Using Shell Commands

This chapter contains the following sections:

General Administration

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

Examining the Version Information

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

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...
Sucessfully 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 sucessful
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, form 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 an 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.