

Modelo de despliegue de la actualización PCA

Contenido

[Garantía primera de la Colaboración \(PCA\) - Actualice su modelo de despliegue](#)

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[HUEVOS pequeños y medios de la actualización](#)

[Actualice los HUEVOS grandes a un muy grande](#)

[Restablezca sus datos del Analytics para el despliegue muy grande](#)

[PCA 11.x](#)

[Fije a su usuario raíz](#)

[PCA 11.x](#)

[PCA 12.x](#)

Garantía primera de la Colaboración (PCA) - Actualice su modelo de despliegue

Introducción

Este documento describe cómo actualizar su modelo de despliegue primero de la garantía de la Colaboración (PCA)

Contribuido por José Koglin, ingeniero de TAC

Prerequisites

Requisitos

- Conocimiento del PCA
- Acceso para editar las configuraciones del hardware de la máquina virtual PCA (VM)
- Acceso a raíz PCA
- Si actualiza a un despliegue muy grande, un ftp del telecontrol/el servidor del sftp es necesarios

Componentes Utilizados

La información en este documento se relaciona con todas las versiones actuales PCA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Usted está cerca o en del sistema máximo capacity que puede causar:

- Los problemas de rendimiento del sistema tales como su, optan alcanzar el 100% o los servicios que causan un crash constantemente.
- Usted no puede desplegar más los puntos finales por su formato abierto de la virtualización (HUEVOS) y necesitar más grande.

Solución

HUEVOS pequeños y medios de la actualización

Paso 1. Refiera por favor a la guía del soporte de la virtualización para su versión, para determinar a los recursos adicionales necesarios.

[HUEVOS específicos Reuirements de la versión PCA](#)

Paso 2. Aunque no haya habido problemas señalados, es siempre el mejor crear un respaldo.

Opción 1

Tome una foto de la máquina virtual (VM)

Paso 1. Login a Vsphere como Usuario administrador.

Paso 1. Click derecho en el VM en Vsphere.

Paso 2. Seleccione la **foto de Snapshot>>Take**. Marque el estatus en la parte inferior de la ventana de Vsphere para monitorear la realización.

O

Opción 2

Tome un respaldo PCA

Paso 1. Navegue a **nuevo selecto del sistema Administration>>Backup Settings>>**. Proporcione la Información requerida basada en sus necesidades, es decir si usted quiere apenas los datos de la garantía o la garantía y el analytics. Una vez que el respaldo es completo, proceda al siguiente paso.

Note: Si usted utiliza PCA 12.x, navegue a **https://PCA_IP_HERE:7443** y inicie sesión con el globaladmin. De allí, navegue a **Maintenance>Backup** y seleccione **nuevo**. Proporcione la información requerida.

Paso 3. Inicie sesión al comando line interface(cli) PCA como raíz y utilice el puerto 26.

Paso 4. Ingrese la **parada de /opt/emms/emsam/bin/cpcmcontrol.sh**.

Paso 5. Navegue a usted PCA VM y accione abajo el VM.

Paso 6. Haga clic con el botón derecho del ratón y edite las configuraciones VM para agregar a los recursos adicionales.

Paso 7. Click derecho para accionar detrás en el VM. Espera 15 minutos.

Paso 8. Inicie sesión al PCA como raíz y utilice el puerto 26.

Paso 9. Ingrese `/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] : █
```

Sept 10. selecto el modelo de despliegue que usted desea actualizar a. Después de que el script acabe, los servicios recomienzan.

Note: Si usted utiliza actualmente un pequeño despliegue, usted actualiza a medio o a grande. Si usted utiliza un despliegue medio, usted actualiza a grande.

Actualice los HUEVOS grandes a un muy grande

Tome un respaldo PCA

Paso 1. Inicie sesión a su PCA usando su usuario del globaladmin.

Paso 2. Navegue el toSystem **Administration>>Backup Settings>>** que Newand selecto proporciona la información requerida para el respaldo del analytics.

Note: Si usa PCA 12.x, teclee adentro a su navegador https://PCA_IP_HERE:7443 y inicie sesión con el usuario del globaladmin. De allí, navegue a **Maintenance>Backup** y a **nuevo** selecto, proporcione la información y asegúrese que completa para el respaldo del analytics.

Paso 3. Refiera por favor a la guía del soporte de la virtualización para su versión, para determinar a los recursos adicionales necesarios.

[HUEVOS específicos Reuirements de la versión PCA](#)

Paso 4. Inicie sesión al comando line interface(cli) PCA como raíz usando el puerto 26 (llame esto el App VM).

Paso 5. Ingrese la parada de `/opt/emms/emsam/bin/cpcmcontrol.sh`.

Paso 6. Navegue a usted PCA VM y accione abajo el VM.

Paso 7. Haga clic con el botón derecho del ratón y edite las configuraciones VM para agregar en los recursos adicionales.

Paso 8. Click derecho para accionar detrás en el VM. Espera 15 minutos.

Paso 9. Inicie sesión al PCA como raíz y utilice el puerto 26.

Paso 10. Ingrese `/opt/emms/emsam/bin/newcpcmtuning.sh`.

```
[root@jdkoglin-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] : █
```

Paso 11 La opción selecta 5, los servicios recomienza otra vez.

Paso 12. Descargue la garantía de la Colaboración de la prima de Cisco y los HUEVOS muy grandes del Analytics clasifían y despliegan a un servidor de bases de datos PCA. Tome la nota de la dirección IP como se utiliza en un paso posterior.

Note: Ingrese el IP Address, cuando está pedido el IP de la aplicación durante el despliegue del servidor de bases de datos.

Paso 13. En el App VM, inicie sesión como el usuario raíz en el CLI y utilice el puerto 26.

Paso 14. Funcione con el comando `/opt/emms/emsam/advance_reporting/bin/enableAnalyticsWithRemoteDB.sh` y señale este servidor al servidor de bases de datos apenas creado.

Paso 15. Después de que el comando complete, restablezca sus datos del analytics sobre el

nuevo servidor de bases de datos

Restablezca sus datos del Analytics para el despliegue muy grande

PCA 11.x

Paso 1. Transfiera su respaldo del analytics a su ftp/servidor del sftp.

Paso 2. Inicie sesión al servidor de bases de datos de la garantía de la Colaboración de la prima de Cisco con la cuenta que usted creó durante la instalación. El login predeterminado es admin.

Ingrese los comandos para crear un depósito en el servidor 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
```

Donde:

- **RepositoryName** es la ubicación a la cual los archivos deben ser sostenidos. Este nombre puede contener un máximo de 30 caracteres alfanuméricos.
- **ftp://ftpserver/directory** es el servidor FTP y el directorio en el servidor al cual se transfiere el archivo. Usted puede también utilizar el SFTP, el HTTP, o el TFTP en vez del FTP.
- **UserName** and **{llano|hash} Password** are el nombre de usuario y contraseña para el FTP, el SFTP, o el servidor TFTP. Hash especifica una contraseña encriptada, y plain especifica una contraseña unencrypted del sólo texto.

Por ejemplo:

```
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
```

Paso 3. Enumere los datos del repositorio. Usted puede enumerar los datos dentro de un repositorio. El login al **admin** del Collaboration Server de la prima de Cisco funciona con este comando:

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

Esto se asegura que el PCA pueda leer el archivo de backup en su ftp del telecontrol/servidor del sftp

Paso 4. Para restablecer los datos, inicie sesión a la consola del asadminthrough VM del servidor de aplicaciones de la Colaboración de la prima de Cisco y utilice al cliente del vSphere. No accione el restore del prompt SSH/Putty.

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

Donde, *Backupfilename* es el nombre del archivo de backup añadió como sufijo con el grupo fecha/hora (YYMMDD-HHMM) y la extensión de archivo .tar .gpg.

Por ejemplo, restablecer en el ftp server:

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

PCA 12.x

Para restablecer los datos:

Paso 1. Teclee adentro a su navegador https://PCA_IP_HERE:7443 y inicie sesión con el usuario del globaladmin.

Paso 2. Navegue a **Maintenance>Restore** y ingrese la información ftp/del sft.

Fije a su usuario raíz

PCA 11.x

El paso 1. Log adentro al PCA con el CLI como el Admin creado por el usuario de instala.

Paso 2. Funcione con el comando: **root_enable**.

Paso 3. Ingrese en su contraseña de raíz.

Paso 4. Abierto una sesión como admin, ingrese en la raíz y ingrese en su contraseña de raíz para acceder para arraigar.

Paso 5. Funcione con el comando: **/opt/emms/emsam/bin/enableRoot.sh**.

Paso 6. Ingrese el **passwd** y éntrelo de nuevo en su misma contraseña de raíz.

PCA 12.x

Paso 1. Teclee adentro a su navegador https://PCA_IP_HERE:7443 y inicie sesión como globaladmin

Paso 2. Seleccione el acceso a raíz

Paso 3. Selecto habilite y ingrese sus credenciales de la raíz. Haga clic en Submit (Enviar).

Root Access	<input type="text" value="Enable"/>
New Password	<input type="text" value="Enter New Password"/>
Confirm New Password	<input type="text" value="Enter Confirm New Password"/>

* Root Access will be Enabled now

* Password Reset will terminate the current active sessions