Aggiorna modello di distribuzione APC

Sommario

Prime Collaboration Assurance (PCA) - Aggiornamento del modello di installazione

Introduzione

Questo documento descrive come aggiornare il modello di distribuzione di Prime Collaboration Assurance (PCA)

Contributo di Joseph Koglin, tecnico TAC

Questa procedura deve essere utilizzata solo per aggiornare il modello di implementazione e non per altri scopi.

Prerequisiti

Requisiti

- Conoscenza dell'APC
- Accesso per modificare le impostazioni hardware della macchina virtuale (VM) di Risoluzione problemi compatibilità programmi
- Accesso alla radice PCA
- Se si esegue l'aggiornamento a un'installazione molto grande, è necessario un server ftp/sftp remoto

Componenti usati

Le informazioni di questo documento si riferiscono a tutte le versioni correnti di PCA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

La capacità del sistema è vicina o al massimo e ciò può causare:

- Problemi relativi alle prestazioni del sistema, ad esempio il sistema, è possibile raggiungere il 100% o i servizi si arrestano in modo costante.
- Non è possibile installare più endpoint in base al formato di virtualizzazione aperto (OAV, Open Virtualization Format) ed è necessaria una versione più grande.

Soluzione

Aggiorna OAV di piccole e medie dimensioni

Passaggio 1. Per determinare le risorse aggiuntive necessarie, consultare la guida alla virtualizzazione per la propria versione.

Requisiti specifici per gli OVA della versione PCA

Passaggio 2. Sebbene non siano stati segnalati problemi, è sempre consigliabile creare un backup.

Opzione 1

Crea snapshot di una macchina virtuale

Passaggio 1. Accedere a Vsphere come utente amministratore.

Passaggio 1. Fare clic con il pulsante destro del mouse sulla VM in Vsphere.

Passaggio 2. Selezionare **Snapshot>>Crea snapshot.** Controllare lo stato nella parte inferiore della finestra di Vsphere per monitorare il completamento.

O

Opzione 2

Backup PCA

Passaggio 1. Passare a **Amministrazione sistema>>Impostazioni di backup>> Seleziona nuovo.** Fornire le informazioni richieste in base alle proprie esigenze, ad esempio se si desidera disporre solo dei dati di garanzia o di garanzia e analisi. Una volta completato il backup, procedere al passaggio successivo.

> **Nota:** Se si utilizza PCA 12.x, passare a **https://PCA_IP_HERE:7443** e accedere con globaladmin. Da qui, passare a **Manutenzione>Backup** e selezionare **Nuovo**. Fornire le informazioni richieste.

Passaggio 3. Accedere all'interfaccia della riga di comando (CLI) di APC come utente root e utilizzare la porta 26.

Passaggio 4. Immettere **/opt/emms/emsam/bin/cpcmcontrol.sh stop.**

Passaggio 5. Passare alla VM PCA e spegnerla.

Passaggio 6. Fare clic con il pulsante destro del mouse e modificare le impostazioni della macchina virtuale per aggiungere ulteriori risorse.

Passaggio 7. Fare clic con il pulsante destro del mouse per riaccendere la VM. Attendere 15 minuti.

Passaggio 8. Accedere a PCA come utente root e utilizzare la porta 26.

Passaggio 9. Immettere **/opt/emms/emsam/bin/newcpcmtuning.sh.**

```
[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] :
```

Passaggio 10. Selezionare il modello di distribuzione da aggiornare. Al termine dell'esecuzione dello script, i servizi vengono riavviati.

> **Nota:** Se al momento si utilizza un'installazione di piccole dimensioni, è possibile eseguire l'aggiornamento a Media o Grande. Se si utilizza una distribuzione di tipo Medio, si esegue l'aggiornamento a grande.

Aggiornare un OAV di grandi dimensioni a un OAV di grandi dimensioni

Backup PCA

Passaggio 1. Accedere all'APC utilizzando l'utente globaladmin.

Passaggio 2. Passare **a Amministrazione sistema>>Impostazioni di backup>** Selezionare Nuovo e fornire le informazioni necessarie per il backup di analisi.

Nota: Se si utilizza PCA 12.x, digitare nel browser **https://PCA_IP_HERE:7443** e accedere con l'utente globaladmin. Da qui, passare a **Manutenzione>Backup** e selezionare **Nuovo**, fornire le informazioni e assicurarsi che siano completate per il backup di analisi.

Passaggio 3. Per determinare le risorse aggiuntive necessarie, consultare la guida alla virtualizzazione per la propria versione.

Requisiti specifici per gli OVA della versione PCA

Passaggio 4. Accedere all'interfaccia della riga di comando (CLI) di APC come utente root utilizzando la porta 26 (chiamata VM dell'app).

Passaggio 5. Immettere **/opt/emms/emsam/bin/cpcmcontrol.sh stop.**

Passaggio 6. Passare alla VM PCA e spegnerla.

Passaggio 7. Fare clic con il pulsante destro del mouse e modificare le impostazioni della macchina virtuale per aggiungere ulteriori risorse.

Passaggio 8. Fare clic con il pulsante destro del mouse per riaccendere la VM. Attendere 15 minuti.

Passaggio 9. Accedere a PCA come utente root e utilizzare la porta 26.

Passaggio 10. Immettere **/opt/emms/emsam/bin/newcpcmtuning.sh.**

```
[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] :
```

Passaggio 11. Selezionare l'opzione 5, quindi riavviare nuovamente i servizi.

Passaggio 12. Scaricare il file Cisco Prime Collaboration Assurance and Analytics Very Large OVA e distribuire un server database PCA. Prendere nota dell'indirizzo IP come verrà utilizzato in un passaggio successivo.

Nota: Immettere l'indirizzo IP quando richiesto per l'indirizzo IP dell'applicazione durante la distribuzione del server database.

Passaggio 13. Sulla macchina virtuale dell'app, accedere come utente root alla CLI e usare la porta 26.

Passaggio 14. Eseguire il comando **/opt/emms/emsam/advance_reporting/bin/enableAnalyticsWithRemoteDB.sh** e puntare il server al server di database appena creato.

Passaggio 15. Dopo il completamento del comando, ripristinare i dati di analisi nel nuovo server di database

Non utilizzare questa procedura per scopi diversi dall'aggiornamento di una distribuzione di grandi dimensioni a molto grandi.

Ripristina i dati di analisi per l'installazione su vasta scala

APC 11.x

Passaggio 1. Trasferire il backup di analisi al server ftp/sftp.

Passaggio 2. Accedere al server del database Cisco Prime Collaboration Assurance con l'account creato durante l'installazione. L'account di accesso predefinito è admin.

Immettere i comandi per creare un repository sul server FTP:

```
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
```

Dove:

- RepositoryName è il percorso in cui eseguire il backup dei file. Il nome può contenere un massimo di 30 caratteri alfanumerici.
- ftp://ftpserver/directoryis il server FTP e la directory sul server in cui il file viene trasferito. È inoltre possibile utilizzare SFTP, HTTP o TFTP anziché FTP.
- UserName e {`plain`|`hash`}Password specificano il nome utente e la password per il server FTP, SFTP o TFTP. Hashspecifica una password crittografata e plainspecifica una password in testo normale non crittografata.

Ad esempio:

```
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
```

Passaggio 3. Elencare i dati del repository. È possibile elencare i dati all'interno di un repository. Accedere al server Cisco Prime Collaboration come amministratore ed eseguire questo comando:

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

In questo modo, l'autorità di certificazione della compatibilità è in grado di leggere il file di backup sul server ftp/sftp remoto

Passaggio 4. Per ripristinare i dati, accedere al server applicazioni Cisco Prime Collaboration come amministratore tramite la console VM e utilizzare il client vSphere. Non attivare il ripristino dal prompt SSH/Putty.

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

Dove,NomeFileBackup è il nome del file di backup con il suffisso dell'indicatore orario (*AAMMGG-HHMM*) e dell'estensione .tar.gpg.

Ad esempio, per eseguire il ripristino sul server ftp:

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

APC 12.x

Per ripristinare i dati:

Passaggio 1. Digitare nel browser https://PCA_IP_HERE:7443 e accedere con l'utente globaladmin.

Passo 2: passare a **Manutenzione>Ripristino** e inserire le informazioni ftp/sft.

Impostazione utente root

APC 11.x

Passaggio 1. Accedere alla PCA tramite CLI come utente amministratore creato dall'installazione.

Passaggio 2. Eseguire il comando:**root_enable**

Passaggio 3. Inserire la password di root.

Passaggio 4. Effettuato l'accesso come admin, immettere in root e immettere la password root per accedere a root.

Passaggio 5. Eseguire il comando: **/opt/emms/emsam/bin/enableRoot.sh.**

Passaggio 6. Immettere **password** e reimmettere la password di root.

APC 12.x

Passaggio 1. Digitare nel browser **https://PCA_IP_HERE:7443 e accedere come globaladmin**

Passaggio 2. Selezione dell'accesso alla radice

Passaggio 3. Selezionare Abilita e immettere le credenziali radice. Fare clic su **Sottometti.**