So lösen Sie doppelte Endgeräte mit Cisco Prime Collaboration Assurance (PCA) auf

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Cisco Prime Collaboration Assurance Duplicate Endpoints (doppelte Endgeräte) aufgelöst werden kann.

Unterstützt von Joseph Koglin, Cisco TAC Engineer

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis des Bestandsmoduls und seiner Betriebsabläufe innerhalb von Prime Assurance
- Grundlegende Linux-Grundlagen zu Prime Assurance

In diesem Dokument muss diese Konfiguration implementiert werden:

- Vollständiger Root-Zugriff ist erforderlich - Wenn Sie keinen Root-Zugriff haben, lesen Sie im unteren Abschnitt "Named Root Access" (Root-Zugriff) nach.
- Die Prime Assurance-Anwendung ist installiert, und Sie haben duplizierte Endpunkte im Inventory System. Beispiel: Zwei Endpunkte mit demselben Namen: SEPAA11BB22CC3

> **Hinweis**: Die in diesem Artikel beschriebenen Vorgänge wirken sich auf die Datenbank aus, daher sollten diese Schritte nur in fachkundiger Anleitung ausgeführt werden. Insbesondere bei PCA 12.1 sollte die Anforderung dieser Schritte nicht erfüllt werden, da die Inventarfunktionalität überholt wurde, sondern als letztes Mittel unter fachkundiger Aufsicht betrachtet werden können.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Prime Assurance-Befehlszeilenschnittstelle
- Prime Assurance-Bestandsmodul
- Alle Softwareversionen

- Keine Hardware-Anforderungen erforderlich

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines beliebigen Befehls verstehen.

Problem

Cisco Prime Assurance - Doppelte Telefone

Dieses Dokument ist für Umgebungen mit duplizierten Telefonen im System bzw. Szenarien vorgesehen, in denen ein Entfernen und erneutes Hinzufügen der Endgeräte möglich ist.

Bei diesem Vorgang werden alle Telefone entfernt und anschließend erneut hinzugefügt.

Lösung

Schritt 1: Anmeldung bei PCA über Secure Shell (SSH) als Root und Port 26

Schritt 2: Eingabe. **cd /opt/emms/emsam/bin/**

Schritt 3: Beenden Sie jetzt Dienste mit der Eingabe. **./cpcmcontrol.sh anhalten**

Schritt 4: Überprüfen Sie nun, ob alle Services am Eingang nicht verfügbar sind. **./cpcmcontrol.sh**

- Sobald alle Services außer Betrieb sind, fahren Sie mit dem nächsten Schritt fort.

Schritt 5: Sie starten nun nur noch den Datenbankdienst durch Eingabe. **./start_db.sh**

In Schritt 6 und Schritt 7 werden die Telefone aus der Datenbank entfernt. In Schritt 11 bringen Sie sie wieder in das System ein.

Schritt 6: Eingabe. **./refreshCDT.sh** (Warten Sie, bis der Vorgang abgeschlossen ist)

Schritt 7: Eingabe. **./refreshPhone.sh** (Warten Sie, bis der Vorgang abgeschlossen ist)

Schritt 8: Jetzt stellen Sie die Services mit den Eingaben wieder her. **./cpcmcontrol.sh starten**

(**./cpcmcontrol.sh** regelmäßig ausführen, um sicherzustellen, dass alle Services wieder verfügbar sind)

Schritt 9: Wenn die GUI wiederhergestellt wird, melden Sie sich als globaler Admin-Benutzer an, und führen Sie als nächsten Schritt eine Cluster-Datenerkennung durch.

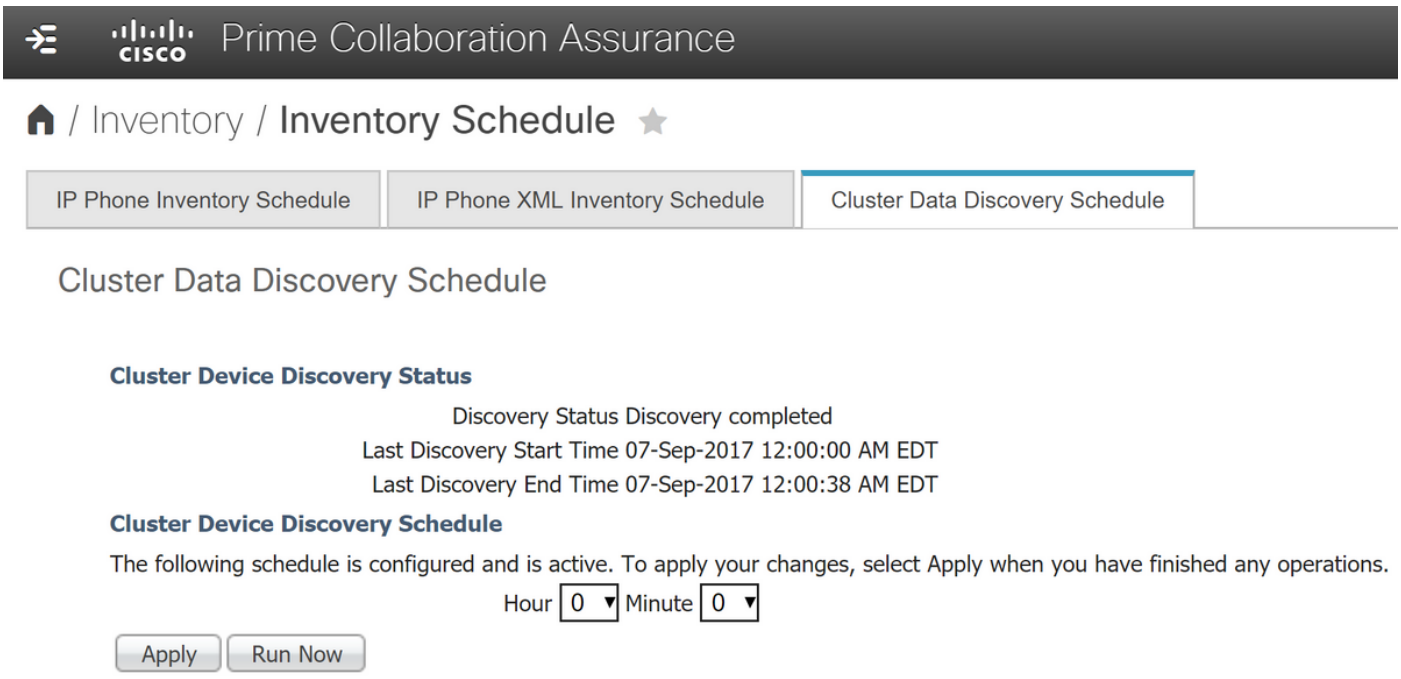
Schritt 10: Als Nächstes führen Sie eine Cluster-Datenerkennung durch: Navigieren Sie zu **Inventory > Inventory Plan > Cluster Data Discovery.**

Schritt 11: Wählen Sie **Jetzt ausführen** (Dieser Schritt ruft die Telefone zurück) aus.

Schritt 12: Warten Sie, bis der Vorgang abgeschlossen ist, und die Telefone sollten wieder zurück sein und keine Duplikate haben.

Hinweis: Diese Erkennung hängt von der Anzahl der Endpunkte in Ihrem Cluster ab und die Zeit bis zur Fertigstellung kann variieren.

Zum Beispiel können Sie die Start- und Endzeit vergleichen und sehen, dass dieser Vorgang nur 38 Sekunden dauerte.



Hinweis: Zu Informationszwecken ruft PCA die Telefone über den Real-Time Information Service (RIS) und die Administrative Extensible Markup Language (AXL) vom Cisco Unified Communication Manager (CUCM) Publisher ab.

Nützliche Protokolle, wenn Probleme auftreten:

Wenn weiterhin Duplikate auftreten, lesen Sie die Protokolle, die erwähnt wurden.

Hinweis: Vollständiger Root-Zugriff ist erforderlich. Falls Sie nicht über diese Option verfügen, lesen Sie den Abschnitt Root Access. Wenn der vollständige Root-Zugriff aktiviert ist, verwenden Sie ein Programm wie Winscp, um Port 26 und die Root-Benutzeranmeldeinformationen zu verbinden und zu verwenden.

/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 <— dieses Dialogfeld lässt Sie ob Probleme mit den ausgeführten Skripten aufgetreten sinding

Weitere Hinweise zur Fehlerbehebung und Hintergrundinformationen:

Sie können auch prüfen, ob Sie den RIS-Dienst im Call Manager-Cluster neu starten können, da dadurch einige Unstimmigkeiten oder Probleme behoben werden können.

Wenn die Telefone in CUCM gesammelt werden, verwendet es axl+ris, sodass Sie bei Problemen den RIS-Dienst in CUCM möglicherweise neu starten möchten.

Wenn Sie den RIS-Service im Cluster neu starten, sind keine geschäftlichen Auswirkungen zu erwarten. Ein Neustart des AXL-Service wird während der Geschäftszeiten nicht empfohlen.

Außerdem müssen Sie den AXL-Dienst nur selten neu starten. Bevor ich dies tue, würde ich in den Protokollen nachsehen, ob ein Neustart erforderlich ist.

Stellen Sie außerdem sicher, dass die Call Manager verwaltet werden und dass der cucm Publisher-Hostname/IP unter System>Server in cucm pingbar und auflösbar ist.

Da Sie möglicherweise auf einen Fall stoßen, in dem Sie den Call Manager als IP erkannt und verwaltet haben, wird er im System>Server des Call Managers unter Hostname aufgeführt.

Wenn PCA die Telefone über axl+ris sammelt, wird sie jedoch unter System>Server aufgelistet. Wenn Sie sie also als Hostname aufgelistet haben und sie nicht über pca auflösbar sind, werden Sie diese Telefone nie erhalten, auch wenn der CUCM verwaltet wird, weil er von ip verwaltet wurde.

Dieses Szenario kann auf zwei Arten behoben werden:

Szenario 1

Schritt 1: Anmeldung bei PCA über SSH-Root-Benutzer und Port 26

Schritt 2: **Cd /etc**

Schritt 3: **Vi-Hosts**

Schritt 4: Drücken Sie **i** zum Einfügen.

- Als Beispiel einfügen (zwischen IP und Hostname gibt es einen Leerzeichen)
- In diesem Beispiel werden 10.10.10.10 und testexample.csc.edu verwendet.

```
# 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
```

Schritt 5: Ermitteln Sie anschließend erneut Ihren Call Manager. Navigieren Sie zu: Inventory > Inventory Management > Infrastructure > UC Applications > Communications Server

Szenario 2

Schritt 1: Stellen Sie sicher, dass die umgekehrte Suche des Domanin Name Service (DNS) für das betroffene Gerät über DNS aufgelöst werden kann.

Schritt zwei: Erkennen Sie das Call Manager-Cluster erneut. Navigieren Sie zu: **Inventory >**

Inventory Management > Infrastructure > UC Applications > Communications Server

- Wählen Sie die betroffenen Call Manager aus, und wählen Sie Neu erkennen aus.

Root-Zugriff

In diesem Abschnitt wird beschrieben, wie Sie vollständigen Root Access für PCA erhalten.

Schritt 1: Melden Sie sich über SSH bei PCA an, und verwenden Sie Port 26 als Admin-Benutzer.

Schritt 2: Eingabe. **root_enable**

Geben Sie das gewünschte Root-Kennwort ein.

Schritt 3: Eingabe. **root** und das root-Passwort eingeben

Schritt 4: Nach der Anmeldung als root Input. **/opt/emms/emsam/bin/enableRoot.sh**

Schritt 5: Eingabe. **Kennwort** eingeben und erneut Ihr root-Kennwort eingeben

Sie sollten jetzt die SSH-Sitzung schließen und sich direkt als root erneut anmelden können.