Pre-Upgrade Tasks (Manual Process)

The manual pre-upgrade tasks in this appendix can be used if you are upgrading from a release prior to 10.0(1) or if you want to complete the pre-upgrade tasks manually.

Pre-Upgrade Tasks

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

Note The steps in this task flow apply to all upgrades and migrations, unless stated otherwise.

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	Run Upgrade Readiness COP File (Pre-upgrade)	The Upgrade Readiness COP file checks your system for issues that may interfere with the upgrade. **Note** We strongly recommend that you run the COP file in order to reduce the possibility of an upgrade failure.
Step 3	Consider Smart Licensing Requirements	Release 12.x introduces Smart Licensing as a replacement for Prime License Manager. You must set up a Customer Smart account, and create the Virtual account (optionally) under the Smart account based on the organization structure. For more details on Cisco Smart

	Command or Action	Purpose
		Accounts, see https://www.cisco.com/c/en/us/buy/smart-accounts.html. For details on Smart Software Licensing Overview, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html.
Step 4	Check that the software version you are upgrading from is running on a virtual machine.	If your software is running on MCS hardware, you must complete the PCD migration task. See *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.
Step 5	Review the Requirements and Limitations for this release.	Ensure that your system meets all network, platform, and software requirements. Do this step for all upgrade and migration methods.
Step 6	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 7 • Check Database Replication, on page 8 • Check Performance Reports, on page 8 • Run CLI Diagnostics, on page 9	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.
Step 7	Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. If there are expired certificates: • Delete a Trust Certificate, on page 9 • Regenerate a Certificate, on page 10 if an Identity certificate is expired.	For Direct upgrades, ensure that your system meets all the certificate requirements. **Note** For Multi-server(SAN) certificates, ensure that SAN entries are present in all the nodes of the cluster.
Step 8	Take a Fresh Backup, on page 12	Complete a system backup. **Caution** You may lose data or you may be unable to restore your system if your backup is outdated.
Step 9	Back Up Custom Ringtones and Background Images, on page 13	If you have custom ring-tones or background images in the TFTP directory, create a separate backup for these files as they are not included in system backups.

	Command or Action	Purpose
Step 10	Check Network Connectivity, on page 14	Use this procedure to verify connectivity between Unified Communications Manager nodes and services in your network, such as NTP, SMTP, and DNS.
Step 11	Verify IPv6 Networking, on page 14	For Unified Communications Manager nodes only. Verify IPv6 networking between the publisher and subscriber nodes. Load detection may take 20 minutes if IPv6 is configured incorrectly.
Step 12	Check Connectivity between IM and Presence and Cisco Unified Communications Manager, on page 15	Verify that the IM and Presence Service has connectivity with Unified CM. For upgrades only. You can skip this task for migrations.
Step 13	Collect Configuration and Login Information, on page 15	Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.
Step 14	Record the Registered Device Count, on page 16	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.
Step 15	Record the Number of Assigned Users, on page 16	Record the number of assigned users on IM and Presence Service nodes so that you can verify this information after the upgrade is complete.
Step 16	Record TFTP Parameters, on page 17	The upgrade process changes a TFTP parameter. Record the current setting so that you can reset the parameter after the upgrade is complete.
Step 17	Record Enterprise Parameters, on page 17	During the upgrade, the Unified Communications Manager enterprise parameter settings may overwrite the IM and Presence Service enterprise parameter settings if the configurations are different.
Step 18	Export User Records, on page 17	Export user records using the Bulk Administration Tool (BAT).
Step 19	Upgrade IP Phone Firmware, on page 18	You can upgrade your IP phones to the firmware that corresponds to the new release as a pre-upgrade task in order to minimize phone downtime after an upgrade. You can skip this task for migrations.

	Command or Action	Purpose
Step 20	Verify Critical Services, on page 19	Verify that all critical services are activated.
Step 21	Deactivate Cisco Extension Mobility, on page 19	For upgrades from Release 9.x or earlier only. You must stop Cisco Extension Mobility services on Unified CM nodes before you upgrade. You can skip this task for migrations.
Step 22	Stop the IM and Presence Sync Agent, on page 20	If you need to upgrade Unified Communications Manager as part of your IM and Presence upgrade, you must stop the IM and Presence Sync Agent service before you upgrade. You can skip this task for migrations.
Step 23	Check the Available Common Partition Space, on page 20	Verify that you have enough common partition space for the upgrade. You can skip this task for migrations.
Step 24	If you do not have enough common partition space, perform one or more of the following procedures: • Adjust High and Low Watermarks, on page 20 • Maximize Usable Disk Space, on page 21	Do this step for only for direct upgrades, which use either the Unified CM OS Administration interface or the PCD Upgrade task to perform the upgrade. **Caution** Performing an upgrade without sufficient disk space can cause the upgrade to fail.
Step 25	Obtain Upgrade Files, on page 22	Download the required upgrade files. For refresh upgrades, you must also download any required COP files. **Note** Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You can skip this task for migrations.
Step 26	Increase the Database Replication Timeout, on page 23	Optional. Unified Communications Manager publisher node only. Use this procedure when you upgrade large clusters. You can skip this task for migrations.
Step 27	Disable High Availability on Presence Redundancy Groups, on page 23	IM and Presence Service only. If High Availability is enabled, disable it prior to the upgrade. You can skip this task for migrations.

	Command or Action	Purpose
Step 28	Add a Serial Port to the Virtual Machine, on page 24	Add a serial port to the virtual machine so that you can dump logs if an upgrade fails. Perform this procedure for all nodes.
Step 29	Configure High Availability for RTMT, on page 24	For megacluster deployments that monitor with RTMT, Cisco recommends configuring high availability for RTMT so that you don't lose connectivity during simplified clusterwide upgrades.
Step 30	Database Migration Required for Upgrades with Microsoft SQL Server, on page 25	This procedure applies to IM and Presence Service nodes only. If you have Microsoft SQL Server deployed as an external database with the IM and Presence Service and you are upgrading from 11.5(1), 11.5(1)SU1, or 11.5(1)SU2, you must create a new SQL Server database and migrate to the new database.
Step 31	Before you upgrade your system, ensure that you configure the **Trusted List of Hosts in HTTP Referer/Host Header** and add the public IP address or DNS alias in the Cisco Unified CM Administration Enterprise Parameters page.	This configuration is necessary if your network topology has public IP address configured for external interfaces along with private IP address for the individual nodes in the cluster. Unified CM will now validate the IP address or hostname present in the Host header with the servers configured in the Unified CM cluster first before allowing access to Unified CM. You must also configure the DNS alias used to access the Unified CM under the Trusted List of Hosts configuration. For example, if your server is cm1.example.local, and you use phone.example.local to access the server, you must add phone.example.local to the Trusted List of Hosts configuration. From Cisco Unified CM Administration user interface, select **System > Enterprise Parameters** to configure the external IP addresses or DNS alias used. **Note** If you are performing this activity post-upgrade, then you need to restart the Cisco Tomcat service for all the web pages to load correctly.

Run Upgrade Readiness COP File (Pre-upgrade)

The Upgrade Readiness COP file checks for the following things:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- Licensing sync
- VMware tools compatibility
- Hard disk partition size
- Swap size check
- Filesystem type and guest OS checks
- Usable Disk space for destination versions
- ESXi version check
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Remote Call Control (RCC) feature status
- Services status
- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameters settings
- TFTP Maximum Service Counts
- Active and Inactive versions
- List the expired certificates
- FIPS mode password length restrictions
- IPSec Policy configuration check for ESP and Encryption Algorithm in FIPS mode

Note

- It's strongly recommended that you run the Upgrade Readiness COP file before you upgrade as it reduces significantly the chances of a failed upgrade.
- The COP file is fully supported where the pre-upgrade version is 10.x or later.
- Since the 3DES Algorithm isn't supported in FIPS mode, you must delete the IPSec policy with the 3DES Algorithm and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes where IPSec tunnel is to be established.

Procedure

Step 1 Download the Upgrade Readiness COP file to run pre upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.preUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version).

Step 2 Check your system readiness for upgrades:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Run the COP file again.
d) Repeat this process until the COP file returns no errors.

Step 3 Install the cop file from GUI or CLI. Once the installation is complete, from CLI run **file view install PreUpgradeReport.txt** to view the report.

Step 4 To view the report from RTMT

a) Log in into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** and click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double-click on nodes, expand **CUCM Publisher** > **System** > **Install upgrade Logs**.
f) Double-click on **Install** and select the file which you require and download.

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

Step 2 Select **System Reports**.

Step 3 Check database replication on the node:

- For Unified CM, select **Unified CM Database Status**.
- For IM and Presence, 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 with 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.

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 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html.

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 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html.
- 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. It can also break a certificate chain if the certificate is part of an existing chain. 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 you delete the “CAPF-trust”, “tomcat-trust”, “CallManager-trust”, or “Phone-SAST-trust” certificate type, the certificate is deleted across all servers in the cluster.
- Deletion of certificates from phone edge trust should be done from publisher.
- If you import a certificate into the CAPF-trust, it is enabled only on that particular node and is not replicated across 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.

Note Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported.

Note During an upgrade, the ITLRecovery certificate is generated per cluster. If the cluster is in mixed mode, manually update the CTL file. Reset the phones to reflect the latest updates. This is applicable only for refresh upgrades. From Release 12.5(1)SU3 update CTL is no longer required.

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**.

Enter search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the **Certificate List** window.

Click **Regenerate** button in certificate details page, a self-signed certificate with the same key length is regenerated.

Note When regenerating a certificate, the **Certificate Description** field is not updated until you close the **Regeneration** window and open the newly generated certificate.

Click **Generate Self-Signed Certificate** to regenerate a self-signed certificate with a new key length of 3072 or 4096.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See 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 Certificate Names and Descriptions, on page 11 for more information.

Step 5 Update the CTL file (if configured) after you regenerate the CAPF, ITLRecovery Certificates or CallManager Certificates.

Note After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register.

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 11

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	Services to be Restarted
tomcat tomcat-ECDSA	This certificate is used by WebServices, Cisco DRF Services, and Cisco CallManager Services when SIP Oauth mode is enabled.	**Note** Restart of the below mentioned services are applicable for Release 14 onwards. Cisco Tomcat Services, Cisco Disaster Recovery System (DRS) Local and Master Services, Cisco UDS Tomcat, Cisco AXL Tomcat, and Cisco SSOSP tomcat web services. If SAML SSO is enabled with Tomcat certificate, you must re-provision the SP metadata on the IDP.

Name	Description	Services to be Restarted
ipsec	This self-signed root certificate is generated during installation for IPsec connections with Unified Communications Manager, MGCP, H.323, and IM and Presence Service.	IPsec Service.
CallManager CallManager-ECDSA	This is used for SIP, SIP trunk, SCCP, TFTP etc.	**Note** Restart of the below mentioned services are applicable for Release 14 onwards. CallManager - HAProxy Service, update CTL file if the server is in secure mode. CallManager-ECDSA - Cisco CallManager Service, HAProxy Service.
CAPF	Used by the CAPF service running on the Unified Communications Manager Publisher. This certificate is used to issue LSC to the endpoints (except online and offline CAPF mode)	N/A
TVS	This is used by Trust verification service, which acts as a secondary trust verification mechanism for the phones in case the server certificate changes.	N/A

Note

- A new enterprise parameter Phone Interaction on Certificate Update under section Security Parameter is introduced to reset phones either manually or automatically as applicable when one of the TVS, CAPF, or TFTP certificates are updated. This parameter is by default set to reset the phones automatically.
- After regeneration, deletion, and updation of certificates, ensure you restart the appropriate services mentioned in the column "Services to be Restarted".

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 Unified Communications Manager cluster nodes must be running the same version of the 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 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 Unified Communications Manager node to ensure that it resolves to the IP address.
b) Ping the IP address of each Unified Communications Manager to ensure that it resolves to the FQDN.

Verify IPv6 Networking

This procedure applies to Unified Communications Manager nodes only.

Verify that IPv6 networking on the first node (Unified Communications Manager database publisher node) and Unified Communications Manager subscriber nodes. If IPv6 is configured incorrectly on the 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 service node has connectivity with 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 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

Step 2 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

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 Service nodes. Some Enterprise Parameters exist on both Unified Communications Manager nodes and IM and Presence Service 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 Service nodes during the upgrade process. Enterprise Parameters that are unique to IM and Presence Service 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 Information" and "Inactive Load Information" for the specific Device Type fields for the new load on the TFTP server.

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 Unified Communications Manager critical services, select a 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 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

Perform this procedure only if you are upgrading from Release 9.x or earlier. For upgrades from Release 9.x or earlier, you must stop Cisco extension mobility on 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** services.

Step 4 Click **Stop**.

Step 5 Repeat Steps 2 through 4 for each node that is running **Cisco Extension Mobility** 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 Unified Communications Manager as part of your IM and Presence Service upgrade, you must stop the IM and Presence Service 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 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. However, your deployment may require more space if you have numerous TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed. In some cases, even if 25GB of free space is available, upgrade may fail with the error message as insufficient space.The workaround is to delete the unnecessary files and create more space in the common partition.

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.

Maximize Usable Disk Space

When you upgrade from 11.5(X) to 12.5, verify the COP files that are required to be downloaded. To download the COP files and the Readme files, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > **<*Version*>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

To create additional space in the common partition, you can perform one or more of the steps in this procedure.

If your current version has previously used a serial connection to upgrade from a pre-11.5(x) version then it's likely that have an older OS partitioning scheme and virtual disk layout. This will amplify "out of disk space" issues, thereby limiting the effectiveness of adding additional virtual disk space. The upgrade readiness COP file checks for these issues, and provides guidance on how to resolve them.

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

Note Run the **show diskusage tftp <sort>** command, to check tftp device load size, which is sorted by descending file size.

Run the **show diskusage common <sort>** command, to check the common partition size for available, and free space, which is sorted by descending file size.

Step 2 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.

Note For 110G or two 80G disk deployments, available space for upgrade should be at least twice the active partition disk space. For example, in a two 80G disk deployment, active partition should not be more than 25G, and available space should be at least 50G. Following are commands to check the disk usage.

a. Run the **show diskusage activelog <sort>** command, to check active side partition size, which is sorted by descending file size.

b. Run the **show diskusage common <sort>** command, to check the common partition size for available, and free space, sorted by descending file size.

c. Run the **show diskusage tftp <sort>** command, to check tftp device load size, which is sorted by descending file size.

d. Run the **file delete activelog <filename>** command, to delete logs from active partition.

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 Unified Communications Manager upgrade file, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, 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 Service upgrade file, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, 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 > click **Software Download** link under **Download & Upgrade** section, and then, 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 Unified Communications Manager.

Step 4 Go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, 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.

Required COP Files

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.

For more information on the COP files that are required, see the *Supported Upgrade and Migration Paths with COP Files* section.

Increase the Database Replication Timeout

Perform this procedure on the Unified Communications Manager publisher node only.

Increase the database replication timeout value when you upgrade large clusters so that more Unified Communications Manager subscriber nodes have sufficient time to request replication. When the timer expires, the first Unified Communications Manager subscriber node, plus all other Unified Communications Manager subscriber nodes that requested replication within that time period, begin a batch data replication with the 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 Service nodes only. Use it to disable high availability on the IM and Presence Service presence redundancy group.

Before you begin

Take a record of the number of active users for each cluster node in each Presence Redundancy Group. You can find this information in the (**System** > **Presence Topology**) window of Cisco Unified CM IM and Presence Administration. You will need this information later when you re-enable High Availability.

Procedure

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

Step 2 Click **Find** and select the group.

Step 3 On the Presence Redundancy Group Configuration window, uncheck the **Enable High Availability** check box.

Step 4 Click **Save**.

Step 5 Repeat this procedure for each Presence Redundancy Group.

Step 6 When you are done, wait at least two minutes to sync the new HA settings across the cluster before you make any further changes

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.

Configure High Availability for RTMT

If you use Cisco Unified Real-Time Monitoring Tool (RTMT) and have a mega-cluster deployment, Cisco recommends configuring high availability for RTMT to avoid connectivity loss during a simplified cluster-wide upgrade.

Procedure

Step 1 Log in to any Cisco Unified Communications Manager node.

Step 2 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 3 From the **Server** drop-down, select a Unified CM node.

Step 4 From the **Service** drop-down, select **Cisco AMC Service**.

Step 5 For the **Primary Collector** service parameter, select any subscriber node.

Step 6 For the **Failover Collector** service parameter, select a different subscriber node.

Step 7 Click **Save**.

Step 8 Connect the Cisco Unified Real-Time Monitoring Tool to any subscriber node.

Database Migration Required for Upgrades with Microsoft SQL Server

If you have Microsoft SQL Server deployed as an external database with the IM and Presence Service and you are upgrading from 11.5(1), 11.5(1)SU1, or 11.5(1)SU2, you must create a new SQL Server database and migrate to the new database. This is required due to enhanced data type support in this release. If you don't migrate your database, schema verification failure occurs on the existing SQL Server database and services that rely on the external database, such as persistent chat, will not start.

After you upgrade your IM and Presence Service, use this procedure to create a new SQL Server database and migrate data to the new database.

Note This migration is not required for Oracle or PostgreSQL external databases.

Before you begin

The database migration depends on the `MSSQL_migrate_script.sql` script. Contact Cisco TAC to obtain a copy.

Procedure

Step 1 Create a snapshot of your external Microsoft SQL Server database.

Step 2 Create a new (empty) SQL Server database. For details, see the following chapters in the Database Setup Guide for the IM and Presence Service:

a. "Microsoft SQL Installation and Setup"—See this chapter for details on how to create your new SQL server database on your upgraded IM and Presence Service.

b. "IM and Presence Service External Database Setup"—After your new database is created, refer to this chapter to add the database as an external database in the IM and Presence Service.

Step 3 Run the System Troubleshooter to confirm that there are no errors with the new database.

a. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**.

b. Verify that no errors appear in the **External Database Troubleshooter** section.

Step 4 Restart the Cisco XCP Router on all IM and Presence Service cluster nodes:

a. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

b. From the **Server** menu, select an IM and Presence Service node and click **Go**.

c. Under **IM and Presence Services**, select **Cisco XCP Router**, and click **Restart**.

Step 5 Turn off services that depend on the external database:

a. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**.

b. From the **Server** menu, select an IM and Presence node and click **Go**.

c. Under **IM and Presence Services**, select the following services:

Cisco XCP Text Conference Manager

Cisco XCP File Transfer Manager

Cisco XCP Message Archiver

d. Click **Stop**.

Step 6 Run the following script to migrate data from the old database to the new database `MSSQL_migrate_script.sql`.

Note Contact Cisco TAC to obtain a copy of this script.

Step 7 Run the System Troubleshooter to confirm that there are no errors with the new database.

a. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**.

b. Verify that no errors appear in the **External Database Troubleshooter** section.

Step 8 Start the services that you stopped previously.

a. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**.

b. From the **Server** menu, select an IM and Presence node and click **Go**.

c. Under **IM and Presence Services**, select the following services:

Cisco XCP Text Conference Manager

Cisco XCP File Transfer Manager

Cisco XCP Message Archiver

d. Click **Start**.

Step 9 Confirm that the external database is running and that all chat rooms are visible from a Cisco Jabber client. Delete the old database only after you're confident that the new database is working.