Troubleshooting

This chapter contains the following sections:

Backing up the Monitoring Database in a Multi-Node Setup

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

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

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) 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 presss <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 presss <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 presss <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 presss <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 presss <Enter> : 5
```

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

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

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

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

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
Uloaded 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.