Upgrade PCA Deployment Model

Contents

Prime Collaboration Assurance (PCA) - Upgrade Your Deployment Model

Introduction

This Document describes how to upgrade your Prime Collaboration Assurance (PCA) deployment Model

Contributed by Joseph Koglin, TAC Engineer

This procedure should be used only for upgrading depolyment model and not for any other purposes.

Prerequisites

Requirements

- Knowledge of PCA
- Access to edit the PCA Virtual Machine (VM) hardware settings
- PCA Root access
- If upgrading to a Very Large deployment, a remote ftp/sftp server is needed

Components Used

The information in this document is related to all current PCA Versions

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, make sure that you understand the potential impact of any command.

Problem

You are near or at max system capaicty which can cause:

- System performance issues such as your, opt to reach 100% or services crashing consistently.
- You are not able to deploy anymore endpoints per your Open Virtualization Format (OVA) and need a larger one.

Solution

Upgrade Small and Medium OVA's

Step 1. Please refer to the virtualization support guide for your version, in order to determine the extra resources needed.

PCA Version Specific OVA Reuirements

Step 2. Although there have been no reported issues, it is always best to create a backup.

Option 1

Take a Virtual Machine (VM) Snapshot

Step 1. Log in to Vsphere as an admin user.

Step 1. Right-click on the VM in Vsphere.

Step 2. Select **Snapshot>>Take Snapshot.** Check the status at the bottom of Vsphere window to monitor completion.

Or

Option 2

Take a PCA Backup

Step 1. Navigate to **System Administration>>Backup Settings>> Select New.** Provide the required information based on your needs, i.e. if you want just the assurance data or assurance and analytics. Once the backup is complete, proceed to the next step.

> **Note**: If you utilize PCA 12.x, navigate to **https://PCA_IP_HERE:7443** and log in with globaladmin. From there, navigate to **Maintenance>Backup** and select **New**. Provide the information required.

Step 3. Log in to PCA Command Line Interface (CLI) as root and use port 26.

Step 4. Enter **/opt/emms/emsam/bin/cpcmcontrol.sh stop.**

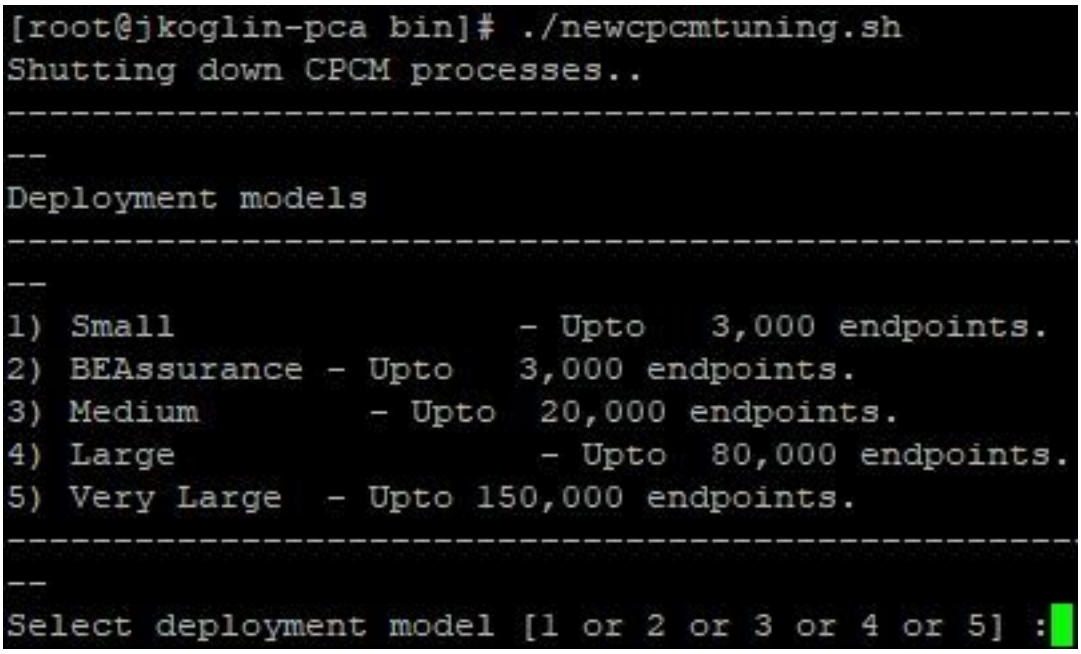
Step 5. Navigate to you PCA VM and power down the VM.

Step 6. Right-click and Edit the VM settings in order to add the additional resources.

Step 7. Right-click in order to Power back on the VM. Wait 15 minutes.

Step 8. Log in to PCA as root and use port 26.

Step 9. Enter **/opt/emms/emsam/bin/newcpcmtuning.sh.**



Sep 10. Select the deployment model you wish to upgrade to. After the script finishes, the services restart.

> **Note**: If you currently use a Small deployment, you upgrade to Medium or Large. If you use a Medium deployment, you upgrade to large.

Upgrade A Large OVA to a Very Large

Take a PCA Backup

Step 1. Log in to your PCA using your globaladmin User.

Step 2. Navigate to**System Administration>>Backup Settings>>** Select **New**and provide the needed information for the analytics backup.

> **Note**: If using PCA 12.x, type in your browser **https://PCA_IP_HERE:7443** and log in with the globaladmin user. From there, navigate to **Maintenance>Backup** and select **New**, provide the information and ensure it completes for the analytics backup.

Step 3. Please refer to the virtualization support guide for your version, in order to determine the extra resources needed.

PCA Version Specific OVA Reuirements

Step 4. Log in to PCA Command Line Interface (CLI) as root using port 26 (call this the App VM).

Step 5. Enter **/opt/emms/emsam/bin/cpcmcontrol.sh stop.**

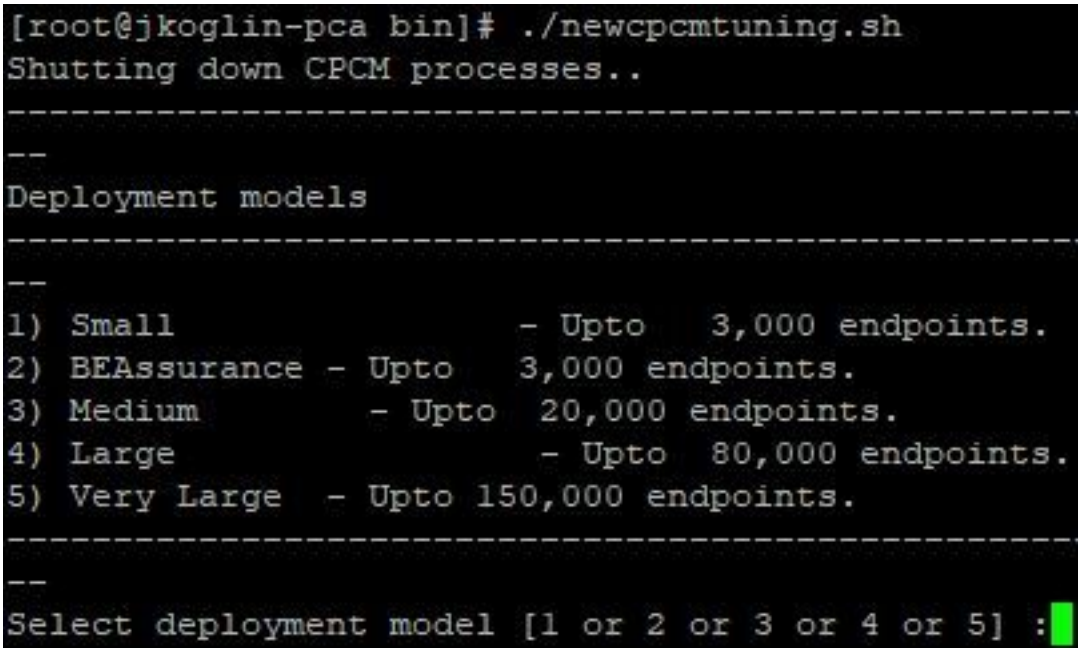
Step 6. Navigate to you PCA VM and power down the VM.

Step 7. Right-click and Edit the VM settings to add in the additional resources.

Step 8. Right-click in order to Power back on the VM. Wait 15 minutes.

Step 9. Log in to PCA as root and use port 26.

Step 10. Enter **/opt/emms/emsam/bin/newcpcmtuning.sh.**



Step 11. Select Option 5, the services restart again.

Step 12. Download the Cisco Prime Collaboration Assurance and Analytics Very Large OVA file and deploy a PCA Database Server. Take note of the IP address as it is used in a later step.

> **Note**: Enter the IP adress, when asked for the Application IP during the deployment of the database server.

Step 13. On the App VM, log in as the root user into CLI and use port 26.

Step 14. Run the command **/opt/emms/emsam/advance_reporting/bin/enableAnalyticsWithRemoteDB.sh** and point this server to the database Server just created.

Step 15. After the command completes, restore your analytics data on the new database server

Do not use above procedure for any other purpose than upgrading a Large depolyment to Very Large.

Restore your Analytics Data for the Very Large Deployment

PCA 11.x

Step 1. Transfer your analytics backup to your ftp/sftp server.

Step 2. Log in to the Cisco Prime Collaboration Assurance Database server with the account that you created during installation. The default login is admin.

Enter the commands in order to create a repository on FTP server:

```
admin# config t
admin(config)# repository RepositoryName
admin(config-Repository)# url ftp://ftpserver/directory
admin(config-Repository)# user UserName password {plain | hash} Password
admin(config-Repository)# exit
admin(config)# exit
```

Where:

- RepositoryNameis the location to which files must be backed up. This name can contain a maximum of 30 alphanumeric characters.
- ftp://ftpserver/directoryis the FTP server and the directory on the server to which the file is transferred. You can also use SFTP, HTTP, or TFTP instead of FTP.
- *UserName*and {`plain`|`hash`}*Password*are the username and password for the FTP, SFTP, or TFTP server. H`ash`specifies an encrypted password, and plainspecifies an unencrypted plain text password.

For example:

```
admin# config t
admin(config)# repository tmp
admin(config-Repository)# url ftp://ftp.cisco.com/incoming
admin(config-Repository)# user john password plain john!23
admin(config-Repository)# exit
admin(config)# exit
```

Step 3. List the Repository Data. You can list the data within a repository. Log in to the Cisco Prime Collaboration server as*admin*and run this command:

```
admin# show repository RepositoryName
For example:
admin# show repository myftp
assurance_Sun_Feb_09_14_20_30_CST_2018.tar.gpg
```

This ensures PCA is able to read the backup file on your remote ftp/sftp server

Step 4. To restore the data, log in to the Cisco Prime Collaboration application server as*admin*through VM console and use the vSphere client. Do not trigger the restore from SSH/Putty prompt.

```
admin# restore Backupfilename repository RepositoryName application cpcm
```

Where,*Backupfilename*is the name of the backup file suffixed with the timestamp (*YYMMDD-HHMM*) and file extension .tar.gpg.

For example, to restore on the ftp server:

```
admin# restore assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg repository myftp application cpcm
```

PCA 12.x

To restore the data:

Step 1. Type in your browser https://PCA_IP_HERE:7443 and log in with the globaladmin user.

Step 2. Navigate to **Maintenance>Restore** and enter the ftp/sft information.

Set Your Root User

PCA 11.x

Step 1.Log in to the PCA through CLI as the Admin User created from install.

Step 2. Run the command:**root_enable.**

Step 3. Enter in your root password.

Step 4. Logged in as admin, enter in root and enter in your root password to gain access to root.

Step 5. Run the command: **/opt/emms/emsam/bin/enableRoot.sh.**

Step 6. Enter **passwd** and re-enter in your same root password.

PCA 12.x

Step 1. Type in your browser **https://PCA_IP_HERE:7443 and log in as globaladmin**

Step 2. Select Root Access

Step 3. Select Enable and enter your root credentials.Click **Submit.**

Root Access	Enable ▾
New Password	Enter New Password
Confirm New Password	Enter Confirm New Password

Submit

*** Root Access will be Enabled now**

*** Password Reset will terminate the current active sessions**