

Verifica preparazione aggiornamento file COP per CUCM e IMPS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Modalità d'uso?](#)

[Come ottenere il report e rivederlo?](#)

[1. Stato della rete](#)

[2. COPS installato](#)

[3. Stato del servizio](#)

[4. Sanità della base dati](#)

[5. Stato database cluster](#)

[6. Data ultimo backup DRS](#)

[7. Controllo dello spazio su disco](#)

[10. Numero di telefono](#)

[12. Controlli di aggiornamento](#)

[13. Modelli telefonici deprecati](#)

[14. Compatibilità delle schede di rete](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come verificare la preparazione dell'aggiornamento del file COP per Cisco Unified Communications Manager (CUCM), IM e Presence Server.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager 9.x e versioni successive
- IM e Presence Server 9.x e versioni successive

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Unified Communications Manager versione 10.5.2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'aggiornamento di Cisco Unified Communications Manager e dei server di presenza richiede alcuni prerequisiti, ad esempio la disponibilità di una partizione di registrazione sufficiente, l'esecuzione corretta del backup, lo stato del database e della rete non corretto, ecc.

Analogamente, pochi controlli dovrebbero soddisfare anche dopo l'aggiornamento per assicurarsi che il cluster sia in buono stato dopo l'aggiornamento.

Cisco ha creato dei file cop che automatizzeranno queste attività e aiuteranno a massimizzare la probabilità di successo dell'aggiornamento di UCM, IM&P in modo che l'amministratore possa evitare ulteriori tempi di inattività e sprecare sforzi nel tentativo di ripristinare da problemi o ripristinare o interrompere l'aggiornamento.

L'amministratore deve solo eseguire questi file di copia sui server che verranno aggiornati che controllano i diversi aspetti e forniscono un rapporto.

Esistono due tipi di file cop.

Controllo pre-aggiornamento COP: Verifica che lo stato del sistema sia corretto per avviare l'aggiornamento. Il file PreUpgradeCheck COP contiene test che in alcuni casi fanno parte della sezione Pre-upgrade tasks della [Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, release 11.5\(1\)](#).

Controllo post-aggiornamento COP: Verifica che il sistema sia in buono stato dopo l'aggiornamento. Questo COP utilizza i dati creati dal file COP di controllo pre-aggiornamento per confrontare i vari aspetti dello stato del sistema prima e dopo l'aggiornamento.

Il file POSTUpgradeCheck COP contiene test che in alcuni casi fanno parte della sezione Post-upgrade Tasks della [Guida all'aggiornamento e alla migrazione per Cisco Unified Communications Manager e i servizi di messaggistica immediata e presenza, versione 11.5\(1\)](#).

Configurazione

I file cop PreUpgradeCheck e PostUpgradeCheck sono disponibili nella pagina di download del software Cisco e possono essere scaricati tramite questo collegamento.

[Fare clic per scaricare i file COP.](#)

Modalità d'uso?

Prima dell'aggiornamento, scaricare e installare/eseguire l'ultima versione del file

preUpgradeCheck COP. Osservare l'output PASS / WARNING / FAIL. Risolvere tutti gli errori FAIL e forse gli avvisi. Ripetete finché felici.

Dopo l'aggiornamento, scaricare e installare/eseguire l'ultima versione del file **postUpgradeCheck** COP. In questo modo viene verificata l'integrità del sistema e vengono confrontati gli elementi nelle versioni attive e inattive. I servizi e i telefoni possono richiedere un po' di tempo per venire su, quindi si consiglia di ripetere l'esecuzione del poliziotto alcune volte ad un certo intervallo.

L'installazione del file cop è simile a quella di altri file cop e i passaggi dettagliati per l'installazione sono presenti nel file Readme dei file cop.

Fare clic su [PrecheckUpgrade Readme](#) o [PostUpgradeCheck Readme](#) per visualizzare i dettagli.

Come ottenere il report e rivederlo?

Al termine dell'installazione dei file di copia, verrà visualizzato un riepilogo dei risultati del test e il percorso/comando per visualizzare il report completo.

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

Per PreUpgradeCheck eseguire **visualizzazione file installare PreUpgradeReport.txt** e per PostUpgradeControllare visualizzazione file installare PostUpgradeReport.txt.

L'output è simile a questa immagine e mostra i risultati come PASS/FAIL/WARNING per diversi aspetti.

```
admin:file view install PreUpgradeReport.txt
```

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

```
=====
                        Pre Upgrade Test                        Date: 01/25/2019 19:14:13
=====
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 recover your
      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 length
      requirement not enforced
```

Questo è l'elenco dei diversi componenti selezionati.

1. Stato della rete

Questi sono i controlli di prova:

Connettività tra cluster

Raggiungibilità DNS

Stato NTP

Raggiungibilità NTP - Verifica la raggiungibilità dei server NTP esterni

Deriva orologio NTP: controlla la deriva dell'orologio locale dai server NTP

NTP stratum - Controlla il livello di strato dell'orologio di riferimento.

In caso di problemi in uno o in tutti i controlli di cui sopra, il test è contrassegnato come **FAIL** e il motivo appropriato è indicato nel rapporto.

2. COPS installato

Questo test elenca i COP installati in una partizione attiva del server.

Il test visualizza un avviso se sono installate più versioni della stessa copia locale o se dp-ffr.3-1-16.GB.cop è installato su un server 9.x.

3. Stato del servizio

Questo test controlla lo stato di tutti i servizi (AVVIATI o ARRESTATI) e segnala i servizi seguenti:

- Servizi di rete critici e sono arrestati.
- Si attiva ma non viene eseguito.
- Il test viene contrassegnato come **FAIL** se viene rilevato un servizio che soddisfa i criteri indicati.
- Il test memorizza inoltre lo stato di tutti i servizi per l'utilizzo da parte di Controllo COP post-aggiornamento.

4. Sanità della base dati

Questo test verifica la presenza di voci non standard in alcune tabelle di database. La presenza di queste voci potrebbe causare un errore nella migrazione del database di aggiornamento.

Se il test rileva voci non standard, le voci insieme al nome della tabella del database residente vengono visualizzate nel report e il test viene contrassegnato come **FAIL**.

L'amministratore deve eliminare tali voci non standard prima di tentare un aggiornamento.

5. Stato database cluster

Questo test è valido solo per Unified Communications Manager Publisher e IM&P Publisher.

Il test esegue i controlli nella stessa sequenza descritta di seguito.

Stato autenticazione nodo: se uno dei nodi del cluster non è autenticato, il test viene contrassegnato come **FAIL** e nel report viene visualizzato il nome del nodo non autenticato.

Stato replica: se un nodo del cluster ha un valore di impostazione della replica diverso da **2**, il test viene contrassegnato come **FAIL** e il nome del nodo viene visualizzato nel report.

6. Data ultimo backup DRS

Questo test mostra quando è stato eseguito l'ultimo backup DRS. È trascorso più di 3 giorni o se DRS è configurato o meno?

Se la data di backup è molto vecchia, l'amministratore può eseguire il backup della configurazione più recente in modo da evitare di perdere la configurazione più recente nel caso in cui sia necessario ripristinare il backup DRS.

7. Controllo dello spazio su disco

Il test controlla lo spazio libero richiesto per tutte le versioni superiori (fino alla 12.5) rispetto alla versione corrente del server.

Se lo spazio disponibile non è sufficiente per l'aggiornamento a tutte le versioni successive, il test viene contrassegnato come **FAIL**. Se lo spazio disponibile è sufficiente per eseguire l'aggiornamento ad almeno una, ma non a tutte le versioni successive, il test visualizza un avviso.

8. Stato della licenza PLM/SLM

Per le versioni da 9.x a 11.x di CUCM, viene controllato lo stato della licenza PLM e viene visualizzato un messaggio di avvertenza appropriato, se applicabile.

Per la versione 12.x, questo test controlla lo stato della licenza SLM in base allo stato di registrazione e allo stato di autorizzazione.

9. Lunghezza comune password di protezione

La release 12.5 richiede una password di sicurezza comune superiore a 14 caratteri in modalità FIPS, ESM o CC. Questo test ha esito negativo se è abilitata la modalità FIPS, ESM o CC e la lunghezza della password è inferiore a 14 caratteri. Viene ignorato se la modalità FIPS non è attivata.

10. Numero di telefono

Questo test elenca il numero di telefoni registrati e non registrati.

Questo test memorizza anche questi dati per il confronto durante la COP post-aggiornamento.

11. Tipo di strumenti VM

Verifica il tipo di strumenti VM. Se il tipo di strumenti VM è **open vmtools**, stampa il tipo e la versione di vmtools.

Se il tipo di strumenti VM è **vmtools nativo**, vengono stampati il tipo di strumenti VM e la versione insieme al suggerimento seguente.

12. Controlli di aggiornamento

Questo test fornisce informazioni critiche applicabili all'aggiornamento alla versione 12.5

13. Modelli telefonici deprecati

Questo test verifica la presenza nel cluster Unified Communications Manager di telefoni non più supportati a partire dalla versione 12.x (qui sono riportati i telefoni non supportati)

Questo test visualizza un avviso se sono presenti telefoni deprecati di questo tipo (ID MAC e il modello del telefono sono mostrati nel report)

14. Compatibilità delle schede di rete

Questo test verifica se la scheda di rete corrente è supportata nelle versioni 12.x di Unified Communications Manager e del servizio di messaggistica immediata e presenza.

Se la scheda di rete non è compatibile, il test ha esito negativo e si consiglia di passare alla scheda VMXNET3.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Se alcuni test hanno esito negativo e la stringa consigliata non è sufficiente, eseguire le seguenti procedure di risoluzione dei problemi:

Cercare i dettagli nei log di installazione per problemi generici relativi all'esecuzione di un COP come filtrare il file COP, le fasi di download e installazione avviate e completate.

- Verificare che il COP venga eseguito solo su prodotti CCM o IM&P.
- Verificare che il COP venga eseguito nella versione minima supportata di 9.x o in una versione superiore.

I log di pre e post-aggiornamento non sono ancora disponibili per il download da RTMT, quindi utilizzare **file dump** o **file get** the option to download the logs.

Utilizzare i comandi CLI `get install PreUpgradeReport.txt` (PreUpgrade) e `file get install PostUpgradeReport.txt`(PostUpgrade).