

Procedimiento de recuperación de VM PCRf - OpenStack

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Procedimiento de copia de seguridad](#)

[Paso 1. Controlador de servicios elásticos \(ESC\)](#)

[Paso 2. Copia de seguridad de Cisco Policy Suite](#)

[Troubleshoot](#)

Introducción

Los documentos describen el procedimiento para recuperar las instancias de Virtual Cisco Policy and Charging Rules Function (vPCRf) implementadas en un entorno Ultra-M/OpenStack.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- OpenStack
- Cisco Policy Suite (CPS)
- Ya está disponible el cálculo en el que se implementaron las instancias afectadas
- Los recursos de cálculo están disponibles en la misma zona de disponibilidad que la instancia afectada

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Procedimiento de copia de seguridad

Paso 1. Controlador de servicios elásticos (ESC)

Las configuraciones en ESC-HA se deben realizar una copia de seguridad mensual, antes/después de cualquier operación de ampliación o reducción con el VNF y antes/después de los cambios de configuración en ESC. Se debe realizar una copia de seguridad para poder realizar una recuperación ante desastres de ESC de manera eficaz.

ESC opdata como XML

Siga esto para exportar los **opdata** ESC como XML:

1. Inicie sesión en ESC con las credenciales de administrador.

2. Exportar **opdata** a XML:

```
/opt/cisco/esc/confd/bin/netconf-console --host 127.0.0.1 --port 830 -u <admin-user> -p <admin-password> --get-config > /home/admin/ESC_config.xml
```

3. Descargue este archivo en su equipo local de **ftp/sftp** a un servidor fuera de la nube.

4. Todos los scripts y archivos de datos de usuario a los que se hace referencia en XML de implementación. Busque todos los archivos de datos de usuario a los que se hace referencia en XML de implementación de todas las VNF desde los datos opdata exportados en el paso anterior.

```
grep "file://" /home/admin/ESC_config.xml | sort | uniq
```

Ejemplo de resultado

```
<file>file:///opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-cm_cloud.cfg</file>
<file>file:///opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-oam_cloud.cfg</file>
<file>file:///opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-pd_cloud.cfg</file>
<file>file:///opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-qns_cloud.cfg</file>
<file>file:///opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-sm_cloud.cfg</file>
```

5. Encuentre todas las secuencias de comandos posteriores a la implementación utilizadas para enviar la API de orquestación de CPS.

6. Fragmentos de ejemplo de la secuencia de comandos **post_implementación** en **datos operativos ESC**

Ejemplo de resultado

```
<policies>
  <policy>
    <name>PCRF_POST_DEPLOYMENT</name>
    <conditions>
      <condition>
        <name>LCS::POST_DEPLOY_ALIVE</name>
```

```

        </condition>
    </conditions>
    <actions>
        <action>
            <name>FINISH_PCRF_INSTALLATION</name>
            <type>SCRIPT</type>
            <properties>
                -----
<property>
                <name>script_filename</name>
                <value>/opt/cisco/esc/cisco-cps/config/gr/tmo/cfg/./cps_init.py</value>
            </property>
            <property>
                <name>script_timeout</name>
                <value>3600</value>
            </property>
            </properties>
        </action>
    </actions>
</policy>
</policies>

```

Ejemplo 2:

```

<policy>
    <name>PCRF_POST_DEPLOYMENT</name>
    <conditions>
        <condition>
            <name>LCS::POST_DEPLOY_ALIVE</name>
        </condition>
    </conditions>
    <actions>
        <action>
            <name>FINISH_PCRF_INSTALLATION</name>
            <type>SCRIPT</type>
            <properties>
                <property>
                    <name>CLUMAN_MGMT_ADDRESS</name>
                    <value>10.174.132.46</value>
                </property>
                <property>
                    <name>CLUMAN_YAML_FILE</name>
                    <value>/opt/cisco/esc/cisco-cps/config/vpcrf01/ cluman_orch_config.yaml</value>
                </property>
                <property>
                    <name>script_filename</name>
                    <value>/opt/cisco/esc/cisco-
cps/config/vpcrf01/vpcrf_cluman_post_deployment.py</value>
                </property>
                <property>
                    <name>wait_max_timeout</name>
                    <value>3600</value>
                </property>
            </properties>
        </action>
    </actions>
</policy>

```

Si la implementación **ESC opdata** (extraída en el paso anterior) contiene alguno de los archivos resaltados, realice una copia de seguridad con la ayuda de este comando.

```
tar -zcf esc_files_backup.tgz /opt/cisco/esc/cisco-cps/config/
```

Descargue este archivo en su equipo local de **ftp/sftp** a un servidor fuera de la nube.

Nota: Aunque **opdata** se sincroniza entre ESC primary y standby, los directorios que contienen datos de usuario, secuencias de comandos XML y posteriores a la implementación no se sincronizan en ambas instancias. Se sugiere que los clientes impulsen el contenido del directorio que contiene estos archivos con el uso de SCP o SFTP, estos archivos deben ser constantes a través de ESC-Primary y ESC-Standby para recuperar una implementación cuando no esté disponible la VM ESC que era principal en el momento de la implementación.

Programación de copias de seguridad sugerida en ESC

Estas son las entradas de crontab sugeridas para que el usuario raíz sea agregado en ESC Primario y ESC En espera. Sin embargo, puede modificar las horas/día/mes según sus requisitos y la frecuencia de los cambios en la red.

```
30 01 * * * tar -zcf /home/admin/esc_files_backup_$(date +"%Y-%m-%d").tgz
/opt/cisco/esc/cisco-cps/config/
00 02 * * * /opt/cisco/esc/confd/bin/netconf-console --host 127.0.0.1 --port 830 -u <admin-user>
-p <admin-password> --get-config > /home/admin/ESC_config_$(date +"%Y-%m-%d").xml
```

Paso 2. Copia de seguridad de Cisco Policy Suite

Cluster Manager actúa como marioneta principal para un clúster CPS. Por lo tanto, se hace necesario tomar una instantánea de esta instancia. Además, la utilidad de copia de seguridad y restauración proporcionada por Cisco se puede utilizar para recopilar copias de seguridad de mongoDB, configuración de políticas, base de datos de grafana, usuarios, redes y otros archivos de configuración de pcrf. Estos archivos se deben realizar copias de seguridad con frecuencia mediante la utilidad de copia de seguridad CPS y se deben almacenar en una ubicación fuera de la nube Ultra-M.

Instantánea de la VM Cluster Manager

Se debe realizar una copia de seguridad de Cluster Manager Instance Snapshot mensualmente, también antes y después de cualquier cambio de configuración, actualizaciones de parches y actualizaciones. Las instantáneas antiguas se pueden eliminar después de realizar actividades correctas para ahorrar espacio en disco. Este procedimiento describe los pasos para realizar una copia de seguridad de la instancia del administrador del clúster como una instantánea:

1. Este comando para ver las instancias nova y observar el nombre de la instancia de VM del administrador de clúster:

```
nova list
```

2. Cree una imagen de instantánea de nova como se muestra aquí:

```
nova image-create --poll <cluman_instance_name> <cluman_snapshot_name>
```

Ejemplo de resultado

```
Server snapshotting... 100% complete
```

```
Finished
```

Nota: Asegúrese de tener suficiente espacio en disco para la instantánea. El Administrador de clústeres a veces se vuelve inalcanzable en el momento de la creación de la instantánea y se reanuda después de que se ha creado la instantánea. Si la instancia permanece inalcanzable incluso después de que el proceso de instantánea haya terminado, verifique el estado de VM con el uso del comando **nova list**. Si está en estado **SHUTOFF**, debe iniciar la VM manualmente, con el uso del comando **nova start**.

3. Asegúrese de que la imagen de instantánea se crea con este comando.

```
glance image-list
```

Ejemplo de resultado

ID	Name
1683d05f-2a9f-46d8-877d-10982ee819e1	cluman_backup_image
30f2ece1-6438-4ef7-b4cf-44a0e7de183e	CPS_13.1.1.release.iso
d38321a1-27c1-4c47-bc0f-24aedab5867a	CPS_13.1.1_Base

4. Cuando realiza cualquier cambio de plataforma en la que Ceph pueda verse afectado, siempre se sugiere convertir la instantánea de Cluster Manager en un archivo QCOW y guardarlo en alguna ubicación remota.

```
glance image-download --file /var/Pcrf/cluman_snapshot.raw <image-id of the snapshot>
```

5. Descargue este archivo en su equipo local de **ftp/sftp** a un servidor fuera de la nube.

Copia de seguridad de la base de datos y las configuraciones de CPS

1. Para realizar una copia de seguridad de las configuraciones de CPS y del contenido de la base de datos, la utilidad **config_br.py** está incorporada en la plataforma CPS. Los detalles sobre el uso de la utilidad **config_br.py** están presentes en la Guía de Copia de Seguridad y Restauración de CPS. Este es un ejemplo de crontab en el cluster manager para realizar una copia de seguridad de todas las configuraciones y bases de datos a las 100 horas todos los días.

```
00 01 * * * /var/platform/modules/config_br.py -a export --all /mnt/backup/backup_$(date +%Y-%m-%d).tar
```

2. MongoDB puede alternativamente ser respaldado con el uso de **mongodump**.

```
30 01 * * * mongodump --host sessionmgr01 -port 27721 --out /mnt/backup/mongo_admin_27721_$(date +%Y-%m-%d)/
```

```
30 01 * * * mongodump --host sessionmgr01 -port 27720 --out /mnt/backup/mongo_spr_27720_$(date +%Y-%m-%d)/
```

```
30 01 * * * mongodump --host sessionmgr01 -port 27718 --out /mnt/backup/mongo_bal_27718_$(date
+ \%Y-\ \%m-\ \%d)/
```

```
30 01 * * * mongodump --host sessionmgr01 -port 27719 --out
/mnt/backup/mongo_report_27721_$(date + \%Y-\ \%m-\ \%d)/
```

3. Orquestación de respaldo YAML.

```
curl -i -X GET http://<Cluster Manager IP>:8458/api/system/config -H "Content-Type:
application/yaml" > /mnt/backup/CPS_orc_$(date + \%Y-\ \%m-\ \%d).yaml
```

Si se utiliza la API de orquestación CPS para configurar el sistema, se sugiere realizar una copia de seguridad de esta configuración también.

Nota: Todas las copias de seguridad se deben almacenar/transferir fuera de CPS VNF y, preferiblemente, fuera de la nube en la que se implementa CPS.

Troubleshoot

Procedimientos de recuperación de instancia de VNF de CPS

Encienda cualquier instancia desde el estado de SHUTOFF.

Si alguna instancia se encuentra en estado SHUTOFF debido a un apagado planificado o a algún otro motivo, utilice este procedimiento para iniciar la instancia y habilitar su supervisión en ESC.

1. Verifique el estado de una instancia a través de OpenStack.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f| destackovs-
compute-2 | SHUTOFF|
```

2. Compruebe si la herramienta Compute está disponible y asegúrese de que el estado esté activo.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f| destackovs-
compute-2 | SHUTOFF|
```

3. Inicie sesión en ESC Primary como usuario administrador y verifique el estado de la instancia en **opdata**.

```
echo "show esc_datamodel opdata tenants tenant Pcrf deployments * state_machine | tab" |
/opt/cisco/esc/confd/bin/confd_cli -u admin -C | grep cm
cm_0_170d9c14-0221-4609-87e3-d752e636f57f VM_ERROR_STATE
```

4. Encienda la instancia desde OpenStack.

```
source /home/stack/destackovsrc-Pcrf
```

```
nova start cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

5. Espere cinco minutos para que la instancia se inicie y llegue al estado **ACTIVE**.

```
source /home/stack/destackovsrc-Pcrf
```

```
nova list --fields name,status | grep cm
```

```
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f | ACTIVE |
```

6. Habilite VM Monitor en ESC después de que la instancia se encuentre en un estado **ACTIVE**.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

Para obtener más información sobre la recuperación de las configuraciones de instancias, consulte aquí **los procedimientos específicos del tipo de instancia**.

Recuperar cualquier instancia del estado de ERROR

Se puede utilizar el siguiente procedimiento si el estado de la instancia de CPS en OpenStack es **ERROR**:

1. Compruebe el estado de una instancia en OpenStack.

```
source /home/stack/destackovsrc-Pcrf
```

```
nova list --fields name,host,status | grep cm
```

```
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f | destackovs-  
compute-2 | ERROR|
```

2. Compruebe si la herramienta Compute está disponible y se está ejecutando correctamente.

```
source /home/stack/destackovsrc-Pcrf
```

```
nova list --fields name,host,status | grep cm
```

```
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f | destackovs-  
compute-2 | ERROR|
```

3. Inicie sesión en ESC Primary como usuario administrador y verifique el estado de una instancia en **opdata**.

```
echo "show esc_datamodel opdata tenants tenant Pcrf deployments * state_machine | tab" |  
/opt/cisco/esc/confd/bin/confd_cli -u admin -C | grep cm
```

```
cm_0_170d9c14-0221-4609-87e3-d752e636f57f VM_ERROR_STATE
```

4. Restablezca el estado de la instancia para obligar a la instancia a volver a un estado **ACTIVE** en lugar de un estado de error. Cuando haya terminado, reinicie la instancia.

```
source /home/stack/destackovsrc-Pcrf
```

```
nova reset-state --active cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

```
nova reboot --hard cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

5. Espere cinco minutos para que la instancia se inicie y llegue a un estado **ACTIVO**.

```
source /home/stack/destackovsrc-Pcrf
```

```
nova list --fields name,status | grep cm
```

| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f | ACTIVE |

6. Si Cluster Manager cambia el estado a **ACTIVE** después del reinicio, habilite VM Monitor en ESC.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR  
cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

7. Post recovery to RUNNING/ACTIVE state, consulte el procedimiento específico del tipo de instancia para recuperar config/data de backup.