Pre-upgrade Tasks

- Pre-Upgrade Task Flow, page 1

Pre-Upgrade Task Flow

Procedure

	Command or Action	Purpose
Step 1	Read the release notes for the new release: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html	Ensure that you understand the new features and how the upgrade interacts with the other products that are associated with your system.
Step 2	Familiarize yourself with the requirements and limitations of this release: Requirements and Limitations	Ensure that your system meets all requirements, including network requirements, platform requirements, and software requirements.
Step 3	Ensure that the software version you are upgrading from is running on a virtual machine. If your current deployment is running on MCS hardware, see the *Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for information about how to migrate an existing cluster to a virtualized cluster.	You cannot install or run Cisco Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines.
Step 4	Export User Records, on page 3	Export user records using the Bulk Administration Tool (BAT).
Step 5	Check the Available Common Partition Space, on page 4	Verify that you have enough common partition space for the upgrade. Typically, you need at least 25G of common partition space; however, your

	Command or Action	Purpose
		deployment may require more space if you have a lot of TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed.
Step 6	If you do not have enough common partition space, perform one or more of the following procedures: • Adjust High and Low Watermarks, on page 4 • Create Additional Partition Space, on page 5	**Caution** Performing an upgrade without sufficient disk space can cause the system to fail.
Step 7	Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain.	Perform this step for refresh upgrades on IM and Presence Service nodes only. Expired certificates are not imported during a refresh upgrade. As a result, a new certificate is generated during upgrade process and can cause errors.
Step 8	Obtain Upgrade Files, on page 6	Download the upgrade files for the Cisco Unified Communications Manager and the IM and Presence Service. For refresh upgrades, you must also download the upgrade COP files.
Step 9	Ensure that you have the necessary license files for the new release.	Use the Cisco Prime License Manager to allocate and monitor the licenses for Cisco Unified Communications Manager, its applications and endpoints. See the *Cisco Prime License Manager User Guide* at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-license-manager/products-user-guide-list.htmlfor information about generating and installing licenses. **Note** Apply all pre-9.0 licenses to Cisco Unified Communications Manager before you upgrade to Release 9.0 or later software. After you upgrade to Release 9.0 or later software, you cannot apply these licenses to Cisco Unified Communications Manager and you cannot apply them using the Cisco Prime License Manager. Ensure that you install all unused licenses or Product Authorization Keys (PAKs) before you upgrade the system. The Cisco Unified Communications Manager displays a warning to prompt you to install any unused licenses before proceeding.

	Command or Action	Purpose
Step 10	Back Up the System, on page 7	Create a backup file in case you need to restore your existing system.
Step 11	Increase the Database Replication Timeout, on page 8	Optional. This procedure applies to Cisco Unified Communications Manager nodes only. Use this procedure when you upgrade large clusters. If you increase the database replication timeout, you must restore the timeout to the default value after the entire cluster upgrades and the Cisco Unified Communications Manager subscriber nodes have successfully set up replication.
Step 12	Verify IPv6 Networking, on page 8	This procedure applies to Cisco Unified Communications Manager nodes only. Verify IPv6 networking on the first node (Cisco Unified Communications Manager database publisher node) and Cisco Unified Communications Manager subscriber nodes. If IPv6 is configured incorrectly on the Cisco Unified Communications Manager subscriber nodes, load detection may take 20 minutes.
Step 13	Disable High Availability on Presence Redundancy Groups, on page 9	This procedure applies to IM and Presence Service nodes only. If you have configured presence redundancy groups for high availability, you must disable it during the upgrade process.
Step 14	Check Connectivity, on page 9	Verify that the IM and Presence Service node has connectivity with Cisco Unified Communications Manager.
Step 15	Stop the IM and Presence Sync Agent, on page 10	If you need to upgrade Cisco Unified Communications Manager as part of your IM and Presence upgrade, you must stop the IM and Presence Sync Agent service before you begin the upgrade process.
Step 16	Add a Serial Port to the Virtual Machine, on page 10	Add a serial port to the virtual machine so that you can dump logs in the event of an upgrade failure. Perform this procedure for all nodes.

Export User Records

Export user records using the Bulk Administration Tool (BAT).

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Export Users**.

Step 2 Click **Find** to display all user records.

Step 3 Click **Next**.

Step 4 Enter a filename in the in the **File Name** text box and choose file format from the **File Format** drop-down list.

Step 5 In the **Job Information** area, enter the Job description.

Step 6 Click **Run Immediately** to export user records immediately

Step 7 Click **Submit**.

Step 8 To download the exported file, choose **Bulk Administration** > **Upload/Download Files**.

Step 9 Enter search criteria for the file that you generated and click **Find**.

Step 10 Select the check box that corresponds to the file that you want to download and click **Download Selected**.

Step 11 In the File Download pop-up window, click **Save**.

Step 12 In the Save As pop-up window, choose the location where you want to save the file and click **Save**. Ensure that you copy the file off of the server and save it to a remote PC or device.

Check the Available Common Partition Space

Use the Real-Time Monitoring Tool (RTMT) to verify that you have enough common partition space for the upgrade.

Procedure

Step 1 In the Real-Time Monitoring Tool, select **Disk Usage** from the list of **System** counters on the left navigation pane.
A page displays detailed information about disk usage.

Step 2 View the tables on the bottom of the page and compare the **Total Space** to the **Used Space** for the common partition. You need a minimum 25G of available common partition space before you begin an upgrade.

Adjust High and Low Watermarks

Use this procedure to adjust the low and high watermarks to reduce the traces and remove unnecessary log files. After the upgrade, you must restore the high and low watermarks to their original values in order to avoid premature purging of traces. The default value for the high watermark is 85. The default value for the low watermark is 80.

Procedure

Step 1 In the Real Time Monitoring Tool (RTMT) interface, double-click **Alert Central** in the left navigation pane.
Step 2 On the **System** tab, right-click **LogPartitionLowWaterMarkExceeded** and select **Set Alert/Properties**.
Step 3 Select **Next**.
Step 4 Adjust the slider value to 30.
Step 5 On the **System** tab, right-click **LogPartitionHighWaterMarkExceeded** and select **Set Alert/Properties**.
Step 6 Select **Next**.
Step 7 Adjust the slider value to 40.

Create Additional Partition Space

To create additional space in the common partition, you can perform one or more of the steps in this procedure. To download the COP files and the Readme files listed in this procedure, go to https://software.cisco.com and navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > **<*Version*>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Procedure

Step 1 Manually remove outdated or unused firmware files from the TFTP directory using one of the following options:

- From the Cisco Unified OS Administration interface, select **Software Upgrades** > **TFTP File Management** and delete any unnecessary files.
- From the command line interface, use the `file list tftp` and `file delete tftp` commands delete any unnecessary files.

Step 2 Use the Free Common Space COP file (ciscocm.free_common_space_v<latest_version>.cop.sgn). This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before you proceed.

Note You will not be able to switch back to the inactive version after installing this file.

Step 3 If you are upgrading from release 9.x and earlier, use the Disk Expansion COP file (ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) to expand the vDisk size if your virtual environment has additional available disk space.
Ensure that you review the Readme file that supports this COP file before you proceed.

Obtain Upgrade Files

You must download the upgrade file for the new release, as well as any upgrade Cisco Option Package (COP) files that are required. Upgrade COP files are required for refresh upgrades only. The tables below lists the upgrade paths that require COP files.

Table 1: Cisco Cisco Unified Communications Manager Upgrade Paths, Release 11.5(1)

From	To	Upgrade Type
8.6(x) installed on a virtual machine	11.5(1)	Refresh upgrade. Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • ciscocm.version3-keys.cop.sgn
9.1(x) installed on a virtual machine	11.5(1)	Refresh upgrade. Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • ciscocm.version3-keys.cop.sgn
10.5(x) installed on a virtual machine	11.5(1)	Standard upgrade
11.0(1) installed on a virtual machine	11.5(1)	Standard upgrade

Table 2: Upgrade Paths from Cisco Unified Presence Releases

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.6(x) installed on a virtual machine	11.5(1)	Refresh upgrade. Requires the following COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

Table 3: Upgrade Paths from IM and Presence Service Releases

From IM and Presence Release	To IM and Presence Release	Upgrade Type
9.1(x) installed on a virtual machine	11.5(1)	Refresh upgrade. Requires the following COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

From IM and Presence Release	To IM and Presence Release	Upgrade Type
10.5(x) installed on a virtual machine	11.5(1)	Standard upgrade
11.0(1) installed on a virtual machine	11.5(1)	Standard upgrade

Procedure

Step 1 Download the upgrade files for the applications from Cisco.com. The software is available in export restricted and export unrestricted versions, so be sure to confirm that you select the correct file.

- To download the Cisco Unified Communications Manager upgrade file, go to https://software.cisco.com and navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > ***<Version>*** > **Unified Communications Manager/CallManager/Cisco Unity Connection Updates**.
- To download the IM and Presence Service upgrade file, go to https://software.cisco.com and navigate to **Unified Communications** > **Unified Communications Applications** > **Presence Software** > **Unified Communications Manager IM and Presence Service** > ***<Version>*** > **Unified Presence Service (CUP) Updates**.

Step 2 Go to https://software.cisco.com and navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > ***<Version>*** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities** to download the following COP files:

- ciscocm.refresh_upgrade_<latest_version>.cop.sgn
- ciscocm.version3-keys.cop.sgn

Step 3 Go to https://software.cisco.com and navigate to **Unified Communications** > **Unified Communications Applications** > **Presence Software** > **Unified Communications Manager IM and Presence Service** > ***<Version>*** > **Unified Presence Service (CUP) Updates** and select **UTILS** to download the following COP file:

- cisco.com.cup.refresh_upgrade_v<latest_version>.cop

Back Up the System

Before You Begin

- Ensure that you use a network device as the storage location for the backup files. Virtualized deployments of Unified Communications Manager do not support the use of tape drives to store backup files.

- Ensure that all cluster nodes have the same installed version of Cisco Unified Communications Manager or IM and Presence Service.
- The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.
- Make sure that you have a record of the cluster security password. If the cluster security password changes after you complete this backup, you will need to know the password or you will not be able to use the backup file to restore your system.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.

Step 3 Choose a feature from the **Select Features** area.

Step 4 Click **Start Backup.**

Increase the Database Replication Timeout

This procedure applies to Cisco Unified Communications Manager nodes only.

Increase the database replication timeout value when you upgrade large clusters so that more Cisco Unified Communications Manager subscriber nodes have sufficient time to request replication. When the timer expires, the first Cisco Unified Communications Manager subscriber node, plus all other Cisco Unified Communications Manager subscriber nodes that requested replication within that time period, begin a batch data replication with the Cisco Unified Communications Manager database publisher node.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your ssh *adminname@hostname* and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **utils dbreplication setrepltimeout***timeout* command, where *timeout* is database replication timeout, in seconds. Ensure that the value is between 300 and 3600.
The default database replication timeout value is 300 (5 minutes).

Verify IPv6 Networking

This procedure applies to Cisco Unified Communications Manager nodes only.

Verify that IPv6 networking on the first node (Cisco Unified Communications Manager database publisher node) and Cisco Unified Communications Manager subscriber nodes. If IPv6 is configured incorrectly on the Cisco Unified Communications Manager subscriber nodes, load detection may take 20 minutes.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your ssh *adminname@hostname* and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the following command:**utils network ipv6 ping***destination [count]*

- *destination* is a valid IPv6 address or host name that you want to ping
- *count* is the number of times to ping the external server. The default is 4.

Disable High Availability on Presence Redundancy Groups

This procedure applies to IM and Presence Service nodes only. Use it to disable high availability on the IM and Presence presence redundancy group.

Procedure

Step 1 From the Cisco Unified CM Administration user interface, choose **System** > **Presence Redundancy Groups**.

Step 2 Enter the presence redundancy group search parameters and then click **Find**.

Step 3 From the search results, select the presence redundancy group that you want to disable.

Step 4 On the Presence Redundancy Group Configuration window, uncheck the **Enable High Availability** check box.

Step 5 Click **Save**.

Check Connectivity

Verify that the IM and Presence Service node has connectivity with Cisco Unified Communications Manager.

Procedure

Step 1 From the Cisco Unified CM IM and Presence Administration interface, select **Diagnostics** > **System Troubleshooter** .

The system automatically runs a troubleshooting check.

Step 2 When the results of the troubleshooting check are loaded, verify that all of the **Sync Agent Troubleshooter** tests have a green checkmark in the **Outcome** column to indicate that the test was passed.

Step 3 If any of the **Sync Agent Troubleshooter** tests are failed, use the information in the **Problem** and **Solution** columns to resolve the issue before continuing with the upgrade process.

Stop the IM and Presence Sync Agent

If you need to upgrade Cisco Unified Communications Manager as part of your IM and Presence upgrade, you must stop the IM and Presence Sync Agent service before you begin the upgrade process.

Procedure

Step 1 From the Cisco Unified Serviceability interface, select **Tools** > **Control Center - Network Services**.

Step 2 Select an IM and Presence Service node from the **Server** drop-down list and click **Go**.

Step 3 In the **IM and Presence Services** section, select the **Cisco Sync Agent** and click **Stop**.

Add a Serial Port to the Virtual Machine

Add a serial port to the virtual machine so that you can dump logs in the event of an upgrade failure.

Procedure

Step 1 Power off the virtual machine.

Step 2 Edit the settings to add a serial port. For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

Step 3 Attach the serial port to a .tmp file.

Step 4 Power on the virtual machine and proceed with the upgrade.

What to Do Next

After you successfully upgrade the system, follow the procedure to Remove the Serial Port. In the event of an upgrade failure, refer to Dump a Log File After an Upgrade Failure.