Cisco UCS Director Upgrade Guide, Release 6.5

First Published: 2017-07-11

Last Modified: 2019-09-17

Upgrading Cisco UCS Director to Release 6.5

Overview of the Upgrade to Cisco UCS Director, Release 6.5

The upgrade process to Cisco UCS Director, Release 6.5 depends on the current version of the software that is installed on your system. For information on supported upgrade paths, see Supported Upgrade Paths for Cisco UCS Director, Release 6.5(0.4), on page 1.

Cisco UCS Director, Release 6.5 is installed on two disks in the virtual machine (VM). One disk hosts the operating system and the Cisco UCS Director application. The second disk hosts the the Cisco UCS Director database. See Prerequisites for Upgrading to Cisco UCS Director, Release 6.5, on page 4.

Supported Upgrade Paths for Cisco UCS Director, Release 6.5(0.4)

Important Prior to upgrading to Cisco UCS Director Release 6.5(0.4), you must upgrade the Bare Metal Agent to version 6.5(0.2). See Supported Upgrade Paths for Bare Metal Agent Patch Release 6.5(0.2), on page 2.

Important Cisco UCS Director Release 6.5(0.4) includes fixes for security vulnerabilities reported in releases 6.5, 6.5(0.1), 6.5(0.2), and 6.5(0.3). Cisco UCS Director Releases 6.5, 6.5(0.1), 6.5(0.2), and 6.5(0.3) are no longer available for download. For information on the security vulnerabilities reported in releases 6.6 and 6.6(1.0), see the security advisories for CVE-2019-1938, CVE-2019-1935, CVE-2019-1974, CVE-2019-1937, CVE-2019-12634 and CVE-2019-1936 available at this link:

https://tools.cisco.com/security/center/publicationListing.x

The following are the supported upgrade paths to Cisco UCS Director, Release 6.5(0.4):

- From Release 6.5(0.3) to Release 6.5(0.4)
- From Release 6.5(0.2) to Release 6.5(0.4)
- Fom Release 6.5(0.1) to Release 6.5(0.4)
- Fom Release 6.5 to Release 6.5(0.4)

Supported Upgrade Paths from Release 6.0

The following are the supported upgrade paths to Cisco UCS Director, Release 6.5(0.4):

- From Release 6.0(1.3) to Release 6.5(0.1) to Release 6.5(0.4)
- From Release 6.0(1.2) to Release 6.5(0.0) to Release 6.5(0.4)
- From Release 6.0(1.1) to Release 6.5(0.0) to Release 6.5(0.4)
- From Release 6.0(1.0) to Release 6.5(0.0) to Release 6.5(0.4)

Supported Upgrade Paths for Bare Metal Agent Patch Release 6.5(0.2)

The following are the supported upgrade paths for the Bare Metal Agent Patch Release 6.5(0.2):

- From Release 6.5(0.1) to Patch Release 6.5(0.2)
- From Release 6.5 to Patch Release 6.5(0.2)

Digitally Signed Images

Cisco UCS Director images are delivered in digitally signed zip files. These signed zip files are wrapped in a container zip file that includes the following:

- Digitally signed zip file—Contains the Cisco UCS Director installation or upgrade image
- Verification program—Verifies the certificate chain and signature. During certificate chain validation, the program verifies the authenticity of the end-entity certificate using Cisco's SubCA and root CA certificates. Then, the authenticated end-entity certificate is used to verify the signature.
- Digital signature file—Contains the signature that you can verify before installation or upgrade.
- Certificate file—Enables you to verify the digital signature. This Cisco-signed x.509 end-entity certificate contains a public key that can be used to verify the signature. This certificate is chained to the Cisco root posted on http://www.cisco.com/security/pki/certs/crcam2.cer.
- ReadMe file—Provides the information and instructions required to verify the digitally signed zip file.

Verify the image offline. Once the image is verified, you can begin the installation or upgrade of Cisco UCS Director.

Note For upgrading to Release 6.5, you can verify the digital signature of the patch manually and then use the `Apply Patch` option to upgrade. See Verifying a Digitally Signed Image, on page 3.

Requirements for Verifying Digitally Signed Images

Before you verify a Cisco UCS Director digitally signed image, ensure that you have the following on your local machine:

- Connectivity to https://www.cisco.com during the verification process

- Python 2.7.4 or later
- OpenSSL

Verifying a Digitally Signed Image

Before you begin

Download the Cisco UCS Director image from Cisco.com.

Procedure

Step 1 Unzip the file you downloaded from Cisco.com and verify that it contains the following files:

- ReadMe file
- Digitally signed zip file, for example `CUCSD_6_5_0_0_65365_VMWARE_GA.zip`, `CUCSD_6_5_0_0_65717_HYPERV_GA.zip`, or `cucsd_patch_6_5_0_0_65365.zip`
- Certificate file, for example `UUCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`
- Digital signature generated for the image, for example `CUCSD_6_5_0_0_65365_VMWARE_GA.zip.signature`, `CUCSD_6_5_0_0_65717_HYPERV_GA.zip.signature`, or `cucsd_patch_6_5_0_0_65365.zip.signature`
- Signature verification program, for example `cisco_x509_verify_release.py`

Step 2 Review the instructions in the ReadMe file.

Note If there are any differences between these instructions and those in the ReadMe, follow the ones in the ReadMe.

Step 3 Run the signature verification program.

Example: Signature Verification for Upgrade Patch

```
python cisco_x509_verify_release.py -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i cucsd_patch_6_5_0_0_65365.zip -s cucsd_patch_6_5_0_0_65365.zip.signature -v dgst -sha512
```

Example: Signature Verification for VMware OVF Installation

```
python cisco_x509_verify_release.py -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i CUCSD_6_5_0_0_65365_VMWARE_GA.zip -s CUCSD_6_5_0_0_65365_VMWARE_GA.zip.signature -v dgst
 -sha512
```

Example: Signature Verification for Hyper-V VHD Installation

```
python cisco_x509_verify_release.py -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
 -i CUCSD_6_5_0_0_65717_HYPERV_GA.zip -s CUCSD_6_5_0_0_65717_HYPERV_GA.zip.signature -v
dgst -sha512
```

Step 4 Review the output and ensure that the verification has succeeded.

Example: Expected Output for Upgrade

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
```

```
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer
...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of cucsd_patch_6_5_0_0_65365.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

Example: Expected Output for VMware OVF Installation

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer
...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of CUCSD_6_5_0_0_65365_VMWARE_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

Example: Expected Output for Hyper-V VHD Installation

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer
...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of CUCSD_6_5_0_0_65717_HYPERV_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

What to do next

Install or upgrade Cisco UCS Director.

Upgrading Cisco UCS Director

Prerequisites for Upgrading to Cisco UCS Director, Release 6.5

Complete the following prerequisites before you upgrade your current Cisco UCS Director software to Release 6.5.

Plan a Maintenance Window

The upgrade to Release 6.5 requires that you stop all Cisco UCS Director services during the upgrade.We recommend that you plan a maintenance window of between 2 and 4 hours. Prior to upgrade, the length of the mainteannce window depends on the size of your database

For a multi-node setup, you can reduce the length of the maintenance window by upgrading some of the nodes in parallel. See Upgrading a Multi-Node Setup to Release 6.5, on page 8.

Download Cisco UCS Director, Release 6.5 and Verify the Signed Image

Download the Cisco UCS Director, Release 6.5 software patch from http://www.cisco.com and then verify the digitally signed image. See Digitally Signed Images, on page 2.

Place the Verified Release 6.5 Software Patch on a Server

Place the Release 6.5 software patch on the FTP or HTTP server that you plan to use to install the upgrade.

Analyze Your Custom Scripts and Ensure Compatibility

If your existing Cisco UCS Director, Release 6.0(x.x) deployment includes custom tasks, download and run the Custom Task Script Analyzer. The analyzer evaluates all the custom scripts in the Cisco UCS Director database without executing any tasks and then outputs an analysis report.on your custom tasks.

If the report indicates any compatibility issues, resolve these issues in your Release 6.0(x.x) system before completing the upgrade. See Upgrading Custom Tasks, on page 13.

Take a Snapshot of the Current Cisco UCS Director VM

We recommend that you take a snapshot of the current Cisco UCS Director VM before you begin the upgrade. Before you take the VM snapshot, make sure the services and the OS are shutdown gracefully and the VM is in powered off state. If you do this, you do not need to back up the existing configuration database through an FTP server.

Add a Second Virtual Disk to the Cisco UCS Director VM

Cisco UCS Director, Release 6.5 installs the database on a second disk in the VM. We recommend that you create this disk before you start the upgrade. If you do not create the disk first, the upgrade will be stopped until you have done so.

For a standalone setup, add the second virtual disk to the VM for the main appliance. You do not need to add a second disk for the Cisco UCS Director Bare Metal Agent VM.

For a multi-node setup, add the second virtual disk to the following nodes:

- Inventory database node
- Monitoring database node

To add the second disk, perform the following in your hypervisor manager:

1. Power off your Cisco UCS Director VM.
2. Add a second disk to the VM that meets the minimum requirements. See Database Disk Requirements, on page 5. If you do not know the size of your current database, after you choose `Apply Patch` in ShellAdmin, the upgrade displays that information.
3. Power on your Cisco UCS Director VM.

Database Disk Requirements

When you add the second virtual disk to the Cisco UCS Director before you upgrade, ensure that the disk meets the following requirements. These requirements apply to Cisco UCS Director VMs hosted on either VMware vSphere or Microsoft Hyper-V.

Note You only need to add the second disk. The Release 6.5 upgrade handles the formatting, database installation, and data transfer for that disk.

Element	Requirement
Disk Size	The recommended size for the second disk is 2 times the size of the current Cisco UCS Director database. The minimum size for the second disk is 1.5 times the size of the current Cisco UCS Director, or 100G, whichever is higher. The upgrade fails if the second disk is smaller than the minimum size. For example, if your current Cisco UCS Director database size is 80GB, we recommend that your database disk is 160GB. The minimum size is 120GB. If your current Cisco UCS Director database size is only 40G, the minimum size of the second disk is 100G (and not 60G). You can use the `Display Service Status` option to know the status of any associated databases and disks. If you do not know the size of your current database, the upgrade procedure provides that information.
Datastore	High performance datastore. For optimal performance, the datastore must support a minimum IOPS of 1,200 or higher for both read and write operation. If the datastore is slow, the performance of Cisco UCS Director is directly impacted.
Disk Type	Serial Atached SCSI (SAS) disk
Disk Format	Thick Provisioned (Lazy Zeroed) format

Upgrading a Single Node Setup to Release 6.5

Before you begin

Complete all prerequisites in Prerequisites for Upgrading to Cisco UCS Director, Release 6.5, on page 4.

Procedure

Step 1 Log in to the Cisco UCS Director ShellAdmin.

Step 2 To verify that all services are running, choose `Display services status`.

All services must be running before you start the upgrade procedure. If necessary, choose `Start services` and then verify that all services are running.

Step 3 To upgrade Cisco UCS Director to Release 6.5, choose `Apply patch`.

Step 4 At the `Services will be stopped before applying patch. Do you want to continue [y/n]?`, enter **`y`**.

When all services are stopped, the upgrade continues.

Step 5 At the `Do you want to take database backup before applying patch [y/n]?` prompt, enter one of the following:

- **`y`** to back up the Cisco UCS Director database.
- **`n`** if you took a snapshot of the VM before you started and do not want to take an additional backup.

Step 6 When prompted for the `Patch URL`, type the location of the Release 6.5 patch and press **`Enter`**

For example, if you stored the patch file on an FTP server, enter **ftp:**//*username*:*password*@*hostname*|*IP_address*/*software_location_and_name*

Step 7 Wait for the patch file to download to the Cisco UCS Director VM.

If the patch installation fails after the download because you did not add a second disk before the upgrade, do the following in your hypervisor manager:

1. Power off your Cisco UCS Director VM.
2. Add a second disk to the VM that meets the minimum requirements. See Database Disk Requirements, on page 5. If you do not know the size of your current database, the upgrade message provides that information.
3. Power on your Cisco UCS Director VM.

After you have added the second disk, repeat this upgrade procedure, starting at step 1.

Step 8 Wait for the patch upgrade to complete. .

The upgrade process performs extra steps including the following:

- Unpacks the patch file.
- Installs the Release 6.5 files
- Formats the second database disk.
- Copies the existing database to the new disk.
- Initializes the database schema.
- Reboots the Cisco UCS Director appliance. The Cisco UCS Director services start automatically.

Depending upon the size of your database, the upgrade process can take several minutes to complete.

Note The patch process is not complete or successful until all Cisco UCS Director services have been started, Cisco UCS Director is available, the login screen is displayed, and the administrator can log in to Cisco UCS Director.

All Cisco UCS Director services must be started before you attempt to perform other ShellAdmin procedures, such as apply additional patches, take a database backup, or restore a database from a backup.

Step 9 When the upgrade is complete, verify that the version and build in the Cisco UCS Director ShellAdmin match the version and build of the patch that you downloaded from Cisco.com.

You can find the version and build in the following locations:

- Beneath the title of the Shell menu
- From the `Show Version` option in ShellAdmin

Upgrading a Multi-Node Setup to Release 6.5

Before you begin

Complete all prerequisites in Prerequisites for Upgrading to Cisco UCS Director, Release 6.5, on page 4.

Procedure

Step 1 Log in to the Cisco UCS Director ShellAdmin on the primary node and all service nodes.

Step 2 On the primary node and all service nodes, to verify that all services are running, choose `Display services status`.

All services must be running before you start the upgrade procedure. If necessary, choose `Start services` and then verify that all services are running.

Step 3 On the primary and all service nodes, choose `Stop services` and ensure that all services all stopped on the nodes.

Ensure that all services are stopped on the primary and service nodes before you can upgrade the inventory and monitoring database nodes.

Step 4 In the ShellAdmin for the inventory database node and the monitoring database node, choose `Apply patch` to upgrade the nodes to Release 6.5.

Step 5 At the `Services will be stopped before applying patch. Do you want to continue [y/n]?`, enter **`y`**.

When all services are stopped on the database nodes, the upgrade continues.

Step 6 At the `Do you want to take database backup before applying patch [y/n]?` prompt, enter one of the following:

- **`y`** to back up the Cisco UCS Director database.
- **`n`** if you took a snapshot of the VM before you started.

Step 7 When prompted for the `Patch URL`, type the location of the Release 6.5 patch and press **`Enter`**

For example, if you stored the software patch on an FTP server, enter
ftp://*username*:*password*@*hostname*|*IP_address*/*software_location_and_name*

Step 8 Wait for the patch to download to the Cisco UCS Director VM.

If the patch installation fails after the download because you did not add a second database disk to the inventory database and monitoring database nodes, do the following in your hypervisor manager:

1. Power off your Cisco UCS Director VM.

2. Add a second disk to the VM that meets the minimum requirements. See Database Disk Requirements, on page 5. If you do not know the size of your current database, the upgrade message provides that information.
3. Power on your Cisco UCS Director VM.

When you have added the database disk, repeat this upgrade procedure, starting at step 1.

Step 9 Wait for the patch upgrade to complete. .

The upgrade process performs many steps including the following:

- Unpacks the patch file.
- Installs the Release 6.5 files
- Formats the second database disk.
- Copies the existing database to the new disk.
- Initializes the database schema.
- Reboots the Cisco UCS Director appliance. The Cisco UCS Director services start automatically.

Depending upon the size of your database, the upgrade process can take several minutes to complete.

Step 10 In the ShellAdmin, choose `Display services status` and verify that all database services on the monitoring database node and inventory database node have started.

If necessary, you can choose the `Start Database` option to start the services on the database nodes.

Step 11 Upgrade the service nodes using the `Apply Patch` option as described in the steps above.

Step 12 Upgrade the primary node using the `Apply Patch` option as described in the steps above.

Note The patch process is not complete or successful until all Cisco UCS Director services have started, Cisco UCS Director is available, the login screen is displayed, and the admin user can log in to Cisco UCS Director.

All Cisco UCS Director services must be started before you attempt to perform other ShellAdmin procedures, such as apply additional patches, take a database backup, or restore a database from a backup.

Step 13 Verify that all services have started on the service nodes and the primary nodes.

Step 14 When the upgrade is complete, verify that the version and build in the Cisco UCS Director ShellAdmin on all nodes match the version and build of the patch that you downloaded from Cisco.com.

You can find the version and build in the following locations:

- Beneath the title of the Shell menu
- From the `Show Version` option in ShellAdmin

Upgrading Cisco UCS Director Baremetal Agent

Upgrading Bare Metal Agent to Release 6.5

Before you begin

Upgrade Cisco UCS Director to Release 6.5.

Procedure

Step 1 Download the Bare Metal Agent, Release 6.5 patch to the existing Bare Metal Agent VM.

Step 2 Log in to the Bare Metal Agent console through PuTTY or another Secure Shell (SSH) client, using the default root credentials shown or the root credentials for your system.

```
Username: root
Password: pxeboot
```

Step 3 Navigate to the `/opt/infra` directory and run **StopInfraAll.sh** to stop the services.

Step 4 Unzip the patch file.

Step 5 Navigate to the directory of the unzipped file.

```
cd ucsd_bma_patch_6_5_0_0
```

Step 6 Run **./applyPatch.sh** to apply the patch to Bare Metal Agent.

Step 7 Wait for the installation to complete.

Step 8 Navigate to the `/opt/infra` directory.

Step 9 Run **./showBMAVersion.sh** to verify that you have the correct version of Bare Metal Agent.

Step 10 Run **startInfraAll.sh** to start the Bare Metal Agent services.

Step 11 Run **statusInfra.sh** to check the status of the Bare Metal Agent services.

Step 12 When you upgrade the Bare Metal Agent from 6.0.0.0 to 6.5.0.0, wait for the upgrade to complete. Once the Bare Metal Agent appliance is up, wait for 5 minutes and then execute the following commands in the Bare Metal Agent console.

```
setsebool -P samba_export_all_ro=1 samba_export_all_rw=1
find /opt/cnsaroot/templates/ -name "Win*" -exec ln -s '{}' /var/www/html/ \;
```

Step 13 When you upgrade the Bare Metal Agent from 6.0.1.0 to 6.5.0.0, wait for the upgrade to complete and reboot the Bare Metal Agent appliance. Once the Bare Metal Agent appliance is up, wait for 5 minutes and then execute the following commands in the Bare Metal Agent console.

```
setsebool -P samba_export_all_ro=1 samba_export_all_rw=1
find /opt/cnsaroot/templates/ -name "Win*" -exec ln -s '{}' /var/www/html/ \;
```

Step 14 Log in to Cisco UCS Director, Release 6.5, and choose **Administration** > **Physical Accounts** > **Bare Metal Agents**.

Note If you have missed to upgrade Cisco UCS Director to Release 6.5, you should run **/opt/infra-bin/syncDbCredentialsToBMA.sh** from the Cisco UCS Director appliance.

Step 15 Choose the account for the Bare Metal Agent that you have upgraded.

If your system has more than one instance of Bare Metal Agent, you can identify the correct account by the IP address.

Step 16 Confirm that the Bare Metal Agent account is reachable from Cisco UCS Director and then stop and start the services for that account.

Upgrading Cisco UCS Director PowerShell Agent

Downloading Cisco UCS Director PowerShell Agent

Download the installer for PowerShell Agent from Cisco UCS Director to your native Windows machine.

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 Click **PowerShell Agents**.

Step 3 Click **Download Installer**.

Step 4 Review the list of installation requirements on the **Download Agent Installer** page. Ensure that you have them available on the Windows machine where you plan to install the PowerShell Agent.

Step 5 Click **Submit**.

The `PSASetup.exe` file is downloaded to your native Windows machine default download folder.

What to do next

Install Cisco UCS Director PowerShell Agent on your Windows machine.

Installing Cisco UCS Director PowerShell Agent

Note If you do not install the current version of PowerShell Agent for Cisco UCS Director on the Windows machine, some tasks or options on the **PowerShell Agents** tab are not available.

Before you begin

- You need system administrator privileges to complete this task.
- Enable WinRM.
- Configure Firewall.

Procedure

Step 1 If necessary, copy the `PSASetup.exe` file that you downloaded from Cisco UCS Director to your target Windows machine.

Step 2 Double-click the **PSASetup.exe** file.

Step 3 In the **Cisco PSA Service - InstallShield Wizard** screen, click **Next**.

Step 4 In the **Ready to install the Program** screen, click **Install**.

The **Installing Cisco PSA Service** screen displays during the installation. When the installation is complete, the **InstallShield Wizard Completed** message is displayed.

Step 5 Click **Finish**.

The PowerShell Agent is installed to the `C:\Program Files (x86)\Cisco Systems\Cisco PSA Service` folder. This folder is referred to as `%AGENT_INSTALL_FOLDER%` in the remainder of the document.

Step 6 Verify that the Cisco PSA Service is running on the Windows machine by checking the Resource Monitor.

Upgrading Cisco UCS Director SDKs

Upgrading Cisco UCS Director Open Automation to Release 6.5

The following procedure assumes that you are using an Eclipse development environment. If you use a different development environment for your Open Automation projects, perform the appropriate steps for that environment.

Procedure

Step 1 Download the Cisco UCS Director SDK Bundle, Release 6.5 from Cisco.com.

Step 2 Import the project into Eclipse.

Step 3 Execute the examples available to understand the Open Automation execution. The examples are located at `com.cisco.cuic.api.examples`.

Upgrading Cisco UCS Director REST API to Release 6.5

The following procedure assumes that you are using an Eclipse development environment. If you use a different development environment for your REST API projects, perform the appropriate steps for that environment.

Procedure

Step 1 Download the Cisco UCS Director SDK Bundle, Release 6.5 from Cisco.com.

Step 2 Import the project into Eclipse.

Step 3 Execute the examples available to understand the REST API execution. You can download the OA zip file from the CCO link, unzip the file, and import the OA examples into eclipse.

Upgrading Custom Tasks

Custom Task Script Analyzer

The Custom Task Script Analyzer analyses all the classes and methods in the CloupiaScripts that are embedded in a custom task, and provides complete signatures for the methods being used in the CloupiaScript. The analyzer evaluates all the custom scripts in the Cisco UCS Director database without executing any tasks, and then it outputs an analysis report.

The analysis report includes the custom task status (for example, Executed or Not executed), a list of methods used in the custom task, and a list of methods that are not compatible with the methods of the current version. You can use the analysis file to detect potential incompatibilities in the CloupiaScripts before you upgrade.

Configuring the Custom Task Script Analyzer

The Custom Task Script Analyzer is included with Cisco UCS Director as a zipped tar file named `script-analyzer.tgz`.

Procedure

Step 1 Download the `script-analyzer.tgz` tar file from the Cisco software download area.

Step 2 Copy the `script-analyzer.tgz` tar file to the `/opt` directory.

Note If you chose to copy the tar file to any directory other than `/opt`, ensure that you create the folders for saving the tar file and generated report under the same directory.

Step 3 Create a folder (for example, `csatool`) under the `/opt` directory.

Step 4 Untar the `script-analyzer.tgz` tar file into the `csatool` folder using the following command:

```
[root@localhost opt]# tar -zxvf script-analyzer.tgz -C csatool
```

The following files are unpacked into the `csatool` folder:

- `data` folder—This folder contains the API definition file in the JSON format. The Custom Task Script Analyzer uses this file to identify the methods that are not compatible with the methods of the current version.
- `jre1.8.0_121` folder
- `lib` folder
- `analyzer_config.properties` file
- `run-analyzer.sh` file
- `script-analyzer.jar` file

Step 5 Edit the `analyzer_config.properties` file and configure the following properties:

```
# Path for the inframgr.jar file
inframgrJarPath=/opt/infra/inframgr/inframgr.jar
# Path for the lib directory where all dependencies could be found.
# From Cisco UCS Director release 6.5,the libDirPath is /opt/infra/lib.
# For releases prior to 6.5, the libDirPath is /opt/infra/inframgr.
libDirPath=/opt/infra/inframgr
# Path for the API definition file in the JSON format which is available in the data folder.
# For releases prior to 6.5, the inframgr_6500.json file is the API definition file.
# For the release 6.5.0.2, the inframgr_6502.json file is the API definition file.
inframgrJSONDefinitionPath=data/inframgr_6502.json
# Directory where the generated analysis report would be written
reportDirPath=output
# Directory for the JavaScript files. The JavaScript files containing the
CloupiaScripts are fetched using the --fetch-scripts command.
jsFileOrDirPath=javascripts
# JDBC connection URL
db.url=jdbc:mysql://localhost:3306/db_private_admin?verifyServerCertificate=false&useSSL=true
# Database user
db.username=root
# For releases prior to 6.5, use the default database password cloupia.
# For Cisco UCS Director release 6.5, use the reset MySql password.
# You have to reset the database password in Cisco UCS Director Shell as a shell admin,
after bringing up all the services and first successful login to Cisco UCS Director.
db.password=cloupia
# JDBC driver
db.driver=com.mysql.jdbc.Driver
```

Note This is supported only for version prior to Cisco UCS Director, Release 6.5.0.2.

Note To run the analyzer on a Primary Node on a Multi Node Environment, edit the analyzer_config.properties file and configure the following :

JDBC connection URL

db.url=jdbc:mysql://<ip address of the inventory node>:3306/db_private_admin

Step 6 Save and close the `analyzer_config.properties` file.

Analyzing Custom Tasks with the Custom Task Script Analyzer

You can connect to Cisco UCS Director through a terminal and then run the Custom Task Script Analyzer from the terminal. To view the commands that are available to run the Custom Task Script Analyzer, run the following command:

```
[root@localhost csatool]# ./run-analyzer.sh --help
```

The following commands are available:

- fetch-scripts—Fetches scripts from the database. By default, this option is set to True.
- file—Specify the path of the JavaScript file to be processed.
- help—Displays the command line menu options.

Procedure

Step 1 Open a terminal and connect to Cisco UCS Director.

Step 2 To generate an analysis report for all custom tasks, execute the Custom Task Script Analyzer with the `--fetch-scripts` command as follows:

```
[root@localhost csatool]# ./run-analyzer.sh --fetch-scripts
```

On execution of this command, you will get:

- JavaScript files for all CloupiaScripts in your custom tasks and any tasks that were created with the Execute Cloupia Script library task. The JavaScript files are saved along with the corresponding byte code text files in the `javascripts` folder identified in the jsFileOrDirPath key of the `analyzer_config.properties` file.
- The analysis report in the `output` folder identified in the reportDirPath key of the `analyzer_config.properties` file.

By default, these folders are created in `/opt/csatool/`, or whichever path you configured in the `analyzer_config.properties` file.

Note The `javascripts` and the reports within the `output` folder are suffixed with the time stamp if:

- The `--fetch-scripts` command is executed more than once.
- The `javascripts` and `output` folders already exist in the `csatool` folder and the folders are not empty.

Step 3 To generate an anlaysis report for all JavaScript files in the `javascripts` folder, execute the Custom Task Script Analyzer with the **--file** command as follows:

```
[root@localhost csatool]# ./run-analyzer.sh --file javascripts
```

This command generates an analysis report for all JavaScripts in the `javascripts` folder and saves the analysis report in the output folder as configured in the `analyzer_config.properties` file.

Step 4 To generate an anlaysis report for a JavaScript file in the `javascripts` folder, execute the Custom Task Script Analyzer with the **--file** command as follows:

```
[root@localhost csatool]# ./run-analyzer.sh --file javascripts/Change_VM_Max_Boot_Wait_Time.js
```

Where, the Change_VM_Max_Boot_Wait_Time.js is a javascript file in the `javascripts` folder. This command generates an analysis report for the Change_VM_Max_Boot_Wait_Time.js in the `javascripts` folder and saves the analysis report in the output folder as configured in the `analyzer_config.properties` file.

The analysis report includes the following details:

- taskLabel—Name of the custom task that was analyzed by the Custom Task Script Analyzer.
- workflowList—List of workflows in which the custom task is used.
- status—Executed or Not executed. If any of the workflows in the workflowList was executed at least once, the status is displayed as Executed.

- usedMethodsList—List of methods that are used in the custom task.
- incompatibleMethodsList—List of methods that are not compatible with the methods of the current version.

The following is a sample analysis report:

```
{
    "taskLabel": "Change_VM_Max_Boot_Wait_Time",
    "workflowList": [
      "Provision_VM",
      "UpdateVM"
    ],
    "status": NotExecuted,
    "usedMethodsList": [
      "public static com.cloupia.service.cIM.inframgr.profiles.PrivateCloudSystemProfile
com.cloupia.service.cIM.inframgr.InfraPersistenceUtil.getPrivateCloudSystemProfile(java.lang.String)
 throws java.lang.Exception",
      "public int
com.cloupia.service.cIM.inframgr.profiles.PrivateCloudSystemProfile.getLinuxVMMaxBootTime()",

      "public void
com.cloupia.service.cIM.inframgr.profiles.PrivateCloudSystemProfile.setWindowsVMMaxBootTime(int)",

      "public static boolean
com.cloupia.service.cIM.inframgr.InfraPersistenceUtil.modifyPrivateCloudSystemProfile
(com.cloupia.service.cIM.inframgr.profiles.PrivateCloudSystemProfile) throws
java.lang.Exception",
      "public void
com.cloupia.service.cIM.inframgr.profiles.PrivateCloudSystemProfile.setLinuxVMMaxBootTime(int)"

    ],
    "incompatibleMethodsList": [
      "public static com.cloupia.service.cIM.inframgr.profiles.PrivateCloudSystemProfile
com.cloupia.service.cIM.inframgr.InfraPersistenceUtil.getPrivateCloudSystemProfile(java.lang.String)
 throws java.lang.Exception",
      "public void
com.cloupia.service.cIM.inframgr.profiles.PrivateCloudSystemProfile.setWindowsVMMaxBootTime(int)"

    ]
  }
```