Cisco UCS Director Upgrade Guide, Release 6.7

First Published: 2019-01-09

Last Modified: 2020-03-09

Upgrading Cisco UCS Director to Release 6.7

Overview of the Upgrade to Cisco UCS Director, Release 6.7(x.x)

Important Cisco UCS Director Release 6.7, Release 6.7(1.0), and Release 6.7(2.0) are no longer available for download. It is recommended that you upgrade immediately to release 6.7(3.0).

The upgrade process to Cisco UCS Director, Release 6.7(x.x) depends on the current version of the software that is installed on your system. For information on supported upgrade paths, see Supported Upgrade Paths to Cisco UCS Director, Release 6.7(3.0), on page 1.

Cisco UCS Director, Release 6.7 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 Cisco UCS Director database. See Prerequisites for Upgrading to Cisco UCS Director, Release 6.7, on page 5.

Supported Upgrade Paths to Cisco UCS Director, Release 6.7(3.0)

The following are the supported upgrade paths for Cisco UCS Director, Release 6.7(3.0).

Important Cisco UCS Director Release 6.7, Release 6.7(1.0), and Release 6.7(2.0) are no longer available for download. It is recommended that you upgrade immediately to release 6.7(3.0).

Upgrade Paths from Release 6.7(x.x)

- From Release 6.7(2.0) to Release 6.7(3.0)
- From Release 6.7(1.0) to Release 6.7(3.0)
- From Release 6.7 to Release 6.7(3.0)

Upgrade Paths from Release 6.6(x.x)

- From Release 6.6(2.0) to Release 6.7(3.0)
- From Release 6.6(1.0) to Release 6.7(3.0)
- From Release 6.6 to Release 6.7(3.0)

Upgrading from Versions Prior to Release 6.6

If you have a version prior to Release 6.6(0.0) installed, you cannot upgrade directly to Release 6.7(3.0). You must first upgrade to Release 6.6(0.0) or Release 6.6(1.0) and then upgrade to Release 6.7(3.0).

With release 6.7(x.x), the multi-node configuration in Cisco UCS Director was modified to support only one database node and one primary node. So when you upgrade from release 6.6 to release 6.7(3.0), the upgrade process will make the following changes in your environment:

- Migrates existing data from the inventory database node to the monitoring database node, and converts the monitoring database node to the database node.
- Upgrades the primary node to the current release.

For more information, see the *Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 6.7*.

Supported Upgrade Paths to Cisco UCS Director, Release 6.7(4.0)

Following are the supported upgrade paths for Cisco UCS Director, Release 6.7(4.0):

Upgrade Paths from Release 6.7(x.x)

- From Release 6.7(3.0) to Release 6.7(4.0)
- From Cisco UCS Director Connector Packs version 6.7(3.2) to Release 6.7(4.0)
- From Cisco UCS Director Connector Packs version 6.7(3.1) to Connector Packs version 6.7(3.2) to Release 6.7(4.0)

Upgrade Paths from Release 6.6(x.x)

- From Release 6.6(2.0) to Release 6.7(3.0) to Release 6.7(4.0)
- From Release 6.6(1.0) to Release 6.7(3.0) to Release 6.7(4.0)
- From Release 6.6 to Release 6.7(3.0) to Release 6.7(4.0)

Upgrading from Versions Prior to Release 6.6

If you have a version prior to Release 6.6(0.0) installed, you cannot upgrade directly to Release 6.7(4.0). You must first upgrade to Release 6.6(0.0) or Release 6.6(1.0), then upgrade to Release 6.7(3.0) and finally upgrade to Release 6.7(4.0).

With release 6.7(x.x), the multi-node configuration in Cisco UCS Director was modified to support only one database node and one primary node. So when you upgrade from release 6.6 to release 6.7(3.0), the upgrade process will make the following changes in your environment:

- Migrates existing data from the inventory database node to the monitoring database node, and converts the monitoring database node to the database node.
- Upgrades the primary node to the current release.

For more information, see the *Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 6.7*.

Supported Upgrade Paths for Bare Metal Agent Patch Release 6.7(4.0)

The following are the supported upgrade paths for the Bare Metal Agent Patch Release 6.7(4.0):

- From Release 6.7(2.0) to Patch Release 6.7(4.0)
- From Release 6.7(3.1) to Patch Release 6.7(4.0)

Note To apply a Bare Metal Agent 6.7(4.0) patch, you must only choose **Apply Patch** option in the shelladmin.

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 6.7, 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 4.

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
- 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_6_0_0_66365_VMWARE_GA.zip`, `CUCSD_6_6_0_0_66717_HYPERV_GA.zip`, or `cucsd_patch_6_6_0_0_66365.zip`
- Certificate file, for example `UUCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`
- Digital signature generated for the image, for example `CUCSD_6_6_0_0_66365_VMWARE_GA.zip.signature`, `CUCSD_6_6_0_0_66717_HYPERV_GA.zip.signature`, or `cucsd_patch_6_6_0_0_66365.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 from the directory where you have unzipped the downloaded content.

Example: Signature Verification for Upgrade Patch

```
python ./cisco_x509_verify_release.py -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i cucsd_patch_6_6_0_0_66365.zip -s cucsd_patch_6_6_0_0_66365.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_6_0_0_66365_VMWARE_GA.zip -s CUCSD_6_6_0_0_66365_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_6_0_0_66717_HYPERV_GA.zip -s CUCSD_6_6_0_0_66717_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_6_0_0_66365.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_6_0_0_66365_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_6_0_0_66717_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 6.7

Complete the following prerequisites before you upgrade your current Cisco UCS Director software to Release 6.7.

Plan a Maintenance Window

The upgrade to Release 6.7 requires that you stop all Cisco UCS Director services during the upgrade. We recommend that you plan a maintenance window of between 2 and 6 hours. Prior to upgrade, the length of the maintenance window depends on the size of your database

Download Cisco UCS Director, Release 6.7 and Verify the Signed Image

Download the Cisco UCS Director, Release 6.7 software patch from http://www.cisco.com and then verify the digitally signed image. See Digitally Signed Images, on page 3.

Place the Verified Release 6.7 Software Patch on a Server

Place the Release 6.7 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 14.

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.

Upgrading a Single Node Setup to Release 6.7

Before you begin

Complete all prerequisites in Prerequisites for Upgrading to Cisco UCS Director, Release 6.7, on page 5.

Procedure

Step 1 Log in to the Cisco UCS Director ShellAdmin.

Step 2 To upgrade Cisco UCS Director to Release 6.7, choose `Apply Signed Patch`.

Step 3 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 4 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 5 At the `Specify the Transfer mode` prompt, enter one of the following:

- HTTP—Enter the URL for the location where you stored the upgrade file.
- 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.
- FILE—Enter the path to the local directory 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, if you stored the patch file on an FTP server, enter **ftp:**//*username*:*password*@*hostname*|*IP_address*/*software_location_and_name*

Step 6 Wait for the patch file to download to the Cisco UCS Director VM.

Step 7 Wait for the patch upgrade to complete.

The upgrade process performs extra steps including the following:

- Unpacks the patch file.
- Installs the Release 6.7 files
- 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 8 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 6.7

Upgrading Your Multi-Node Setup

Following is a summary of the process that you must follow to upgrade your current multi-node setup to the optimized multi-node setup introduced in Release 6.7:

1. We recommend that you take snapshots of the VMs in the primary node, the inventory database node and monitoring database node.
2. Stop all services on the primary and service nodes.
3. Ensure that disk-1 has sufficient space in both database nodes for migrating data from the inventory database node. If there is not enough disk space, use the `Clean-up patch files` option in the Shell Admin console to create disk space in disk-1.
4. Upgrade the monitoring database node to the current version of Cisco UCS Director and run the database migration script.

   For more information, see Upgrading the Monitoring Node to Release 6.7 , on page 8
5. Upgrade the primary node to the Cisco UCS Director release 6.7.

   For more information, see Upgrading the Primary Node, on page 9
6. Power off the inventory database node and the service nodes.

Note The time taken to upgrade your current multi-node configuration to the optimized multi-node configuration depends on the database size.

Upgrading the Monitoring Node to Release 6.7

When you upgrade the current monitoring node to release 6.7, the inventory and monitoring databases are merged, and the monitoring database node is converted to the new database node.

Before you begin

1. We recommend that you take snapshots of the VMs in the primary node, the inventory database node and monitoring database node.
2. Enable root access on the monitoring database node and the inventory database node.
3. Ensure that the available disk size on the monitoring database node is equal to or more than the combined disk size of the inventory database node and monitoring database node.

Procedure

Step 1 Login to the monitoring database node.

Step 2 From the Shell Admin console, choose `Apply Signed Patch` to upgrade the node to Release 6.7.

Step 3 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 4 At the `Specify the Transfer mode` prompt, enter one of the following:

- HTTP—Enter the URL for the location where you stored the upgrade file.
- 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.
- FILE—Enter the path to the local directory 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, if you stored the patch file on an FTP server, enter **ftp://***username*:*password*@*hostname*|*IP_address*/*software_location_and_name*

Step 5 When prompted for the `Patch URL`, type the location of the Release 6.7 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 6 Wait for the patch to download to the Cisco UCS Director VM.

Step 7 Wait for the patch upgrade to complete.

The upgrade process performs many steps including the following:

- Unpacks the patch file.
- Installs the Release 6.7 files
- Initializes the database schema.
- Reboots the Cisco UCS Director appliance. The Cisco UCS Director services start automatically.

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

Step 8 Log in as root.

Step 9 Navigate to the migration folder with the following command:

```
cd /opt/scalability/migration
```

Step 10 Run the `upgradeMultiNodeDB.sh` script.

Step 11 When prompted, enter **y** to confirm that you have taken a snapshot of the existing multi-node setup

Step 12 When prompted, enter **y** to confirm converting the monitoring database node to the database node.

Step 13 When prompted, enter the IP address of the inventory database node.

Step 14 When prompted, enter the root password for the inventory database node.

At this point, the process to migrate data from the inventory database node to the monitoring database node and to convert the monitoring database node into the database node is initiated.

Step 15 Wait for the `upgradeMultiNodeDB.sh` script to execute completely.

After the script executes completely, do not power off the inventory database node. This node must be powered on and running to upgrade the primary node successfully.

What to do next

Upgrade the primary node.

Upgrading the Primary Node

Before you begin

- Take a snapshot of the VM in the primary node.
- Upgrade the monitoring database node. See Upgrading the Monitoring Node to Release 6.7 , on page 8.
- Ensure that the monitoring database node and the inventory database node is powered on.

Procedure

Step 1 Login to the primary node.

Step 2 From the Shell Admin console, choose `Apply Signed Patch` to upgrade the node to Release 6.7.

Step 3 When prompted, enter y to stop the services on the primary node.

Step 4 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 5 At the `Specify the Transfer mode` prompt, enter one of the following:

- HTTP—Enter the URL for the location where you stored the upgrade file.
- 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.
- FILE—Enter the path to the local directory 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, if you stored the patch file on an FTP server, enter **ftp://***username*:*password@hostname*|*IP_address*/*software_location_and_name*

Step 6 When prompted for the `Patch URL`, type the location of the Release 6.7 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 7 Wait for the patch to download to the Cisco UCS Director VM.

Step 8 Wait for the patch upgrade to complete.

The upgrade process includes the following steps:

- Unpacks the patch file.
- Verifies that the database node upgrade is complete. If the database node upgrade is incomplete, the upgrade process is cancelled.
- Installs the Release 6.7 files
- Upgrades the primary node.
- Initializes the database schema.
- Reboots the Cisco UCS Director appliance. The Cisco UCS Director services start automatically.

Upgrading Optimized Multi-Node Setup to Release 6.7(3.0) or Later Versions

Before you begin

Login to the primary node and from the Shell Admin console, choose **Stop Services** to halt all services running on the primary node.

Procedure

Step 1 Login to the database node.

Step 2 From the Shell Admin console, choose **Apply Signed Patch** to upgrade the node to Release 6.7(3.0) or the later version.

Step 3 Login to the primary node, and from the Shell Admin console, choose **Apply Signed Patch** to upgrade the node to Release 6.7(3.0) or the later version.

Step 4 Choose **Start Services** to start all the services on the primary node.

Upgrading Cisco UCS Director Baremetal Agent

Upgrading from Bare Metal Agent Release 6.6 to Release 6.7

Before you begin

Upgrade Cisco UCS Director to Release 6.7.

Note You cannot upgrade the Bare Metal Agent to Release 6.7 directly from a release earlier than 6.6. To upgrade an earlier release to 6.7, first upgrade the earlier Release to 6.6 as described in the Release 6.6 Upgrade Guide, then follow these instructions to upgrade to Release 6.7.

Procedure

Step 1 Download the Bare Metal Agent, Release 6.7 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 root credentials for your system.

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__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 Log in to Cisco UCS Director, Release 6.7, and choose **Administration** > **Physical Accounts** > **Bare Metal Agents**.

Step 13 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 14 Confirm that the Bare Metal Agent account is reachable from Cisco UCS Director and then stop and start the services for that account.

Upgrading Bare Metal Agent to Release 6.7 from Release 6.6(1.0)

Before you begin

Upgrade Cisco UCS Director to Release 6.7.

- Upgrade Cisco UCS Director to Release 6.7
- Delete the `patch` folder from the `/tmp` directory, if available

Procedure

Step 1 Download the Bare Metal Agent, Release 6.7 patch to the existing Bare Metal Agent VM.

Step 2 Log on to the Bare Metal Agent VM using SSH client as 'shelladmin' user.

Step 3 Choose **`Apply Signed Patch`** to apply the signed patch. For more information about how to apply signed patch, see the Cisco UCS Director Shell Guide.

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 get the **Error 1001** error message while uninstalling the PowerShell agent, delete the PSA registry folders.

To delete the PSA registry folders, do the following:

1. Open the Windows Registry Editor (**Start > Run> regedit.exe**).
2. In the left pane of the Registry Editor, right-click and choose **Find**.
3. In the **Find What** field, enter **`PSAServiceNew`** and click **Find Next** to view the PSA registry folders.
4. Right-click and choose **Delete** to delete the PSA registry folders.

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 6.7

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 6.7 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 6.7

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 6.7 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 analysis 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 analysis 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)"

    ]
  }
```