

Upgrade Readiness Checks COP File for CUCM and IMPS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[How to Use](#)

[How to Get the Report and Review it](#)

[1. Network Status](#)

[2. COPS Installed](#)

[3. Service Status](#)

[4. Data Base Sanity](#)

[5. Cluster Database Status](#)

[6. Last DRS Backup Date](#)

[7. Disk Space Check](#)

[10. Phone Count](#)

[12. Upgrade Checks](#)

[13. Deprecated Phone Models](#)

[14. Network Adapter Compatibility](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how the upgrade readiness checks COP file for Cisco Unified Communications Manager (CUCM) and IM and Presence Server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager 9.x and later
- IM and Presence Server (IMPS) 9.x and later

Components Used

The information in this document is based on Cisco Unified Communications Manager version 10.5.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Upgrade of Cisco Unified Communications Manager and Presence Servers have some prerequisites like enough logging partition can be available, the successful backup can be taken, database and network can be incorrect state and so on.

Similarly, few checks can satisfy post upgrade to make sure the cluster is in good health after the upgrade.

Cisco has come up with cop files which can automate these tasks and helps in maximize the likelihood of UCM, IM&P upgrade success so that the admin can avoid extra downtime and wasted effort trying to recover from problems, or revert, or abort the upgrade.

The admin needs to just run these cop files on the Servers which are going to be upgraded, and which checks different aspects and provides a report.

There are two types of cop files.

PreUpgradeCheck COP: It verifies that the system is in a good state to start the upgrade. PreUpgradeCheck 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, Release 11.5\(1\)](#).

PostUpgradeCheck COP: It verifies that the system is in a good state after the upgrade. This COP uses the data created by Pre Upgrade Check COP file for comparing the various aspects of system state before and after the upgrade.

PostUpgradeCheck COP file contains tests some of which are part of Post-upgrade Tasks section of [Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5\(1\)](#).

Configure

The PreUpgradeCheck and PostUpgradeCheck cop files are available on the Cisco Software Download Page and can be downloaded through this link.

[Click to Download COP files.](#)

How to Use

Before the upgrade, download and install/run the latest version of **preUpgradeCheck** COP file. Look at PASS / WARNING / FAIL output. Resolve all FAIL and the WARNINGS. Repeat until satisfied.

After the upgrade, download and install/run the latest version of **postUpgradeCheck** COP file. This checks for system sanity and compares items in Active and Inactive Versions. Services and phones can take some time to come up, so it is recommended to repeat running the cop a few times at some interval.

Installing the cop file is similar to other cop file installation, and the detailed steps for installation are present in the Readme of the cop files.

Click on [PrecheckUpgrade Readme](#) or [PostUpgradeCheck Readme](#) to see the details.

How to Get the Report and Review it

Once the installation of cop files finishes, it can show a summary of test results and path/command to view

the complete report.

Summary:

Total Test Run : 14
Total Passed : 10
Total Warnings : 3
Total Failed : 1

Note: Please refer to the readme of Pre Upgrade cop for test details and pass/fail/warn/criteria

Duration for running tests: 0:01:49

=====
Use "file view install PreUpgradeReport.txt" to view the report

For PreUpgradeCheck run **file view install PreUpgradeReport.txt** and for PostUpgradeCheck **file view install PostUpgradeReport.txt**.

The output is similar to this image that shows the results as PASS/FAIL/WARNING for different aspects.

```
admin:file view install PreUpgradeReport.txt

Use "file view install PreUpgradeReport.txt" to view the report
=====
                                Pre Upgrade Test                                Date: 01/25/2019
=====
Active Version:  10.5.2.12900-14
Server:  cucm1051 , CUCM Publisher
=====

Result  Test
-----  -----
1.1  WARN    DRS backup status
      WARNING: No backup device is configured. This is required to reco
      system in case of failure.

1.2  PASS    Cluster Database Status
1.3  PASS    Deprecated Phone Models
1.4  PASS    Common Security Password Length
      System not in FIPS mode, Common Security Password's Minimum lengt
      requirement not enforced
```

This is the list of different components that are checked.

1. Network Status

These are the test checks:

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 reference clock.

If there are any issues with any or all of the previous checks, the test is marked as **FAIL** and the appropriate reason is mentioned in the report.

2. COPS Installed

This test lists COPs that are installed on an 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.
- Activates but does not run.
- The test is marked as **FAIL** if it finds any service satisfying the previous 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 can cause the upgrade DB Migration to fail.

If the test detects non-standard entries, the entries along with their resident database table name are shown in the report and test is marked as **FAIL**.

Admin is expected to delete those non-standard entries before an upgrade is attempted.

5. Cluster Database Status

This test is applicable only to Unified Communications Manager Publisher and IM&P Publisher.

This test does these checks in the same sequence as described here:

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 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 the latest configuration in case the DRS backup needs to be restored.

7. Disk Space Check

This test checks free space required for all higher releases (till 12.5) than the servers current release. If the free space is insufficient for an 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 an 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 characters. It is skipped if FIPS mode is not enabled.

10. Phone Count

This test lists 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 the this 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 a recommendation to switch to VMXNET3 adapter.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

When some test fails, and the recommendation string is not enough, perform these troubleshoots:

Look for details in the install logs for generic issues with running a COP like Filtering the COP file, download and install phases started and completed.

- Ensure the COP is being run on CCM or IM&P Products only.
- Ensure the COP is being run on or previous minimum supported version of 9.x.

Pre and Post upgrade logs are not yet available for download from RTMT, hence use **file dump or file get** the option to download the logs.

Use the CLI commands `file get install PreUpgradeReport.txt (PreUpgrade)` and `file get install PostUpgradeReport.txt(PostUpgrade)`.