Dubbele endpoints voor Cisco Prime Collaboration Assurance (PCA)

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Prime Collaboration Assurance Duplicaat kunt oplossen.

Bijgedragen door Joseph Koglin, Cisco TAC Engineer

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van de inventarisatiemodule en de activiteiten binnen Prime Assurance
- Basisbeginselen van Linux

Dit document vereist dat deze configuratie wordt uitgevoerd:

- Volledige toegang tot voet is nodig - Als u geen worteltoegang hebt, raadpleeg dan de Onderste sectie Benoemde Root Access
- De Prime Assurance-toepassing is geïnstalleerd en u hebt endpoints in het voorraadsysteem gedupliceerd. Ex. Twee eindpunten met dezelfde naam: SEPAA11B22C3-software

> Opmerking: De in dit artikel uiteengezette operaties zijn databanken die van invloed zijn, zodat deze stappen alleen onder deskundige begeleiding dienen te worden uitgevoerd. Met name in PCA 12.1, aangezien de inventarisfunctionaliteit is herzien, mag de eis van deze stappen niet worden gesteld, maar kan deze worden beschouwd als een laatste oplossing onder toezicht van deskundigen.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Prime Assurance opdrachtregel-interface
- Prime Assurance-voorraadmodule
- Alle van toepassing zijnde softwareversies
- Geen hardwarevereisten vereist

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt

Probleem

Cisco Prime Assurance - dubbele telefoons

Dit document is voor omgevingen die telefoons hebben gedupliceerd in het systeem of scenario's waarin een verwijdering en opnieuw toevoegen van de eindpunten van toepassing is.

Dit proces verwijdert alle telefoons en voegt deze daarna weer toe.

Oplossing

Stap 1. Meld u aan bij PCA via Secure Shell (SSH) als wortel en poort 26

Stap 2. Invoer. **cd/opt/emms/emsam/bin/bin**

Stap 3. U stopt nu de services met de ingang. **./cpcmcontrol.sh**

Stap 4. U gaat nu controleren om er zeker van te zijn dat alle services niet bij de Input zijn **ingediend. ./cpcmcontrol.sh status**

- Als alle services zijn gezakt, ga dan naar de volgende stap

Stap 5. U start nu alleen de Database Service via de Input. **./start_db.sh**

Stap 6 en Stap 7 zullen de telefoons uit de database verwijderen. In stap 11 brengt u ze terug in het systeem

Stap 6. Invoer. **./refreshCDT.sh** (wacht tot deze voltooid is)

Stap 7. Invoer. **./refreshPhone.sh** (wacht tot deze voltooid is)

Stap 8. U brengt nu de services weer omhoog met de Input. **./cpcmcontrol.sh opnieuw.**

(**./cpcmcontrol.sh status** periodiek uitvoeren om er zeker van te zijn dat alle services back-ups maken)

Stap 9. Wanneer de handleiding een back-up maakt van login als de mondiale gebruiker en een clustergegevensontdekking doet als de volgende stap.

Stap 10. Daarna voert u een Cluster gegevensontdekking uit: **Navigator** to **Inventory>Tijdschema inventaris>Cluster gegevensontdekking.**

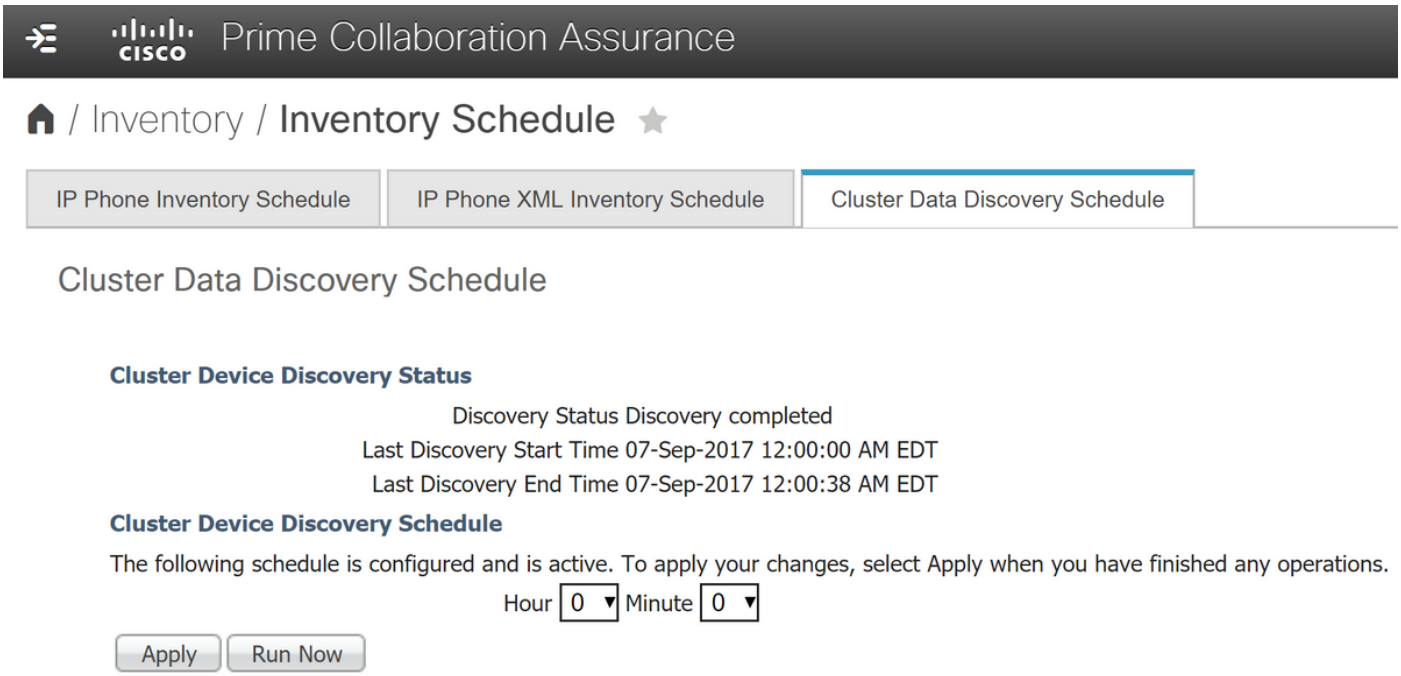
Stap 1. Selecteer **Nu uitvoeren** (deze stap haalt de telefoons terug)

Stap 12. Wacht tot het klaar is en de telefoons moeten terug zijn en geen duplicaten hebben.

Opmerking: Deze ontdekking is afhankelijk van het aantal endpoints in uw cluster en de tijd

tot voltooiing kan variëren

Bijvoorbeeld: u kunt de begin- en eindtijd vergelijken en deze specifieke tijd zien duurt slechts 38 seconden om te voltooien.



Opmerking: Voor informatiedoeleinden zal PCA de telefoons via Real-time Information Service (RIS) en Administration Extensible Markup Language (AXL) ophalen van de Cisco Unified Communications Manager (CUCM)-uitgever

Handige logbestanden als er zich problemen voordoen:

Indien u nog steeds duplicaten tegenkomt, raadpleegt u de genoemde stammen om te bekijken

Opmerking: Volle Root Access is vereist, indien u dit niet hebt, raadpleegt u de sectie Root Access. Zodra de volledige toegang van de root is geactiveerd, kunt u een programma gebruiken zoals Winscp om poort 26 en de basisgebruikersreferenties aan te sluiten en te gebruiken.

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

RISCollected.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 <— dit zal u weten of er problemen waren met de draaiende scriptsring

Aanvullende opmerkingen over probleemoplossing en achtergrondinformatie:

U kunt ook willen zien of u de RIS-service in de Call Manager-cluster kunt hervatten omdat dit een aantal verschillen of problemen kan oplossen.

Wanneer de telefoons in crm worden verzameld zal het axl+ris gebruiken, dus als u problemen hebt, kunt u de RIS-service in het systeem opnieuw starten.

Er zal geen impact op het bedrijfsleven zijn wanneer u de RIS-dienst opnieuw start in het cluster, waar een herstart van de AXL-dienst niet wordt aanbevolen tijdens de uren waarop de dienst wordt uitgevoerd.

Daarnaast hoeft u de AXL-service zelden opnieuw te starten voordat u dit doet. Ik verwijs naar de logbestanden om te zien of een herstart nodig is.

Zorg er ook voor dat de Call Manager's worden beheerd en dat in het CSM onder System>Server de cucm uitgever hostname/ip kan worden ingepingbaar en opgelost.

Aangezien u in een case kunt lopen waar u de Call Manager hebt ontdekt en beheerd als de ip, echter in het System>Server van de Call Manager wordt deze aangegeven door hostname.

Wat er gebeurt is dat wanneer PCA de telefoons via axl+ris verzamelt, deze lijst zal worden opgenomen onder System>server, dus als u de naam van de hostname hebt en de telefoon niet kan worden opgelost, dan ontvangt u deze telefoons nooit, zelfs niet als het algoritme wordt beheerd omdat het door ip wordt beheerd.

Dit scenario wordt op twee manieren vastgesteld:

Scenario One

Stap 1. Meld u aan bij PCA via SSH-basisgebruiker en poort 26

Stap 2. **Cd/etc**

Stap 3. **Vi-hosts**

Stap 4. Druk op **i** voor invoegen

- Inzetten als voorbeeld (er is een ruimte tussen ip en hostname)
- In dit voorbeeld wordt 10.10.10.10 en testvoorbeeld.csc.edu gebruikt.

```
# 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
```

Stap 5. Ontvang uw Call Manager later. Navigeren in: inventaris>voorraadbeheer>Infrastructuur>UCS-toepassingen>Communicatieserver

Scenario Twee

Stap één. Zorg ervoor dat de omgekeerde raadpleging van de Naam (DNS) door dns voor het getroffen apparaat kan worden opgelost.

Stap twee. Ontdek de Cluster van Call Manager. Navigeer aan: **inventaris>voorraadbeheer>Infrastructuur>UCS-toepassingen>Communicatieserver**

- Selecteer de getroffen Call Managers en selecteer Opnieuw ontdekken

Root Access

In dit deel wordt beschreven hoe u volledige Root Access voor PCA kunt verkrijgen

Stap 1. Meld u aan bij SSH en gebruikt u poort 26 als beheerder.

Stap 2. Voer de informatie in. **wortel_enabled**

Typ het gewenste hoofdwachtwoord

Stap 3. Invoer. **wortel** en type in het hoofdwachtwoord

Stap 4. Na inloggen als wortelingang. **/opt/emms/emsam/bin/enableRoot.sh**

Stap 5. Invoer. ingestuurd en opnieuw ingevoerd in het basiswachtwoord

U dient nu de SSH-sessie te kunnen sluiten en direct als root opnieuw te kunnen inloggen