Cisco Unified Communications Manager
Cisco Unified Instant Messaging and Presence
Pre Upgrade Check COP(ciscocm.preUpgradeCheck-0019.cop) File

Release Notes Version 19
December 12th , 2018

Introduction:

These release notes contain important information about installation procedures for the Pre-Upgrade Check COP file for Cisco Unified Communications Manager and Cisco Unified Instant Messaging and Presence. Henceforth, in this document, the term **server** refers to both **Cisco Unified Communications Manager** and **Cisco Unified Instant Messaging and Presence.** This COP file is designed for and tested on CUCM 9.x, 10.x, 11.x and 12.x releases and IM & Presence 9.x, 10.x, 11.x and 12.x releases.

Note: Before you run this COP file, we recommend that you review the *Important Notes* section for information about issues that may affect your system.

What this COP file provides:

This COP file contains tests some of which are part of Pre-upgrade tasks section of ***Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence service***.

The tests are executed when the COP runs and a report is displayed that shows the test results and recommendations. The particulars about the tests are as given below:
(All the tests are applicable to Unified Communications Manager publisher, Unified Communications Manager subscriber, IM&P Publisher and IM&P Subscriber. Any exception to the applicability will be mentioned in test details):

1. Network status:

- This test checks the following:
  - Intra-cluster connectivity
  - DNS reachability
  - NTP status
    - NTP reachability - Checks the reachability of external NTP server(s)
    - NTP clock drift - Checks the local clock's drift from the NTP server(s)
    - NTP stratum - Checks the stratum level of the refrence clock.
- If there are any issues with any or all of the above checks, the test is marked as “FAIL” and appropriate reason is mentioned in the report.

2. COPS Installed:

- This test lists COPs that are installed on active partition of the server.
- The test displays a warning if there is more than one version of the same local cop installed or If dp-ffr.3-1-16.GB.cop is installed on a 9.x server.

3. Service status:

- This test inspects the state of all services (STARTED or STOPPED) and reports services that are:
  - Critical network services and are stopped
  - Activated but not running
- The test is marked as “FAIL” if it finds any service satisfying the above criteria.
- The test also stores the state of all services for use by Post Upgrade Check COP.

4. **Data Base Sanity:**
    - This test checks if there are non-standard entries present in a few database tables. The presence of these entries may cause the upgrade DB Migration to fail.
    - If the test detects non-standard entries, the entries along with their resident database table name is shown in the report and test is marked as "FAIL".
    - Admin is expected to delete those non-standard entries before upgrade is attempted.

5. **Cluster Database Status:**
    - This test is applicable only to Unified Communications Manager Publisher and IM&P Publisher:
    - This test does the following checks in the same sequence as described below:
        - *Node authentication state*: if any node in the cluster is unauthenticated, the test is marked as "FAIL" and unauthenticated node name is shown in the report.
        - *Replication state*: if any node in the cluster has replication setup value other than "2", the test is marked as "FAIL" and node name is shown in the report.

6. **Last DRS backup date:**
    - This test shows when the Last DRS backup was taken. Is it is more than 3 days back or whether DRS is configured or not.
    - If the backup date is very old, Admin can take backup of the latest configuration so that the admin can avoid losing latest configuration in case the DRS backup needs to be restored.

7. **Disk Space Check:**
    - The test checks free space required for all higher releases (till 12.5) than the server's current release.
    - If the free space is insufficient for upgrade to all higher releases, the test is marked as "FAIL". If the free space is sufficient to upgrade to at least one, but not all of the higher releases, the test displays a warning.

8. **PLM/SLM License Status:**
    - For CUCM version 9.x to 11.x, this checks PLM License Status and shows appropriate warning if applicable.
    - For 12.x, this test checks SLM License status based on Registration Status and Authorization Status.

9. **Common Security Password Length:**
    - Release 12.5 requires common security password to be more than 14 characters when in FIPS, ESM or CC mode. This test fails if FIPS, ESM or CC mode is enabled and password length is less than 14 chars. It is skipped if FIPS mode is not enabled.

10. **Phone Count:**
    - This test list the count of Registered and Unregistered Phone.
    - This test also stores this data for comparison during post upgrade COP.

11. **VM Tools Type:**
    - Checks the VM tools type, If VM tools type is "open vmtools", then, it prints the vmtools type and version.
    - If VM tools type is "native vmtools", then, it prints the VM tools type and version along with following recommendation.

12. **Upgrade Checks:**
    - This test gives critical information applicable for upgrading to 12.5

13. **Deprecated Phone Models:**
    - This test checks for the phones in Unified Communications Manager Cluster that are no longer supported from 12.x release onwards (unsupported phones can be found here)
    - This test displays a warning if there are any such deprecated phones (MAC Id and the phone model are shown in the report)

14. **Network Adapter compatibility:**

- This test checks whether the current network adapter is supported in 12.x releases of Unified Communications Manager and IM and Presence service.
- If Network Adapter is incompatible, the test fails with recommendation to switch to VMXNET3 adapter.

Related Documentation:

To view documentation that talks about Pre-upgrade tasks for specific releases, go to: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Determining the Software Versions:

Unified Communications Manager

You can determine the System Version of your Cisco Unified Communications Manager software that is running on your server by accessing Cisco Unified Operating System Administration.

The following information displays:

- System version: xxxxx
- VMware Installation: xxxxx

Important Notes:

- When you run the COP file, it does not change any executables or configuration of the system.
- Some tests are not applicable to 9.x release of CUCM and IM & Presence.
- It executes a few shell commands and CLI commands to gather information about the current system state and preserves this information for use by "Post Upgrade Check" COP.
- Admin is expected to run "Post Upgrade Check" COP after server is upgraded to validate whether the system is in a good state.

Installation Instructions:

As with any installation or upgrade, we recommend that you run this COP during off peak hours.

Apply this COP to all nodes in the cluster.
Caution: ***The updates applied with this COP cannot be uninstalled***. Be sure to back up your system data before starting the software upgrade process. For more information, see the ***Disaster Recovery System Administration Guide.***

From Remote Source:

Step 1: Download *ciscocm.preUpgradeCheck-0001.cop*

Step 2: Copy the file to an FTP or SFTP server.

Step 3: Access the Cisco Unified Communications Operating System Administration page directly by entering the following URL:

http://server-name/cmplatform

(where, server-name is the host name or IP address of the admin server.)

Step 4: Enter your OS Administrator username and password.

Step 5: Choose **Software Upgrades** > **Install/Upgrade**.

Step 6: For the software location source, choose **Remote File System**.

Step 7: Enter the directory name for the software upgrade, if required.

If the upgrade file is located on a Linux or UNIX server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter /patches.

If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

Step 8: Enter the required upgrade information as described in the following table:

Remote Server: Host name or IP address of the remote server from which software will be downloaded.

Remote User: Name of a user who is configured on the remote server.

Remote Password: Password that is configured for this user on the remote server.

Download Protocol: Choose SFTP or FTP.

Step 9: To continue the upgrade process, click **Next**.

Step 10: Choose "<cop name to be added>" and click **Next**.

Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are transferred.

When the download completes, the **Checksum** window displays.

Step 12: Verify the checksum value:

<check-sum value to be added>

Step 13: After determining that the checksums match, click **Next** to proceed with the software upgrade.

A Warning window displays the selected option.

Step 14: Click **Install**.

The 'Install Status' window displays the install log.

Step 15: When the installation completes, click **Finish**.

Step 16: Verify the COP file version using this command from the CLI:

admin:show version active

Active Master Version: 9.1.1.xxxxx-xx <-- *Note: 9.1.1 is shown for example only; your version may vary*

Active Version Installed Software Options:
ciscocm.preUpgradeCheck-0001.cop