Come risolvere i duplicati degli endpoint Cisco Prime Collaboration Assurance (PCA)

Sommario

Introduzione

In questo documento viene descritto come risolvere i duplicati degli endpoint di Cisco Prime Collaboration Assurance.

Contributo di Joseph Koglin, Cisco TAC Engineer

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del modulo Inventory e delle relative operazioni in Prime Assurance
- Nozioni fondamentali di Linux su Prime Assurance

Il documento richiede l'implementazione della configurazione seguente:

- Sarà necessario l'accesso completo alla directory principale. Se non si dispone dell'accesso alla directory principale, fare riferimento alla sezione inferiore denominata Accesso alla directory principale.
- L'applicazione Prime Assurance viene installata e gli endpoint sono duplicati nel sistema di inventario. Es. Due endpoint con lo stesso nome: SEPA11B22CC3

  Nota: Le operazioni illustrate in questo articolo hanno un impatto sulle banche dati, pertanto queste operazioni devono essere eseguite solo da personale qualificato. In particolare, nell'APC 12.1, poiché la funzionalità dell'inventario è stata rivista, il requisito di tali fasi non dovrebbe essere soddisfatto, ma può essere considerato come un ultimo rimedio sotto la supervisione di esperti.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Interfaccia della riga di comando di Prime Assurance
- Prime Assurance Inventory Module

- Tutte le versioni software applicabili
- Nessun requisito hardware richiesto

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

Problema

Cisco Prime Assurance - Duplicazione di telefoni

Questo documento è destinato agli ambienti con telefoni duplicati nel sistema o agli scenari in cui è possibile rimuovere e aggiungere nuovamente gli endpoint.

Questo processo rimuoverà tutti i telefoni e dopo che il processo li riaggiungerà

Soluzione

Passaggio 1. Accedere a PCA tramite Secure Shell (SSH) come root e port 26

Passaggio 2. Input. **cd /opt/emms/emsam/bin/**

Passaggio 3.Ora si interromperanno i servizi con Input. **./cpcmcontrol.sh stop**

Passaggio 4. Verificare che tutti i servizi siano inattivi in base allo stato Input. **./cpcmcontrol.sh**

- Dopo l'interruzione di tutti i servizi passare alla fase successiva

Passaggio 5. Verrà avviato solo il servizio di database tramite Input. **./start_db.sh**

Il passo 6 e il passo 7 rimuoveranno i telefoni dal database. Nel passo 11 li riporterete nel sistema

Passaggio 6. Inserire. **./refreshCDT.sh** (attendere il completamento)

Passaggio 7. Inserire. **./refreshPhone.sh** (attendere il completamento)

Passaggio 8. Ora i servizi verranno ripristinati con l'input. **./cpcmcontrol.sh riavviare**

(eseguire periodicamente **./cpcmcontrol.sh status** per garantire il ripristino di tutti i servizi)

Passaggio 9. Quando la GUI esegue il backup, eseguire il login come utente globaladmin ed eseguire il rilevamento dei dati del cluster come passaggio successivo.

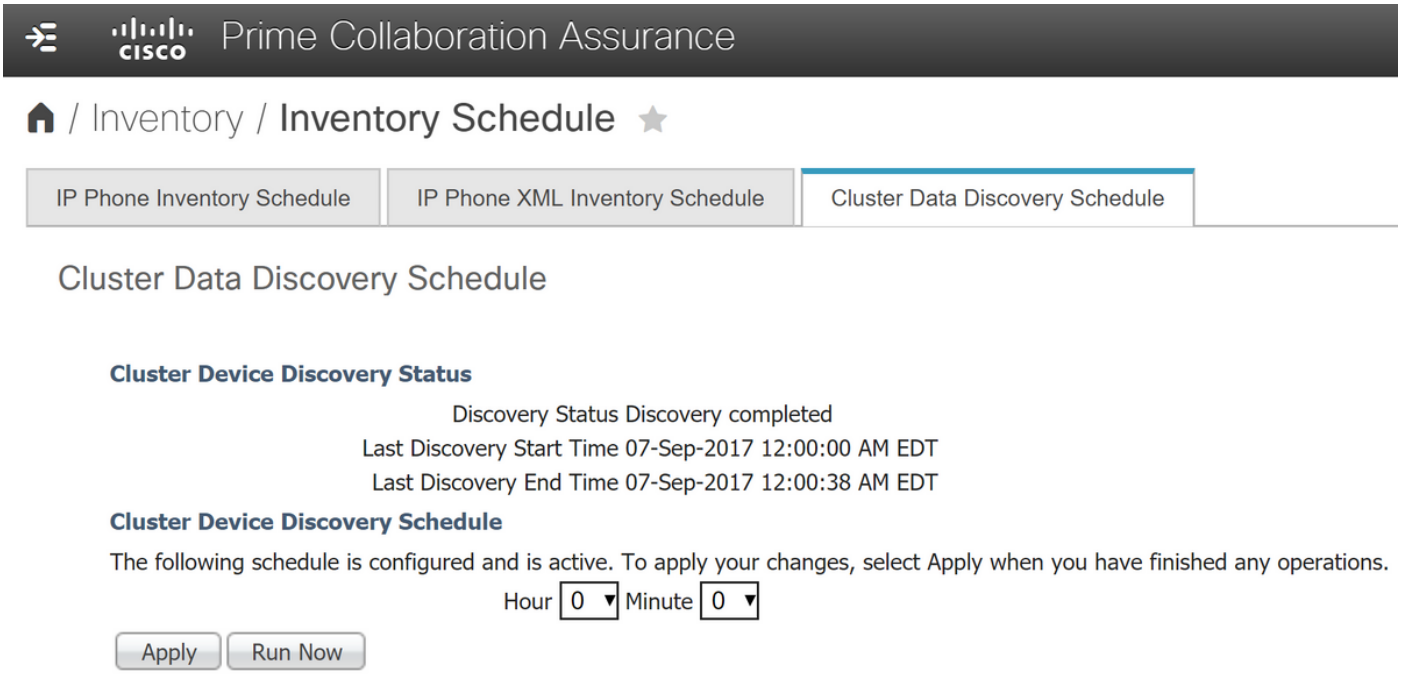
Passaggio 10. Verrà quindi eseguito un rilevamento dei dati del cluster: Passare a **Inventario>Programmazione inventario>Individuazione dati cluster.**

Passaggio 11. Selezionare **Esegui adesso** (questo passaggio recupererà i telefoni)

Passaggio 12. Attendere che sia finito e i telefoni dovrebbero essere di nuovo e non avere duplicati.

Nota: Questo rilevamento dipende dal numero di endpoint nel cluster e i tempi di completamento possono variare

Ad esempio, potete confrontare l'ora di inizio e di fine e vedere che per completare questo particolare studio sono stati necessari solo 38 secondi.



Nota: A scopo informativo, il PCA recupererà i telefoni tramite Real-time Information Service (RIS) e Administrative Extensible Markup Language (AXL) dall'editore Cisco Unified Communication Manager (CUCM)

Registri utili in caso di problemi:

Se si riscontrano ancora duplicati, fare riferimento ai registri indicati per la revisione

Nota: Se non si dispone di, fare riferimento alla sezione Accesso alla radice. Dopo aver abilitato l'accesso completo alla directory principale, utilizzare un programma quale Winscp per connettersi e utilizzare la porta 26 e le credenziali dell'utente root.

/opt/emms/cuom/log/CUOM/CDT

RISCollection.log, CDT.log, CDTAPI.log, CDTAudit.log

/opt/emms/emsam/log/Inventory/CDT.log
/opt/emms/emsam/log/Tomcat/CDT.log

/var/log/refreshPhone.log <— consente tu sapere se si sono verificati problemi con gli script eseguitire

Ulteriori note sulla risoluzione dei problemi e informazioni generali:

Èinoltre possibile verificare se è possibile riavviare il servizio RIS nel cluster di Gestione chiamate in quanto ciò potrebbe eliminare alcune discrepanze o problemi.

Quando i telefoni vengono raccolti in cucm utilizzerà axl+ris, quindi in caso di problemi è possibile riavviare il servizio RIS in cucm.

Il riavvio del servizio RIS nel cluster non avrà alcun impatto sull'attività aziendale, poiché non è consigliabile riavviare il servizio AXL durante l'orario di lavoro.

Inoltre, raramente è necessario riavviare il servizio AXL, quindi prima di eseguire questa operazione, è necessario consultare i registri per verificare se è necessario riavviare.

Verificare inoltre che i Call Manager siano gestiti e che in cucm in System>Server sia possibile eseguire il ping e risolvere l'hostname/ip dell'editore cucm.

Poiché si potrebbe verificare un caso in cui Gestione chiamate è stato individuato e gestito come IP, tuttavia nel sistema di Gestione chiamate>Server è elencato per nomehost.

Ciò che accade è quando PCA raccoglie i telefoni tramite axl+ris esso elencherà comunque è elencato sotto Sistema>server quindi se si dispone di elencato come il nome host e non è risolvibile da pca allora non riceverete mai questi telefoni anche se il cucm è gestito perché è stato gestito da ip.

Questo scenario viene risolto in due modi:

Scenario 1

Passaggio 1. Accedere a PCA tramite l'utente root SSH e la porta 26

Passaggio 2. Cd/ecc

Passaggio 3. Host Vi

Passaggio 4. premere i per inserire

- Inserire come esempio (tra ip e hostname è presente uno spazio)
- Nell'esempio vengono usati 10.10.10.10 e testexample.csc.edu

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
172.20.116.24  cm90assu
10.10.10.10 testexample.csc.edu
```

Passaggio 5. Riscoprire il Call Manager in seguito. Accedere a: Inventario>Gestione articoli>Infrastruttura>Applicazioni UC>Communications Server

Scenario due

Passaggio uno. Verificare che la ricerca inversa DNS (Domain Name Service) sia risolvibile tramite DNS per il dispositivo interessato.

Passaggio due. Individuare nuovamente il cluster di Gestione chiamate. Passare a: Inventario>Gestione articoli>Infrastruttura>Applicazioni UC>Communications Server

- Selezionare i Call Manager interessati e scegliere Nuova individuazione

Accesso alla radice

In questa sezione viene descritto come ottenere l'accesso radice completo per PCA

Passaggio 1. Accedere tramite SSH a PCA e usare la porta 26 come utente amministratore

Passaggio 2. Input. **root_enable**

Digitare la password root desiderata

Passaggio 3. Input. **root** e digitare la password root

Passaggio 4. Dopo aver eseguito il login come input radice. **/opt/emms/emsam/bin/enableRoot.sh**

Passaggio 5. Input. **passwd** e immettere nuovamente la password root

A questo punto, è possibile chiudere la sessione SSH e accedere nuovamente direttamente come utente root