Upgrade des PCA-Bereitstellungsmodells

Inhalt

Prime Collaboration Assurance (PCA) - Upgrade Ihres Bereitstellungsmodells

Einführung

In diesem Dokument wird beschrieben, wie Sie ein Upgrade Ihres Prime Collaboration Assurance (PCA)-Bereitstellungsmodells durchführen.

Mitarbeiter: Joseph Koglin, TAC Engineer

Dieses Verfahren sollte nur für die Aktualisierung des Bereitstellungsmodells und nicht für andere Zwecke verwendet werden.

Voraussetzungen

Anforderungen

- Kenntnisse des PCA
- Zugriff zur Bearbeitung der Hardwareeinstellungen für PCA Virtual Machine (VM)
- PCA-Root-Zugriff
- Bei einem Upgrade auf eine sehr große Bereitstellung ist ein Remote-FTP/SFTP-Server erforderlich.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf alle aktuellen PCA-Versionen.

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 Befehls verstehen.

Problem

Sie befinden sich in der Nähe oder haben maximal Systemkapazität, was Folgendes verursachen kann:

- Systemleistungsprobleme wie Ihr, 100 % erreichen oder Services stürzen konsistent ab.
- Sie können keine Endgeräte mehr pro OVA (Open Virtualization Format) bereitstellen und benötigen einen größeren.

Lösung

Upgrade von kleinen und mittleren OVAs

Schritt 1: Weitere Informationen zu den benötigten Ressourcen finden Sie im Leitfaden zur Virtualisierungsunterstützung für Ihre Version.

Versionsspezifische OVA-Anforderungen für PCA

Schritt 2: Obwohl keine Probleme gemeldet wurden, ist es immer am besten, eine Sicherung zu erstellen.

Option 1

Snapshot für ein virtuelles System (VM) erstellen

Schritt 1: Melden Sie sich als Administrator bei vSphere an.

Schritt 1: Klicken Sie mit der rechten Maustaste auf die VM in vSphere.

Schritt 2: Wählen Sie **Snapshot >>Snapshot erstellen aus.** Überprüfen Sie den Status unten im Fenster "vSphere", um die Fertigstellung zu überwachen.

oder

Option 2

PCA-Sicherung durchführen

Schritt 1: Navigieren Sie zu **Systemverwaltung >>Sicherungseinstellungen>> Neu auswählen.** Geben Sie die erforderlichen Informationen basierend auf Ihren Anforderungen an, z. B. wenn Sie nur die Assurance- oder Assurance- und Analysedaten benötigen. Wenn die Sicherung abgeschlossen ist, fahren Sie mit dem nächsten Schritt fort.

> **Hinweis**: Wenn Sie PCA 12.x verwenden, navigieren Sie zu **https://PCA_IP_HERE:7443** und melden Sie sich mit globaladmin an. Navigieren Sie von dort zu **Maintenance > Backup** und wählen Sie **New** aus. Geben Sie die erforderlichen Informationen an.

Schritt 3: Melden Sie sich bei der PCA-Befehlszeilenschnittstelle (CLI) als Root an, und verwenden Sie Port 26.

Schritt 4: Geben Sie **/opt/emms/emsam/bin/cpcmcontrol.sh stop ein.**

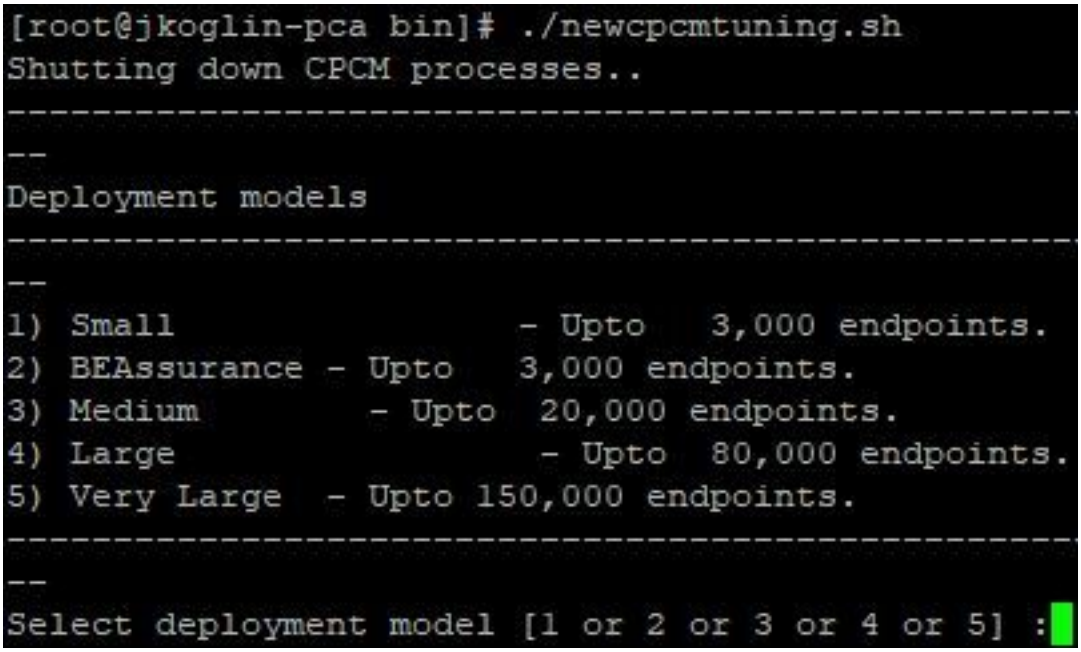
Schritt 5: Navigieren Sie zu Ihrem PCA VM, und schalten Sie das virtuelle System aus.

Schritt 6: Klicken Sie mit der rechten Maustaste, und bearbeiten Sie die VM-Einstellungen, um die zusätzlichen Ressourcen hinzuzufügen.

Schritt 7: Klicken Sie mit der rechten Maustaste, um das virtuelle System wieder einzuschalten. Warten Sie 15 Minuten.

Schritt 8: Melden Sie sich bei PCA als Root an, und verwenden Sie Port 26.

Schritt 9: Geben Sie **/opt/emms/emsam/bin/newcpcmtuning.sh ein.**



10. September Wählen Sie das Bereitstellungsmodell aus, auf das Sie ein Upgrade durchführen möchten. Nach Abschluss des Skripts wird der Dienstneustart durchgeführt.

> **Hinweis**: Wenn Sie derzeit eine kleine Bereitstellung verwenden, aktualisieren Sie auf Mittel oder Groß. Wenn Sie eine mittelgroße Bereitstellung verwenden, aktualisieren Sie auf groß.

Upgrade einer großen OVA auf eine sehr große OVA

PCA-Sicherung durchführen

Schritt 1: Melden Sie sich mit Ihrem global-admin-Benutzer bei Ihrem PCA an.

Schritt 2: Navigieren Sie **zuSystemverwaltung >>Sicherungseinstellungen>>** Wählen SieNeu, und stellen Sie die erforderlichen Informationen für die Analyse-Sicherung bereit.

> **Hinweis**: Wenn Sie PCA 12.x verwenden, geben Sie Ihren Browser

https://PCA_IP_HERE:7443 ein und melden Sie sich bei dem globalen Administrator-Benutzer an. Navigieren Sie von dort zu **Maintenance > Backup**, und wählen Sie **New aus**, stellen Sie die Informationen bereit und stellen Sie sicher, dass sie für die Analyse-Sicherung vollständig sind.

Schritt 3: Weitere Informationen zu den benötigten Ressourcen finden Sie im Leitfaden zur Virtualisierungsunterstützung für Ihre Version.

Versionsspezifische OVA-Anforderungen für PCA

Schritt 4: Melden Sie sich mit Port 26 bei der PCA Command Line Interface (CLI) als Root an (nennen Sie dies das App VM).

Schritt 5: Geben Sie **/opt/emms/emsam/bin/cpcmcontrol.sh stop ein.**

Schritt 6: Navigieren Sie zu Ihrem PCA VM, und schalten Sie das virtuelle System aus.

Schritt 7: Klicken Sie mit der rechten Maustaste, und bearbeiten Sie die VM-Einstellungen, um die zusätzlichen Ressourcen hinzuzufügen.

Schritt 8: Klicken Sie mit der rechten Maustaste, um das virtuelle System wieder einzuschalten. Warten Sie 15 Minuten.

Schritt 9: Melden Sie sich bei PCA als Root an, und verwenden Sie Port 26.

Schritt 10: Geben Sie **/opt/emms/emsam/bin/newcpcmtuning.sh ein.**

```
[root@jkoglin-pca bin]# ./newcpcmtuning.sh
Shutting down CPCM processes..
------------------------------------------------
--
Deployment models
------------------------------------------------
--
1) Small              - Upto   3,000 endpoints.
2) BEAssurance - Upto   3,000 endpoints.
3) Medium         - Upto  20,000 endpoints.
4) Large                - Upto  80,000 endpoints.
5) Very Large   - Upto 150,000 endpoints.
------------------------------------------------
--
Select deployment model [1 or 2 or 3 or 4 or 5] :
```

Schritt 11: Wählen Sie Option 5 aus, um den Service erneut neu zu starten.

Schritt 12: Laden Sie die Cisco Prime Collaboration Assurance and Analytics Very Large OVA-Datei herunter, und stellen Sie einen PCA-Datenbankserver bereit. Notieren Sie sich die IP-Adresse, die in einem späteren Schritt verwendet wird.

Hinweis: Geben Sie die IP-Adresse ein, wenn Sie während der Bereitstellung des

Datenbankservers nach der Anwendungs-IP-Adresse gefragt werden.

Schritt 13: Melden Sie sich auf dem VM der App als Root-Benutzer bei der CLI an, und verwenden Sie Port 26.

Schritt 14: Führen Sie den Befehl **/opt/emms/emsam/advance_reporting/bin/enableAnalyticsWithRemoteDB.sh aus,** und verweisen Sie diesen Server auf den soeben erstellten Datenbankserver.

Schritt 15: Stellen Sie nach Abschluss des Befehls die Analysedaten auf dem neuen Datenbankserver wieder her.

Verwenden Sie die oben genannte Prozedur für keinen anderen Zweck, als das Upgrade einer Large-Depolyment auf Sehr Large.

Wiederherstellen der Analysedaten für eine sehr große Bereitstellung

PCA 11.x

Schritt 1: Übertragen Sie Ihre Analyse-Sicherung auf Ihren FTP-/SFTP-Server.

Schritt 2: Melden Sie sich mit dem Konto, das Sie während der Installation erstellt haben, beim Cisco Prime Collaboration Assurance-Datenbankserver an. Die Standardanmeldung lautet admin.

Geben Sie die Befehle ein, um ein Repository auf dem FTP-Server zu erstellen:

```
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
```

Wo:

- RepositoryGibt den Speicherort an, in dem Dateien gesichert werden müssen. Dieser Name darf maximal 30 alphanumerische Zeichen enthalten.
- ftp://ftpserver/directoryis Sie den FTP-Server und das Verzeichnis auf dem Server, auf den die Datei übertragen wird. Sie können auch SFTP, HTTP oder TFTP anstelle von FTP verwenden.
- UserName und {`clear`|`hash`}Kennwort sind Benutzername und Kennwort für den FTP-, SFTP- oder TFTP-Server. Hashgibt ein verschlüsseltes Kennwort an und gibt ein unverschlüsseltes Klartext-Kennwort an.

Beispiel:

```
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
```

Schritt 3: Listen Sie die Repository-Daten auf. Sie können die Daten in einem Repository auflisten. Melden Sie sich beim Cisco Prime Collaboration-Server-Administrator an, und führen Sie den folgenden Befehl aus:

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

Dadurch wird sichergestellt, dass PCA die Sicherungsdatei auf Ihrem FTP-/SFTP-Server lesen kann.

Schritt 4: Melden Sie sich zur Wiederherstellung der Daten über die VM-Konsole beim Cisco Prime Collaboration-Anwendungsserver an, und verwenden Sie den vSphere-Client. Starten Sie die Wiederherstellung nicht von der SSH/Putty-Eingabeaufforderung aus.

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

Dabei ist Backupfilenameis der Name der Sicherungsdatei, die mit dem Zeitstempel (*JJMMTT-HHMM*) und der Dateierweiterung .tar.gpg belegt ist.

So können Sie beispielsweise auf dem FTP-Server wiederherstellen:

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

PCA 12.x

So stellen Sie Daten wieder her:

Schritt 1: Geben Sie Ihren Browser https://PCA_IP_HERE:7443 ein, und melden Sie sich beim globalen Administrator an.

Schritt 2: Navigieren Sie zu **Maintenance>Restore**, und geben Sie die ftp/sft-Informationen ein.

Root-Benutzer festlegen

PCA 11.x

Schritt 1: Melden Sie sich über die CLI als Admin User (Admin-Benutzer) an dem PCA an, der nach der Installation erstellt wurde.

Schritt 2: Führen Sie den Befehl aus:**root_enable.**

Schritt 3: Geben Sie Ihr Root-Passwort ein.

Schritt 4: Als Administrator angemeldet, geben Sie root ein und geben Sie Ihr root-Passwort ein, um Zugriff auf root zu erhalten.

Schritt 5: Führen Sie den Befehl aus: **/opt/emms/emsam/bin/enableRoot.sh**

Schritt 6: Geben Sie **passwd** ein, und geben Sie das Passwort erneut ein.

PCA 12.x

Schritt 1: Geben Sie Ihren Browser ein **https://PCA_IP_HERE:7443 und melden Sie sich als globaladmin an.**

Schritt 2: Root-Zugriff auswählen

Schritt 3: Wählen Sie Aktivieren aus, und geben Sie Ihre Root-Anmeldeinformationen ein. Klicken Sie auf **Senden.**