' user:
Password update takes few minutes. Please wait..... done

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

Starting the infra services...
```

Note After resetting the MySQL 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.

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, on page 19](#).
