Pre-upgrade Tasks

- Pre-Upgrade Task Flow, page 1

Pre-Upgrade Task Flow

Complete the following tasks before you begin an upgrade or migration.

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. Do this step for all upgrade and migration methods.
Step 2	Check 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. Do this step for all upgrade and migration methods.
Step 3	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. Do this step for all upgrade and migration methods.

	Command or Action	Purpose
Step 4	Check the health of your network: • Read Factors that Affect Upgrade Time Requirements and ensure that your system meets the conditions described in that section. • Generate a Database Status Report, on page 6 • Check Database Replication, on page 6 • Check Performance Reports, on page 7 • Run CLI Diagnostics, on page 8	The health of your system affects the amount of time that an upgrade requires. You can reduce the amount of time needed for an upgrade by ensuring that your system meets the conditions described in these sections. Do this step for all upgrade and migration methods.
Step 5	Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. If there are expired certificates, perform one or more of the following procedures: • Delete a Trust Certificate, on page 8 • Regenerate a Certificate, on page 9 if an identify certificate is expired	Perform this step for refresh upgrades on Cisco Unified Communications Manager and 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 6	Take a Fresh Backup, on page 10	You must create a fresh backup file in case you need to restore your existing system. Do this step for all upgrade and migration methods. **Caution** You may lose data or you may be unable to restore your system if your backup is outdated.
Step 7	Back Up Custom Ringtones and Background Images, on page 11	If you have custom ringtones or background images in the TFTP directory, you need to create a separate backup for these files. They are not included in the Disaster Recovery System (DRS) backup file.
Step 8	Check Network Connectivity, on page 11	Use this procedure to verify connectivity between Cisco Unified Communications Manager nodes and services in your network, such as NTP, SMTP, and DNS.
Step 9	Verify IPv6 Networking, on page 12	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

	Command or Action	Purpose
		subscriber nodes, load detection may take 20 minutes. Do this step for all upgrade and migration methods.
Step 10	Check Connectivity between IM and Presence and Cisco Unified Communications Manager, on page 12	Verify that the IM and Presence Service node has connectivity with Cisco Unified Communications Manager. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 11	Collect Configuration and Login Information, on page 13	Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.
Step 12	Record the Registered Device Count, on page 13	Use the Real Time Monitoring Tool (RTMT) to capture the device count so that you can verify your endpoints and resources after the upgrade is complete. You can also use this information to verify that you have not exceeded the capacity of the virtual machine (VM) that you are deploying. Do this step for all upgrade and migration methods.
Step 13	Record the Number of Assigned Users, on page 14	Record the number of assigned users on IM and Presence Service nodes so that you can verify this information after the upgrade is complete. Do this step for all upgrade and migration methods.
Step 14	Record TFTP Parameters, on page 14	The upgrade process changes a TFTP parameter. Record the current setting so that you can reset the parameter after the upgrade is complete.
Step 15	Record Enterprise Parameters, on page 15	Record the settings for Enterprise Parameters on both Unified Communications Manager nodes and IM and Presence Service nodes. Some Enterprise Parameters exist on both types of nodes and the settings that are configured on Unified Communications Manager nodes may overwrite the settings configured on IM and Presence Service nodes during an upgrade. Record the settings so that you can restore them as needed after the upgrade is complete. Do this step for all upgrade and migration methods.
Step 16	Export User Records, on page 15	Export user records using the Bulk Administration Tool (BAT). Do this step for all upgrade and migration methods.

	Command or Action	Purpose
Step 17	Upgrade IP Phone Firmware, on page 16	You can upgrade your IP phones to the firmware that corresponds to the new release as a pre-upgrade task. Although IP phones automatically download their new firmware after an upgrade, you can choose to apply new firmware files to the endpoints in a controlled manner prior to the upgrade in order to minimize phone downtime after an upgrade. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 18	Verify Critical Services, on page 17	Verify that all critical services are activated.
Step 19	Deactivate Cisco Extension Mobility and TFTP Services, on page 17	Stop Cisco extension mobility and TFTP services on Cisco Unified Communications Manager nodes before you begin an upgrade. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 20	Stop the IM and Presence Sync Agent, on page 18	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. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 21	Check the Available Common Partition Space, on page 18	Verify that you have enough common partition space for the upgrade. Typically, you need at least 25G of common partition space; however, your 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. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 22	If you do not have enough common partition space, perform one or more of the following procedures: • Adjust High and Low Watermarks, on page 19 • Create Additional Partition Space, on page 19	Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade. **Caution** Performing an upgrade without sufficient disk space can cause the upgrade to fail.

	Command or Action	Purpose
Step 23	Obtain Upgrade Files, on page 20	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. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 24	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.html for information about generating and installing licenses. Do this step for all upgrade and migration methods. **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.
Step 25	Increase the Database Replication Timeout, on page 22	Optional. This procedure applies to the Cisco Unified Communications Manager publisher node 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. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 26	Disable High Availability on Presence Redundancy Groups, on page 22	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.

	Command or Action	Purpose
		Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 27	Add a Serial Port to the Virtual Machine, on page 23	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. Do this step for all upgrade and migration methods.

Generate a Database Status Report

Use Cisco Unified Reporting Tool (CURT) to generate a Database Status Report to verify that there are no network issues between cluster nodes. For example, verify that there are no issues with reachability or latency that affect database replication between nodes or that affect quality of service (QoS) for voice and video signaling.

Procedure

Step 1 Log in to the reporting interface for the node:

- For Unified Communications Manager nodes, log in to the Cisco Unified Reporting interface.
- For IM and Presence Service nodes, log in to the Cisco Unified IM and Presence Reporting interface.

Step 2 Select **System Reports**.

Step 3 Select the report for the node:

- To check database replication on a Unified Communications Manager node, select **Unified CM Database Status**.
- To check database replication on an IM and Presence Service node, select **IM and Presence Database Status**.

Step 4 Click the **Generate Report** (bar chart) icon in the **Reports** window.

Step 5 Click the **View Details** link to expose details for a section that does not automatically appear.

Step 6 If the report indicates that there are errors, select the **Report Descriptions** report and review the troubleshooting information and possible remedies.

Check Database Replication

Use this procedure to verify that the database replication is functioning correctly before you begin an upgrade.

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 status** command to check for errors or mismatches in the database tables.

Step 3 Execute the **utils dbreplication runtimestate** command to check if the database replication is active on the node.
The output lists all the nodes and if database replication is set up and in a good state, the **replication setup** value for each node is **2**.

If a value other than 2 is returned, you must resolve the errors before proceeding with the upgrade.

Check Performance Reports

Procedure

Step 1 From the Cisco Unified Serviceability interface, select **Tools** > **Serviceability Reports Archive**.

Step 2 Click on the link and choose the most recent report.

Step 3 Click the **CallActivitiesRep** to open the Call Activities Report in a new tab and verify that the number of **Calls Attempted** is not too high for the capacity of the virtual machine. You can determine the threshold for the number of **Calls Attempted** by checking the recommendations for your system in the *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* at http://www.cisco.com/goucsrnd.

Step 4 Return to the Cisco Unified Serviceability interface and click the **PerformanceRep** link for each node to view the Performance Protection Statistics Reports.

Step 5 In each Performance Protection Statistics Report, verify that your system does not exceed the cluster-wide or per-node limits that are specified for your deployment size.
For information about deployment sizing, see:

- *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* at http://www.cisco.com/goucsrnd.
- Collaboration Sizing Tool at http://tools.cisco.com/cucst. Partners can use this tool to evaluate a customer's configuration.

Run CLI Diagnostics

Use the command line interface (CLI) diagnostic commands to diagnose and solve network problems before you begin and upgrade.

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 diagnose test** command.
This command runs all diagnostic commands but does not attempt to fix problems. You can view a list of all the diagnostic commands by executing the **utils diagnose list** command.

Step 3 Execute the **utils diagnose fix** command to attempt to automatically fix system problems.

Delete a Trust Certificate

A trusted certificate is the only type of certificate that you can delete. You cannot delete a self-signed certificate that is generated by your system.

Caution Deleting a certificate can affect your system operations. Deleting a certificate can break a certificate chain if the certificate is part of an existing chain. You can verify this relationship from the username and subject name of the relevant certificates in the **Certificate List** window. You cannot undo this action.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Use the Find controls to filter the certificate list.

Step 3 Choose the filename of the certificate.

Step 4 Click **Delete**.

Step 5 Click **OK**.

Note If the certificate that you delete is of the type “tomcat-trust”, “CallManager-trust” or “Phone-SAST-trust”, the certificate is deleted across all servers in the cluster.

Regenerate a Certificate

Before you begin an upgrade, ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. Regenerate a certificate if it is expired. Follow this procedure after business hours, because you must restart phones and reboot services. You can regenerate only a certificate that is listed as type “cert” in Cisco Unified OS Administration.

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See the online help for more information about the fields and their configuration options.

Step 3 Click **Generate**.

Step 4 Restart all services that are affected by the regenerated certificate. See the Related Topics section for more information about the certificate names and their descriptions.

Step 5 Rerun the CTL client (if configured) after you regenerate the CAPF or CallManager certificates.

Note When a Tomcat certificate is regenerated, the TFTP service should be deactivated and later activated. Else, the TFTP will continue to offer the old cached self-signed tomcat certificate.

What to Do Next

After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates.

Related Topics

Certificate Names and Descriptions, on page 9

Certificate Names and Descriptions

The following table describes the system security certificates that you can regenerate and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Table 1: Certificate Names and Descriptions

Name	Description	Related Services
tomcat tomcat-ECDSA	This self-signed root certificate is generated during installation for the HTTPS node.	Tomcat and TFTP

Name	Description	Related Services
ipsec	This self-signed root certificate is generated during installation for IPsec connections with MGCP and H.323 gateways.	Cisco Disaster Recovery System (DRS) Local and Cisco DRF Master
CallManager	This self-signed root certificate is installed automatically when you install Cisco Unified Communications Manager. This certificate provides node identification, including the node name and the global unique identifier (GUID).	CallManager, CAPF, and CTI
CAPF	The system copies this root certificate to your node or to all nodes in the cluster after you complete the Cisco client configuration.	CallManager and CAPF
TVS	This is a self-signed root certificate.	TVS

Take a Fresh Backup

You must backup the system before you perform an upgrade to ensure that the backup file matches the currently-installed software exactly. If you try to restore the system from a backup file that does not match the current version, the restore will fail.

Perform this procedure for all upgrade and migration methods.

Caution You may lose data or you may be unable to restore your system if your backup is outdated.

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 your system meets the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.

  For each application, the entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and you must create a backup file for version 11.5.1.10000-1.
- 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.**

Back Up Custom Ringtones and Background Images

If you have custom ringtones or background images in the TFTP directory, you need to create a separate backup for these files. They are not included in the Disaster Recovery System (DRS) backup file.

Procedure

Step 1 Use a web browser or TFTP client to access the directories where the ringtones and background images are stored.

Step 2 Backup the following files: `Ringlist.xml` and `List.xml` .

Step 3 Back up the custom ringtones. These are located in the TFTP directory.

Step 4 Back up the background images. These are located in the folder `/Desktops` (and its subfolders) in the TFTP directory.

Check Network Connectivity

Use this procedure to verify connectivity between all nodes and services in your network.

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 **show network cluster** command on each node in your network to verify communication between Cisco Unified Communications Manager servers in the cluster.

Step 3 If you have an NTP server, execute the **utils ntp status** command to verify connectivity to the NTP server.

Step 4 If you have an SMTP server, ping the server to verify connectivity.

Step 5 If you are using DNS, execute the **show network eth0** command on each node in your network to verify that the DNS and domain are configured.

Step 6 Check that DNS name resolution is working correctly:

a) Ping the FQDN of each Cisco Unified Communications Manager node to ensure that it resolves to the IP address.

b) Ping the IP address of each Cisco Unified Communications Manager to ensure that it resolves to the FQDN.

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.

Check Connectivity between IM and Presence and Cisco Unified Communications Manager

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.

Collect Configuration and Login Information

Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.

Procedure

Step 1 Record the following information about your network configuration:

- IP addresses, hostnames, gateways, domain names, DNS servers, NTP servers, the Call Detail Recording (CDR) server, and SMTP information
- server versions and time zones
- services running on each server and the associated activation status
- LDAP information and access details
- SNMP information

Step 2 Record the following login and password information:

- all application users credentials, such as DRS, AXL, and accounts for other third-party integrations
- administrator, cluster security, and Certificate Trust List (CTL) security token passwords

Record the Registered Device Count

Use the Real Time Monitoring Tool (RTMT) to capture the device count before you begin an upgrade, so that you can verify your endpoints and resources after the upgrade is complete. You can also use this information to verify that you have not exceeded the capacity of the virtual machine (VM) that you are deploying.

Procedure

Step 1 From the Unified RTMT interface, select **CallManager** > **Device** > **Device Summary**.

Step 2 Record the number of registered devices for each node:

Item	Count
Registered Phones	
FSX	
FSO	
T1 CAS	
PRI	
MOH	
MTP	
CFB	
XCODE	

Record the Number of Assigned Users

Record the number of assigned users on IM and Presence Service nodes so that you can verify this information after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM IM and Presence Administration interface, select **System** > **Cluster Topology**. The Cluster Topology Details page displays information about nodes and subclusters.

Step 2 Record the number of users that are assigned to each node and cluster.

Record TFTP Parameters

During the upgrade process, the TFTP service parameter **Maximum Serving Count** is changed to allow for an increased number of device registration requests. Record the existing settings so that you can reset the parameter after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM Administration interface, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, select the node that is running the TFTP service.

Step 3 From the **Service** drop-down list, select **Cisco TFTP service**.

Step 4 Click **Advanced**.

Step 5 Click **Save**.

Step 6 Record the value that is configured for the **Maximum Serving Count**.

Record Enterprise Parameters

Record the settings for Enterprise Parameters on both Unified Communications Manager nodes and IM and Presence Service nodes. Some Enterprise Parameters exist on both Unified Communications Manager nodes and IM and Presence Service nodes. Where the same parameter exists, the settings that are configured on Unified Communications Manager nodes overwrite the settings configured on IM and Presence Service nodes during the upgrade process. Enterprise Parameters that are unique to IM and Presence Service nodes are retained during an upgrade.

Record the settings so that you can restore them as needed after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM Administration interface, choose **System** > **Enterprise Parameters**.

Step 2 Take screen captures to record the settings that you have configured, and save the information so that you can restore the settings after the upgrade is complete.

Step 3 From the Cisco Unified CM IM and Presence Administration interface, choose **System** > **Enterprise Parameters**.

Step 4 Take screen captures to record the settings that you have configured, and save the information so that you can restore the settings after the upgrade is complete.

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.

Upgrade IP Phone Firmware

You can upgrade your IP phones to the firmware that corresponds to the new release as a pre-upgrade task. Although phones automatically download their new firmware after an upgrade, you can choose to apply new firmware files to the endpoints in a controlled manner prior to the upgrade in order to minimize phone downtime after an upgrade.

When you apply new firmware to phones in groups, you can eliminate the load on the TFTP server after the upgrade and accelerate the upgrade of the individual devices. Afterwards, restart the TFTP service on the Unified Communications Manager servers, and restart the IP Phones in a controlled order to minimize downtime. Because the phones cannot be used for calls when their firmware is being upgraded, we recommend that you use a maintenance window outside of your upgrade window to upgrade phone firmware.

Before You Begin

- Copy the new firmware load to the following directory on the TFTP server: `/usr/local/cm/tftp`
- Make a record of the system defaults and per-device assignments for your IP phones and registered endpoints.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Install/Upgrade**.

Step 2 Fill in the applicable values in the Software Location section and click **Next**.

Step 3 In the **Available Software** drop-down list, select the device package file and click **Next**.

Step 4 Verify that the MD5 value is correct, and then click **Next**.

Step 5 In the warning box, verify that you selected the correct firmware, and then click **Install**.

Step 6 Check that you received a success message.

Note Skip to Step 8 if you are rebooting the cluster.

Step 7 Stop and restart the TFTP server.

Step 8 Reset the affected devices to upgrade the devices to the new load.

Step 9 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults** and manually change the name of the load file (for specific devices) to the new load.

Step 10 Click **Save**, and then reset the devices.

Verify Critical Services

Use the Cisco Unified Real Time Monitoring Tool (RTMT) to verify that all critical services are activated.

Procedure

Step 1 From the Unified RTMT interface, select **System** > **Server** > **Critical Services**.

Step 2 To display system critical services, click the **System** tab.

Step 3 To display Cisco Unified Communications Manager critical services, select a Cisco Unified Communications Manager node from the drop-down list and click the **Voice/Video** tab.

Step 4 To display IM and Presence Service critical services, click the **IM and Presence** tab and select an IM and Presence Service node from the drop-down list.

Step 5 If the status indicates that any critical services are stopped, reactivate them before beginning the upgrade.

Deactivate Cisco Extension Mobility and TFTP Services

Use this procedure to stop Cisco extension mobility and TFTP services on Cisco Unified Communications Manager nodes before you begin an upgrade.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.
Step 2 From the **Server** list, choose the node on which you want to deactivate services and click **Go**.
Step 3 Deselect the **Cisco Extension Mobility** and **Cisco TFTP** services.
Step 4 Click **Stop**.
Step 5 Repeat Steps 2 and 3 for each node that is running **Cisco Extension Mobility** or **Cisco TFTP** services.
Step 6 Make a list of all the nodes on which you have disabled these services. You will need to restart the services after the upgrade is complete.

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**.

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.
- rom the Cisco Unified OS Administration interface, select **Software Upgrades** > **Device Load Management** and delete any unnecessary files.

Step 2 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.

Step 3 Perform this step only if the previous steps did not create enough disk space for the upgrade. 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 because the inactive partition becomes unusable.

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.

Procedure

Step 1 Refer to the table below this procedure to identify the COP files, if any, that you need.

Step 2 Download the upgrade files for the applications from Cisco.com. The software is available in export restricted (K9) and export unrestricted versions (XU), 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 3 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 COP files for Cisco Unified Communications Manager.

Step 4 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 COP files for IM and Presence Service.

COP Files Required for Upgrades to Release 11.5(1)

The tables below lists the upgrade paths that require COP files. You must install COP files on each node before you begin an upgrade using the Cisco Unified OS Admin interface, or before you begin an upgrade or migration using the Prime Collaboration Deployment (PCD) tool. If you are using PCD, you can perform a bulk installation of the COP files before you begin the upgrade.

Table 2: Required COP Files for Upgrades and Migrations to Cisco Unified Communications Manager Release 11.5(1)

From	To	Upgrade Type
Releases prior to and including 8.5(x)	11.5(1)	Refresh upgrade. Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
8.6(x)	11.5(1)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
9.1(x)	11.5(1)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
10.5(x)	11.5(1)	Standard upgrade; no COP file required.
11.0(x)	11.5(1)	Standard upgrade; no COP file required.
11.5(1)	11.5(x)	Standard upgrade; no COP file required.

Table 3: Required COP Files for Refresh Upgrades from Cisco Unified Presence Releases

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4) through 8.6(1)	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 4: Required COP Files for Refresh Upgrades from IM and Presence Service Releases

From IM and Presence Release	To IM and Presence Release	Upgrade Type
9.1(x)	11.5(1)	Refresh upgrade. Requires the following COP file: • ciscocm.version3-keys.cop.sgn
10.5(x)	11.5(1)	Standard upgrade; no COP file required.
11.0(x)	11.5(1)	Standard upgrade; no COP file required.
11.5(1)	11.5(x)	Standard upgrade; no COP file required.

Increase the Database Replication Timeout

Perform this procedure on the Cisco Unified Communications Manager publisher node 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).

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**.

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.