



Cisco UCS Director Shell Guide, Release 6.0

First Published: 2016-09-16

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.

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: <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. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface vii

Audience vii

Conventions vii

Related Documentation ix

Documentation Feedback ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information for this Release 1

CHAPTER 2

Overview 3

Cisco UCS Director 3

Cisco UCS Director Shell 4

About Cisco UCS Director Shell Commands 5

Prerequisites 5

Logging in to the Shell 6

CHAPTER 3

Using Shell Commands 7

General Administration 7

Examining the Version Information 7

Changing Your Password 8

Synchronizing the System Time 8

Applying a Patch to Cisco UCS Director 9

Shutting Down the Appliance 10

Rebooting an Appliance 10

Using a Multi-Node Setup 11

CHAPTER 4**Configuring Network Details 13**

- Configuring a Network Interface 13
- Displaying Appliance Network Details 14

CHAPTER 5**Managing Cisco Services 15**

- Displaying the Status of Your Services 15
- Stopping Cisco Services 17
- Starting Cisco Services 17

CHAPTER 6**Managing Databases 19**

- Working with Databases 19
- Stopping the Database 19
- Starting the Database 20
- Backing Up the Database 21
- Restoring the Database 21

CHAPTER 7**Managing Bare Metal Agent Details 23**

- Adding the Cisco UCS Director Bare Metal Agent Hostname and IP Address 23
- Enabling the Database for Cisco UCS Director Bare Metal Agent 24

CHAPTER 8**Managing Certificates 27**

- Managing SSL Certificates 27
- Generating Self-Signed Certificates and Certificate Signing Requests 27
- Importing Certification Authority or Self-Signed Certificates 28

CHAPTER 9**Managing Root Access 31**

- Accessing Root Privileges 31
- Configuring Root Access 31
- Enabling Root Access 32
- Disabling Root Access 32
- Logging in as Root 33

CHAPTER 10**Troubleshooting 35**

- Backing up the Monitoring Database in a Multi-Node Setup 35

[Pinging the Hostname and IP Address](#) 35

[Viewing Tail Inframgr Logs](#) 36

[Collecting Logs from a Node](#) 37

[Collecting Diagnostics](#) 38

[Troubleshooting VMware Console Display Issues](#) 38



Preface

- [Audience, page vii](#)
- [Conventions, page vii](#)
- [Related Documentation, page ix](#)
- [Documentation Feedback, page ix](#)
- [Obtaining Documentation and Submitting a Service Request, 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> .

Text Type	Indication
System output	Terminal sessions and information that the system displays appear in <i>this font</i> .
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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). RSS feeds are a free service.



CHAPTER

1

New and Changed Information for this Release

- [New and Changed Information for this Release, page 1](#)

New and Changed Information for this Release

No significant changes were made to this guide for the current release.



Overview

This chapter contains the following sections:

- [Cisco UCS Director, page 3](#)
- [Cisco UCS Director Shell, page 4](#)
- [About Cisco UCS Director Shell Commands, page 5](#)
- [Prerequisites, page 5](#)
- [Logging in to the Shell, 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 network 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, as needed, basis.

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
- Synching 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
- Quitting the shell
- Login as Root
- Configuring Multi-node Setup
- Clean Up Patch Files
- Migrating from Single to Multi-Node

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:6.0.0.0 | UpTime: 19:57:52 up 2 days, 14:23

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) Quit
```




Using Shell Commands

This chapter contains the following sections:

- [General Administration, page 7](#)
- [Examining the Version Information, page 7](#)
- [Changing Your Password, page 8](#)
- [Synchronizing the System Time, page 8](#)
- [Applying a Patch to Cisco UCS Director, page 9](#)
- [Shutting Down the Appliance, page 10](#)
- [Rebooting an Appliance, page 10](#)
- [Using a Multi-Node Setup, page 11](#)

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.
 - Make a backup of your database prior to taking the patch. The Apply Patch option lets you to make a backup as part of the Apply Patch procedure; but the best practice is to create 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 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...
Do you want to take database backup before applying patch (y/n)?
```

Step 2 If you entered y, enter the requested FTP server IP address and login data, then press Enter.

```
y
Backup will upload file to an FTP server.
Provide the necessary access credentials.
  FTP Server IP Address:
  FTP Server Login:
```

Step 3 If you entered n, enter the patch IP address and press Enter.

```
n
```

```
Applying Patch:
Patch URL: http://xxx.xxx.x.xxx/TestPkg.zip
```

```
Applying the Patch http://xxx.xxx.x.xxx/TestPkg.zip [y/n]? y
```

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

- Step 4** If you are prompted to confirm that you want to apply the patch, enter y, then press Enter. Follow the onscreen prompts to complete the process.
-

What to Do Next

After the patch is applied, start the services on the appliance using the Start Services 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](#)



Configuring Network Details

This chapter contains the following sections:

- [Configuring a Network Interface](#), page 13
- [Displaying Appliance Network Details](#), page 14

Configuring a Network Interface

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

Step 1 From the Cisco UCS Director Shell menu, choose Configure a Network Interface and press Enter. The following information displays:

```
Do you want to Configure DHCP/STATIC IP [D/S] ? : 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 Enter s to configure a static IP address 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 displays:

```
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 return to complete the process.

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.



Managing Cisco Services

This chapter contains the following sections:

- [Displaying the Status of Your Services, page 15](#)
- [Stopping Cisco Services, page 17](#)
- [Starting Cisco Services, page 17](#)

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.

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:6.0.0.0 | UpTime: 19:57:52 up 2 days, 14:23
```

- 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) 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.
-



Managing Databases

This chapter contains the following sections:

- [Working with Databases, page 19](#)
- [Stopping the Database, page 19](#)
- [Starting the Database, page 20](#)
- [Backing Up the Database, page 21](#)
- [Restoring the Database, page 21](#)

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 websocket[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 server. Before you begin the backup process, you must first stop the Cisco services. To stop the services, choose the Stop Services option.

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

- FTP server's IP address (where the database is backed up)
- FTP server's login credentials

**Note**

After the FTP credentials are provided, the entire database of the Cisco UCS Director appliance is backed up at the specified FTP 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.

Step 3 Press **Enter**.

The following information is displayed:

```
Backing database.....
```

```
Backup will Upload file to an FTP server. Provide the necessary access credentials
```

```
FTP Server IP Address: xxxx.xxxx.xxxx.xxxx
```

```
FTP Server Login:
```

Step 4 Enter your FTP Server IP address and press Enter.

Step 5 Enter your FTP Server login name and press Enter.

Step 6 Enter your FTP Server password and press Enter.

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 server's IP address (from where the database is restored)
- FTP server's login credentials
- Restore filename

- Confirm to restore

**Note**

After FTP credentials are provided, the entire database of the Cisco UCS Director appliance is restored from the specified FTP 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 server. Provide the necessary access credentials

FTP Server IP Address:
FTP Server Login: root
FTP Server Password:
```

Step 3 Enter your FTP server IP address and press Enter.

Step 4 Enter your FTP server login and press Enter.

Step 5 Enter your FTP server password and press the Enter.

Step 6 Follow the onscreen prompts to complete the process.

Step 7 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, page 23](#)
- [Enabling the Database for Cisco UCS Director Bare Metal Agent, page 24](#)

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 database - 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
Sucessfully 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, page 27](#)
- [Generating Self-Signed Certificates and Certificate Signing Requests, page 27](#)
- [Importing Certification Authority or Self-Signed Certificates, page 28](#)

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? [365]:
```

Step 3

Enter the number of days that you want the self-signed certificate to be valid for and press Enter.

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).
```

```
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 or self-signed certificate using the Importing CA/Self-Signed Certificate option.

-
- Step 1** From the Cisco UCS Director Shell menu, choose the Importing 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 or self-signed certificate, 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
- ```
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 ...
```
-



Managing Root Access

This chapter contains the following sections:

- [Accessing Root Privileges, page 31](#)
- [Configuring Root Access, page 31](#)
- [Enabling Root Access, page 32](#)
- [Disabling Root Access, page 32](#)
- [Logging in as Root, page 33](#)

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 ...
```



Troubleshooting

This chapter contains the following sections:

- [Backing up the Monitoring Database in a Multi-Node Setup, page 35](#)
- [Pinging the Hostname and IP Address, page 35](#)
- [Viewing Tail Inframgr Logs, page 36](#)
- [Collecting Logs from a Node, page 37](#)
- [Collecting Diagnostics, page 38](#)
- [Troubleshooting VMware Console Display Issues, page 38](#)

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 remotng 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.

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:6.0.0.0 | UpTime: 19:57:52 up 2 days, 14:23

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) Quit

SELECT>
    
```

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 generates a Summary Report (SummaryReport.txt) and a detail report (DiagOutput.txt) and stores these files under /opt/diagnostics.

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

Information similar to the following appears, advising you that the diagnostic files have been created:

```
SELECT> 27

*****
Diagnostic Tool
*****

Please find the below files under /opt/diagnostics :
Summary Report: SummaryReport.txt
Diagnostics report: DiagOutput.txt

/opt/diagnostics/rules

Press return to continue...
```

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.
