How to Resolve Cisco Prime Collaboration Assurance (PCA) Duplicate Endpoints

Contents

Introduction

This document describes how to Resolve Cisco Prime Collaboration Assurance Duplicate Endpoints.

Contributed by Joseph Koglin, Cisco TAC Engineer

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of the Inventory Module and it's operations within Prime Assurance
- Basic Linux fundamentals regarding Prime Assurance

This document requires this configuration to be implemented:

- Full Root access will be needed - If you do not have root access please refer to the Bottom Section Named Root Access
- The Prime Assurance application is installed and you have duplicated endpoints in the Inventory System. Ex. Two endpoints with the same name: SEPAA11BB22CC3

> **Note**: The operations explained in this article are database impacting, hence these steps should be carried out only in expert guidance. In PCA 12.1 specifically, since inventory functionality has been overhauled, the requirement of these steps should not happen but can be considered as a last remedy under expert supervision.

Components Used

The information in this document is based on these software versions:

- Prime Assurance Command Line Interface
- Prime Assurance inventory Module
- All software versions applicable
- No hardware requirements required

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

Problem

Cisco Prime Assurance - Duplicate Phones

This document is for environments that have duplicated phones in the system or scenarios where a remove and re-add of the endpoints is applicable.

This process will remove all phones and after that the process re-add them back

Solution

Step 1. Log in into PCA via Secure Shell (SSH) as root and port 26

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

Step 3.Now you will stop services with the Input. **./cpcmcontrol.sh stop**

Step 4. You will now check to ensure all services are down by the Input. **./cpcmcontrol.sh status**

- Once all services are down go to next step

Step 5. You will now start only the Database service by the Input. **./start_db.sh**

Step 6 and Step 7 will remove the phones from the Database, In step 11 you will bring them back into the system

Step 6. Input. **./refreshCDT.sh** (wait till it completes)

Step 7. Input. **./refreshPhone.sh** (wait till it completes)

Step 8. Now you will bring the services back up with the Input. **./cpcmcontrol.sh restart**

(perform **./cpcmcontrol.sh status** periodically to ensure all services come back up)

Step 9. When the gui comes back up log in as the globaladmin user and do a cluster data discovery as the next step.

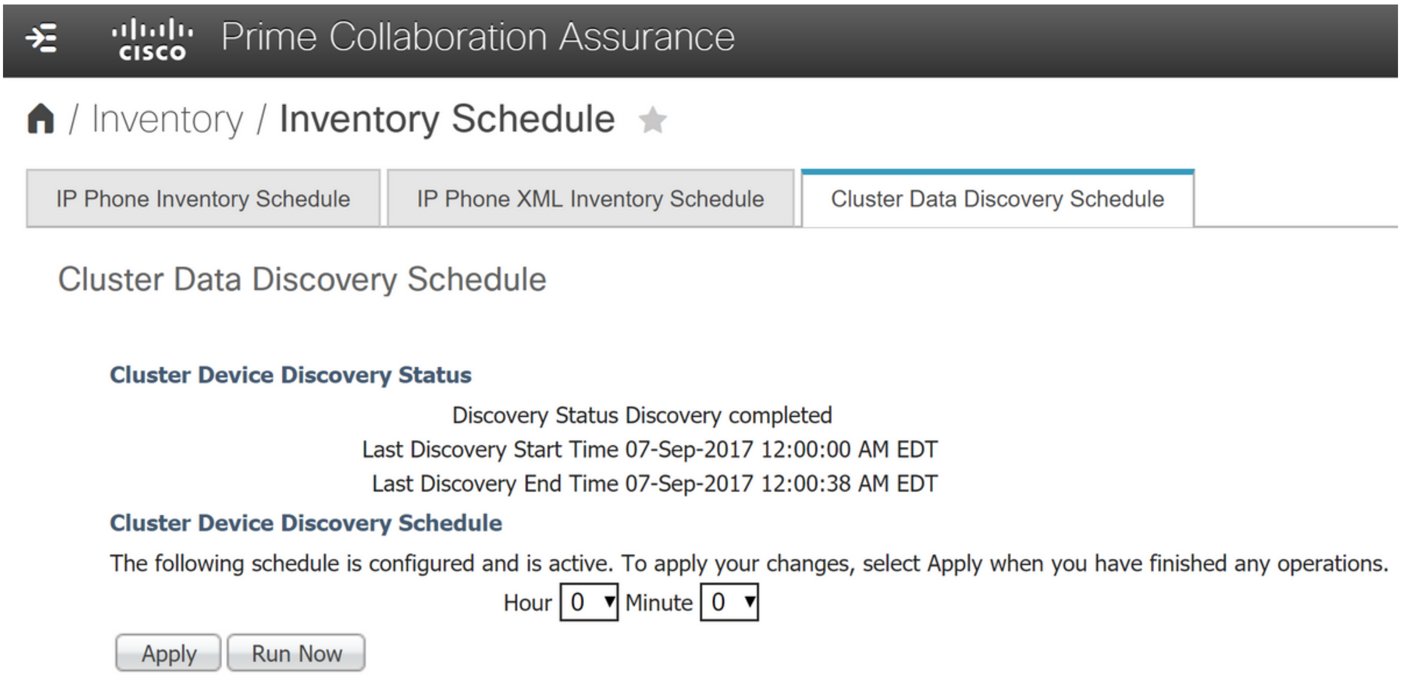
Step 10. Next you will perform a Cluster data discovery: Navigateto **Inventory>Inventory schedule>Cluster data discovery.**

Step 11. Select **Run now** (This step will retrieve back the phones)

Step 12. Wait until it is finished and the phones should be back and have no duplicates.

> **Note**: This discovery is dependant on the number of endpoints in your cluster and the time to completion may vary

For example purposes you can compare the start and end time and see this particular one only took 38 seconds to complete.


Prime Collaboration Assurance
/ Inventory / Inventory Schedule
IP Phone Inventory Schedule
IP Phone XML Inventory Schedule
Cluster Data Discovery Schedule

Cluster Data Discovery Schedule

Cluster Device Discovery Status

Discovery Status Discovery completed
Last Discovery Start Time 07-Sep-2017 12:00:00 AM EDT
Last Discovery End Time 07-Sep-2017 12:00:38 AM EDT

Cluster Device Discovery Schedule

The following schedule is configured and is active. To apply your changes, select Apply when you have finished any operations.

Hour 0 Minute 0

> **Note**: For informational purposes PCA will retrieve the phones via Real-time Information Service (RIS) and Administrative Extensible Markup Language (AXL) from the Cisco Unfied Communication Manager (CUCM) Publisher

Useful logs if any issues are encountered:

If you still are encountering duplicates please refer to the logs mentioned to review

> **Note**: Full Root access will be needed, if you do not have please refer to the section Root Access. Once full root access is enabled please use a program such as Winscp to connect and use port 26 and the root user credentials.

/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 <-- this will let you know if there were any issues with the scripts running

Further troubleshooting Notes and Background information:

You may also want to see if you can restart the RIS service in the Call Manager cluster as this can clear up some discrepancies or issues.

When the phones are collected in cucm it will use axl+ris, so if you have issues you may want to restart the RIS service in cucm.

There will be no business impact when you restart the RIS service in the cluster, where-as a restart of the AXL service is not recommended during business hours.

Additionally rarely will you need to restart the AXL service so before doing so I would refer to the logs to see if a restart is necessary.

Also ensure the Call Manager's are managed and in cucm under System>Server the cucm publisher hostname/ip is pingable and resolvable.

As you may run into a case where you discovered and managed the Call Manager as the ip, however in the Call manager's System>Server it is listed by hostname.

What happens is when PCA collects the phones via axl+ris it will list however it is listed under System>server so if you have it listed as the hostname and it is not resolvable by pca then you will never receive these phones even if the cucm is managed because it was managed by ip.

This scenario is fixed by two ways:

Scenario One

Step 1. Login into PCA through SSH root user and port 26

Step 2. **Cd /etc**

Step 3. **Vi hosts**

Step 4. press **i** for insert

- Put in as an example (there is a space in between ip and hostname)
- In this example 10.10.10.10 and testexample.csc.edu is being used.

```
# 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
```

Step 5. Rediscover your Call Manager afterwards. Navigate to: Inventory>Inventory Management>Infrastructure>UC Applications>Communications Server

Scenario Two

Step one. Ensure the Domanin Name Service (DNS) reverse lookup is resolvable through dns for the affected device.

Step two. Rediscover the Call Manager Cluster. Navigate to: **Inventory>Inventory Management>Infrastructure>UC Applications>Communications Server**

- Select the affected Call Managers and select Rediscover

Root Access

This section describes how to obtain full Root Access for PCA

Step 1. Log in through SSH to PCA and use port 26 as the Admin User

Step 2. Input. **root_enable**

Type in the root password you want

Step 3. Input. **root** and type in the root password

Step 4. Once logged in as root Input. **/opt/emms/emsam/bin/enableRoot.sh**

Step 5. Input. **passwd** and re-enter in your root password

You now should be able to close the SSH session and re-log in directly as root