Procedimientos de respaldo y restauración para varios componentes Ultra-M - CPS

Contenido

Introducción

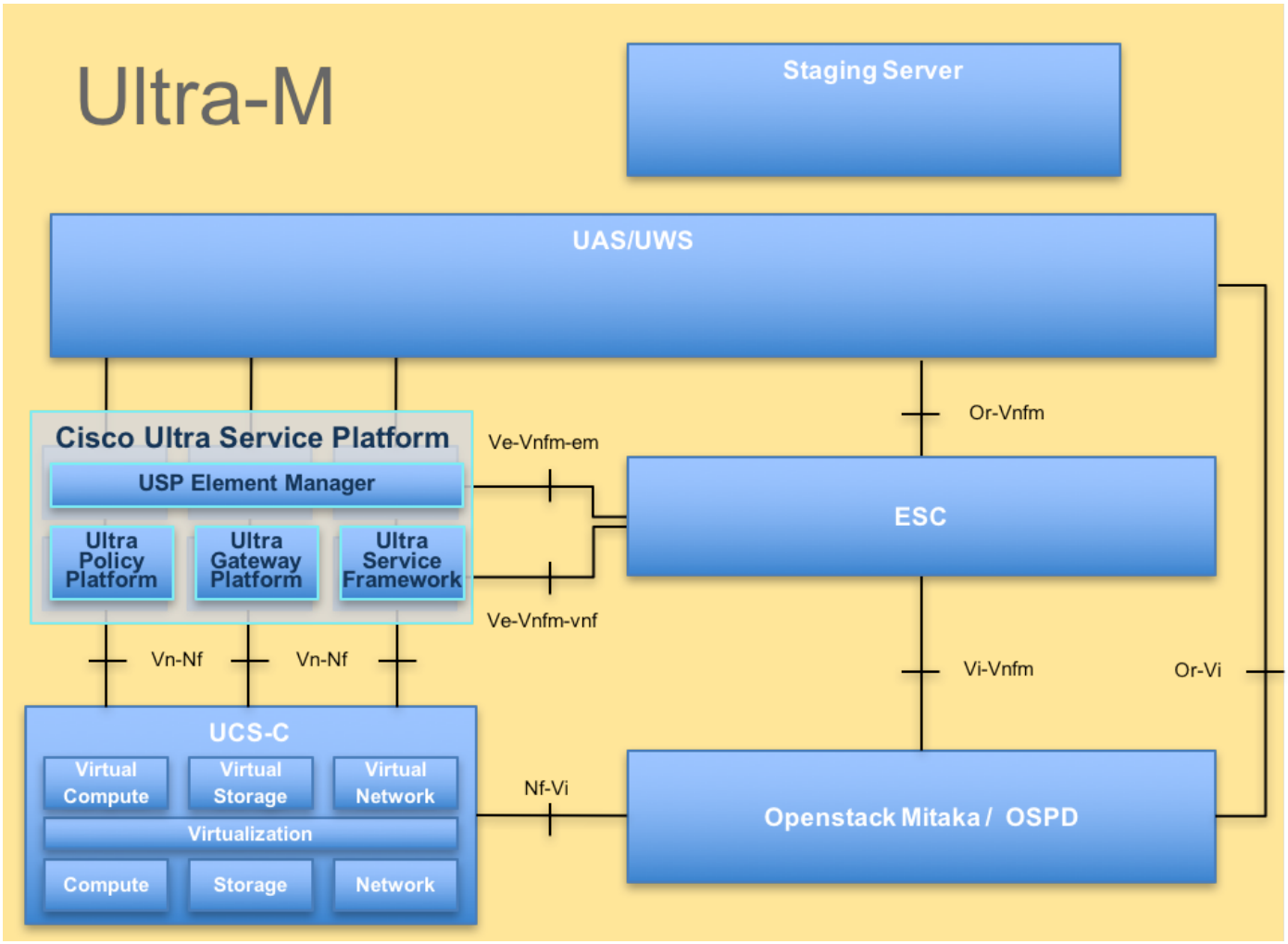
Este documento describe los pasos necesarios para realizar una copia de seguridad y restaurar una máquina virtual (VM) en una configuración Ultra-M que aloja Llamadas Funciones de Red Virtual de Llamadas CPS (VNF).

Antecedentes

Ultra-M es una solución de núcleo de paquetes móviles virtualizada validada y empaquetada previamente diseñada para simplificar la implementación de VNF. La solución Ultra-M consta de los siguientes tipos de máquinas virtuales:

- Controlador de servicios elásticos (ESC)
- Cisco Policy Suite (CPS)

La arquitectura de alto nivel de Ultra-M y los componentes involucrados son como se muestra en esta imagen.



Nota: Se considera la versión Ultra M 5.1.x para definir los procedimientos en este documento. Este documento está dirigido al personal de Cisco que está familiarizado con la plataforma Cisco Ultra-M.

Abreviaturas

VNF	Función de red virtual
ESC	Controlador de servicio elástico
MOP	Método de procedimiento
OSD	Discos de almacenamiento de objetos
HDD	Unidad de disco duro
SSD	Unidad de estado sólido
VIM	Administrador de infraestructura virtual
VM	Máquina virtual
UUID	Identificador único universal

Procedimiento de copia de seguridad

Respaldo OSPD

1. Compruebe el estado de la pila OpenStack y la lista de nodos.

```
[stack@director ~]$ source stackrc
[stack@director ~]$ openstack stack list --nested
[stack@director ~]$ ironic node-list
[stack@director ~]$ nova list
```

2. Compruebe si todos los servicios de la nube inferior están en estado cargado, activo y en ejecución desde el nodo OSP-D.

```
[stack@director ~]$ systemctl list-units "openstack*" "neutron*" "openvswitch*"

UNIT                                     LOAD   ACTIVE SUB     DESCRIPTION

neutron-dhcp-agent.service               loaded active running OpenStack Neutron DHCP Agent
neutron-openvswitch-agent.service        loaded active running OpenStack Neutron Open vSwitch
Agent
neutron-ovs-cleanup.service              loaded active exited  OpenStack Neutron Open vSwitch
Cleanup Utility
neutron-server.service                   loaded active running OpenStack Neutron Server
openstack-aodh-evaluator.service         loaded active running OpenStack Alarm evaluator
service
openstack-aodh-listener.service          loaded active running OpenStack Alarm listener
service
openstack-aodh-notifier.service          loaded active running OpenStack Alarm notifier
service
openstack-ceilometer-central.service     loaded active running OpenStack ceilometer central
agent
openstack-ceilometer-collector.service   loaded active running OpenStack ceilometer collection
service
openstack-ceilometer-notification.service  loaded active running OpenStack ceilometer
notification agent
openstack-glance-api.service             loaded active running OpenStack Image Service (code-
named Glance) API server
openstack-glance-registry.service        loaded active running OpenStack Image Service (code-
named Glance) Registry server
openstack-heat-api-cfn.service           loaded active running Openstack Heat CFN-compatible
API Service
openstack-heat-api.service               loaded active running OpenStack Heat API Service
openstack-heat-engine.service            loaded active running Openstack Heat Engine Service
openstack-ironic-api.service             loaded active running OpenStack Ironic API service
openstack-ironic-conductor.service       loaded active running OpenStack Ironic Conductor
service
openstack-ironic-inspector-dnsmasq.service loaded active running PXE boot dnsmasq service for
Ironic Inspector
openstack-ironic-inspector.service       loaded active running Hardware introspection service
for OpenStack Ironic
openstack-mistral-api.service            loaded active running Mistral API Server
openstack-mistral-engine.service         loaded active running Mistral Engine Server
openstack-mistral-executor.service       loaded active running Mistral Executor Server
openstack-nova-api.service               loaded active running OpenStack Nova API Server
openstack-nova-cert.service              loaded active running OpenStack Nova Cert Server
openstack-nova-compute.service           loaded active running OpenStack Nova Compute Server
openstack-nova-conductor.service         loaded active running OpenStack Nova Conductor Server
openstack-nova-scheduler.service         loaded active running OpenStack Nova Scheduler Server
openstack-swift-account-reaper.service   loaded active running OpenStack Object Storage
(swift) - Account Reaper
openstack-swift-account.service          loaded active running OpenStack Object Storage
(swift) - Account Server
openstack-swift-container-updater.service  loaded active running OpenStack Object Storage
(swift) - Container Updater
```

```
openstack-swift-container.service          loaded active running OpenStack Object Storage
(swift) - Container Server
openstack-swift-object-updater.service     loaded active running OpenStack Object Storage
(swift) - Object Updater
openstack-swift-object.service             loaded active running OpenStack Object Storage
(swift) - Object Server
openstack-swift-proxy.service              loaded active running OpenStack Object Storage
(swift) - Proxy Server
openstack-zaqar.service                    loaded active running OpenStack Message Queuing
Service (code-named Zaqar) Server
openstack-zaqar@1.service                  loaded active running OpenStack Message Queuing
Service (code-named Zaqar) Server Instance 1
openvswitch.service                        loaded active exited  Open vSwitch

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

37 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

3. Confirme que dispone de suficiente espacio en disco antes de realizar el proceso de copia de seguridad. Se espera que este tarball sea de al menos 3,5 GB.

```
[stack@director ~]$df -h
```

4. Ejecute estos comandos como usuario raíz para realizar una copia de seguridad de los datos del nodo de la nube inferior a un archivo denominado **undercloud-backup-[timestamp].tar.gz** y transferirlos al servidor de respaldo.

```
[root@director ~]# mysqldump --opt --all-databases > /root/undercloud-all-databases.sql
[root@director ~]# tar --xattrs -czf undercloud-backup-`date +%F`.tar.gz /root/undercloud-all-
databases.sql
/etc/my.cnf.d/server.cnf /var/lib/glance/images /srv/node /home/stack
tar: Removing leading `/' from member names
```

Copia de seguridad ESC

1. El ESC, a su vez, activa Virtual Network Function (VNF) interactuando con VIM.

2. ESC tiene redundancia 1:1 en la solución Ultra-M. Hay 2 VM ESC implementadas y admiten una única falla en Ultra-M, es decir, recuperar el sistema si hay una única falla en el sistema.

> **Nota:** Si se produce más de una falla, no se admite y puede que sea necesario reimplementar el sistema.

Detalles de la copia de seguridad ESC:

- Configuración en ejecución
- Base de datos CDB de ConfD
- Registros ESC
- Configuración de Syslog

3. La frecuencia de respaldo de la base de datos ESC es complicada y debe manejarse cuidadosamente mientras ESC monitorea y mantiene las diversas máquinas de estado para diversas VM de VNF implementadas. Se recomienda que estas copias de seguridad se realicen después de realizar las siguientes actividades en un VNF/POD/Site dado

4. Verifique que el estado de ESC sea bueno usando la secuencia de comandos health.sh.

```
[root@auto-test-vnfm1-esc-0 admin]# escadm status
0 ESC status=0 ESC Master Healthy

[root@auto-test-vnfm1-esc-0 admin]# health.sh
esc ui is disabled -- skipping status check
esc_monitor start/running, process 836
esc_mona is up and running ...
vimmanager start/running, process 2741
vimmanager start/running, process 2741
esc_confd is started
tomcat6 (pid 2907) is running...                           [  OK  ]
postgresql-9.4 (pid  2660) is running...
ESC service is running...
Active VIM = OPENSTACK
ESC Operation Mode=OPERATION

/opt/cisco/esc/esc_database is a mountpoint

============== ESC HA (MASTER) with DRBD =================

DRBD_ROLE_CHECK=0
MNT_ESC_DATABSE_CHECK=0
VIMMANAGER_RET=0
ESC_CHECK=0
STORAGE_CHECK=0
ESC_SERVICE_RET=0
MONA_RET=0
ESC_MONITOR_RET=0

=======================================

ESC HEALTH PASSED
```

5. Realice la copia de seguridad de la configuración en ejecución y transfiera el archivo al servidor de copia de seguridad.

```
[root@auto-test-vnfm1-esc-0 admin]# /opt/cisco/esc/confd/bin/confd_cli -u admin -C

admin connected from 127.0.0.1 using console on auto-test-vnfm1-esc-0.novalocal
auto-test-vnfm1-esc-0# show running-config | save /tmp/running-esc-12202017.cfg
auto-test-vnfm1-esc-0#exit

[root@auto-test-vnfm1-esc-0 admin]# ll /tmp/running-esc-12202017.cfg
-rw-------. 1 tomcat tomcat 25569 Dec 20 21:37 /tmp/running-esc-12202017.cfg
```

Base de datos ESC de reserva

1. Inicie sesión en la VM ESC y ejecute el siguiente comando antes de realizar la copia de seguridad.

```
[admin@esc ~]# sudo bash
[root@esc ~]# cp /opt/cisco/esc/esc-scripts/esc_dbtool.py /opt/cisco/esc/esc-
scripts/esc_dbtool.py.bkup
[root@esc esc-scripts]# sudo sed -i "s,'pg_dump,'/usr/pgsql-9.4/bin/pg_dump,"
/opt/cisco/esc/esc-scripts/esc_dbtool.py

#Set ESC to mainenance mode
[root@esc esc-scripts]# escadm op_mode set --mode=maintenance
```

2. Verifique el modo ESC y asegúrese de que está en modo de mantenimiento.

```
[root@esc esc-scripts]# escadm op_mode show
```

3. Copia de seguridad de la base de datos mediante la herramienta de restauración de copias de seguridad de la base de datos disponible en ESC.

```
[root@esc scripts]# sudo /opt/cisco/esc/esc-scripts/esc_dbtool.py backup --file
 scp://<username>:<password>@<backup_vm_ip>:<filename>
```

4. Vuelva a establecer ESC en Modo de funcionamiento y confirme el modo.

```
[root@esc scripts]# escadm op_mode set --mode=operation

[root@esc scripts]# escadm op_mode show
```

5. Navegue hasta el directorio de scripts y recopile los registros.

```
[root@esc scripts]# /opt/cisco/esc/esc-scripts

sudo ./collect_esc_log.sh
```

6. Para crear una instantánea del ESC, cierre primero el ESC.

```
shutdown -r now
```

7. Desde OSPD cree una instantánea de imagen

```
nova image-create --poll esc1 esc_snapshot_27aug2018
```

8. Verifique que se haya creado la instantánea

```
openstack image list | grep esc_snapshot_27aug2018
```

9. Iniciar ESC desde OSPD

```
nova start esc1
```

10. Repita el mismo procedimiento en la VM ESC en espera y transfiera los registros al servidor de respaldo

11. Recopile la copia de seguridad de la configuración de syslog en ambos VMS ESC y transfiérelos al servidor de respaldo

```
[admin@auto-test-vnfm2-esc-1 ~]$ cd /etc/rsyslog.d
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/00-escmanager.conf
00-escmanager.conf

[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/01-messages.conf
01-messages.conf

[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/02-mona.conf
02-mona.conf

[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.conf
```

```
rsyslog.conf
```

Copia de seguridad de CPS

1. Creación de una Copia de Seguridad de CPS Cluster-Manager

Utilice este comando para ver las instancias nova y observe el nombre de la instancia de VM del administrador de clúster:

```
nova list
```

Detenga a Cluman del ESC

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action STOP <vm-name>
```

Paso 2. Verifique el Cluster Manager en el estado SHUTOFF.

```
admin@esc1 ~]$ /opt/cisco/esc/confd/bin/confd_cli

admin@esc1> show esc_datamodel opdata tenants tenant Core deployments * state_machine
```

Paso 3. Cree una imagen de instantánea nova como se muestra en el siguiente comando:

```
nova image-create --poll
```

Nota: Asegúrese de tener suficiente espacio en disco para la instantánea.

Importante: en caso de que la VM se vuelva inalcanzable después de la creación de la instantánea, verifique el estado de la VM mediante el comando nova list. Si se encuentra en estado "SHUTOFF", debe iniciar la VM manualmente.

Paso 4. Vea la lista de imágenes con el siguiente comando: nova image-list Figura 1: Ejemplo de salida

```
+--------------------------------------+----------------------------------+-------+----------------------------------+|
ID                                     | Name                             |Status |Server
+--------------------------------------+----------------------------------+-------+----------------------------------+
|146719e8-d8a0-4d5a-9b15-2a669cfab81f  |CPS_10.9.9_20160803_100301_112.iso|ACTIVE|
|1955d56e-4ecf-4269-b53d-b30e73ad57f0  |base_vm                           |ACTIVE|
|2bbfb51c-cd05-4b7c-ad77-8362d76578db  |cluman_snapshot                   |ACTIVE|4842ae5a-83a3-48fd-915b-6ca6361adb2c

+--------------------------------------+----------------------------------+------+----------------------------------+
```

Paso 5. Cuando se crea una instantánea, la imagen de instantánea se almacena en OpenStack Glance. Para almacenar la instantánea en un almacén de datos remoto, descargue la instantánea y transfiera el archivo en OSPD a (/home/stack/CPS_BACKUP)

Para descargar la imagen, utilice el siguiente comando en OpenStack:

```
glance image-download --file For example: glance image-download --file snapshot.raw 2bbfb51c-
```

```
cd05-4b7c-ad77-8362d76578db
```

Paso 6. Enumera las imágenes descargadas como se muestra en el siguiente comando:

```
ls –ltr *snapshot*

Example output: -rw-r--r--. 1 root root 10429595648 Aug 16 02:39 snapshot.raw
```

Paso 7. Almacene la instantánea de la VM Cluster Manager para restaurarla en el futuro.

2. Realice una copia de seguridad de la configuración y la base de datos.

```
1. config_br.py -a export --all /var/tmp/backup/ATP1_backup_all_$(date +\%Y-\%m-\%d).tar.gz OR
2. config_br.py -a export --mongo-all /var/tmp/backup/ATP1_backup_mongoall$(date +\%Y-\%m-
\%d).tar.gz
3. config_br.py -a export --svn --etc --grafanadb --auth-htpasswd --haproxy
/var/tmp/backup/ATP1_backup_svn_etc_grafanadb_haproxy_$(date +\%Y-\%m-\%d).tar.gz
4. mongodump - /var/qps/bin/support/env/env_export.sh --mongo /var/tmp/env_export_$date.tgz
5. patches - cat /etc/broadhop/repositories, check which patches are installed and copy those
patches to the backup directory /home/stack/CPS_BACKUP on OSPD
6. backup the cronjobs by taking backup of the cron directory: /var/spool/cron/ from the
Pcrfclient01/Cluman. Then move the file to CPS_BACKUP on the OSPD.
```

Verifique desde crontab -l si se necesita otra copia de seguridad

Transferir todas las copias de seguridad a OSPD /home/stack/CPS_BACKUP

3. Copia de seguridad del archivo anual desde ESC Master

```
/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
```

Transferir el archivo en OSPD /home/stack/CPS_BACKUP

4. Copia de seguridad de las entradas crontab -l

Cree un archivo txt con crontab -l y ftp en la ubicación remota (en OSPD /home/stack/CPS_BACKUP)

5. Realice una copia de seguridad de los archivos de ruta desde el cliente LB y PCRF

```
Collect and scp the below conifgurations from both LBs and Pcrfclients
route -n /etc/sysconfig/network-script/route-*
```

Procedimiento de restauración

Recuperación de OSPD

El procedimiento de recuperación de OSPD se realiza según las siguientes suposiciones:

1. La copia de seguridad OSPD está disponible desde el servidor OSPD antiguo.

2. La recuperación de OSPD se realizará en el nuevo servidor que es el reemplazo del servidor OSPD antiguo en el sistema. .

Recuperación ESC

1. La VM ESC se puede recuperar si la VM se encuentra en estado de error o de apagado se reinicia con fuerza para activar la VM afectada. Ejecute estos pasos para recuperar ESC.

2. Identifique la VM que se encuentra en estado ERROR o Apagar, una vez que se haya identificado el reinicio duro de la VM ESC. En este ejemplo, está reiniciando auto-test-vnfm1-ESC-0.

```
[root@tb1-baremetal scripts]# nova list | grep auto-test-vnfm1-ESC-

| f03e3cac-a78a-439f-952b-045aea5b0d2c | auto-test-vnfm1-ESC-
0                                     | ACTIVE | -          | running     | auto-testautovnf1-
uas-orchestration=172.57.12.11; auto-testautovnf1-uas-
management=172.57.11.3
                          |
| 79498e0d-0569-4854-a902-012276740bce | auto-test-vnfm1-ESC-
1                                     | ACTIVE | -          | running     | auto-testautovnf1-
uas-orchestration=172.57.12.15; auto-testautovnf1-uas-
management=172.57.11.5
            |

[root@tb1-baremetal scripts]# [root@tb1-baremetal scripts]# nova reboot --hard f03e3cac-a78a-
439f-952b-045aea5b0d2c\
Request to reboot server <Server: auto-test-vnfm1-ESC-0> has been accepted.

[root@tb1-baremetal scripts]#
```

3. Si se elimina la VM ESC y debe volver a activarse. Siga la siguiente secuencia de pasos

```
[stack@pod1-ospd scripts]$ nova list |grep ESC-1
| c566efbf-1274-4588-a2d8-0682e17b0d41 | vnf1-ESC-ESC-
1                                                | ACTIVE | -          | running     | vnf1-
UAS-uas-orchestration=172.168.11.14; vnf1-UAS-uas-
management=172.168.10.4
                         |

[stack@pod1-ospd scripts]$ nova delete vnf1-ESC-ESC-1
Request to delete server vnf1-ESC-ESC-1 has been
accepted.
```

4. Si la VM ESC no se puede recuperar y requiere la restauración de la base de datos, restaure la base de datos a partir de la copia de seguridad realizada anteriormente.

5. Para la restauración de la base de datos ESC, debemos garantizar que el servicio esc se detiene antes de restaurar la base de datos; Para ESC HA, ejecute primero en la VM secundaria y luego en la VM principal.

```
# service keepalived stop
```

6. Verifique el estado del servicio ESC y asegúrese de que todo esté detenido tanto en las VM primarias como secundarias para HA.

```
# escadm status
```

7. Ejecute el script para restaurar la base de datos. Como parte de la restauración de la base de datos a la instancia ESC recién creada, la herramienta promoverá también una de las instancias para ser una ESC principal, montará su carpeta DB en el dispositivo drbd e iniciará la base de datos PostgreSQL.

```
# /opt/cisco/esc/esc-scripts/esc_dbtool.py restore --file
scp://<username>:<password>@<backup_vm_ip>:<filename>
```

8. Reinicie el servicio ESC para completar la restauración de la base de datos. Para HA, ejecute en ambas VM, reinicie el servicio keepalived.

```
# service keepalived start
```

9. Una vez que la máquina virtual se haya restaurado y ejecutado correctamente; asegúrese de que toda la configuración específica de syslog se restaura desde la copia de seguridad conocida anterior exitosa. asegúrese de que se restaura en todas las VM ESC.

```
[admin@auto-test-vnfm2-esc-1 ~]$
[admin@auto-test-vnfm2-esc-1 ~]$ cd /etc/rsyslog.d
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/00-escmanager.conf
00-escmanager.conf

[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/01-messages.conf
01-messages.conf

[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/02-mona.conf
02-mona.conf

[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.conf
rsyslog.conf
```

10. Si el ESC debe reconstruirse a partir de la instantánea OSPD, utilice este comando con el uso de la instantánea tomada durante la copia de seguridad.

```
nova rebuild --poll --name esc_snapshot_27aug2018 esc1
```

11. Compruebe el estado del ESC después de completar la reconstrucción

```
nova list --fileds name,host,status,networks | grep esc
```

12. Comprobar el estado de ESC con el siguiente comando

```
health.sh

Copy Datamodel to a backup file
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli get esc_datamodel/opdata > /tmp/esc_opdata_`date
+%Y%m%d%H%M%S`.txt
```

Cuando ESC no puede iniciar VM

- En algunos casos, ESC no podrá iniciar la VM debido a un estado inesperado. Una solución alternativa es realizar un switchover ESC reiniciando el ESC maestro. La conmutación ESC tardará aproximadamente un minuto. Ejecute health.sh en el nuevo Master ESC para verificar que está activo. Cuando ESC se convierte en Master, ESC puede corregir el estado

de la VM e iniciar la VM. Puesto que esta operación está programada, debe esperar de 5 a 7 minutos para que se complete.

- Puede supervisar /var/log/esc/yangesc.log y /var/log/esc/escmanager.log. Si NO ve que se recupera la máquina virtual después de 5-7 minutos, el usuario tendría que ir y realizar la recuperación manual de las máquinas virtuales afectadas.

- Una vez que la máquina virtual se haya restaurado y ejecutado correctamente; asegúrese de que toda la configuración específica de syslog se restaura desde la copia de seguridad conocida anterior exitosa. Asegúrese de que se restaura en todas las VM ESC

```
root@abautotestvnfm1em-0:/etc/rsyslog.d# pwd
/etc/rsyslog.d

root@abautotestvnfm1em-0:/etc/rsyslog.d# ll

total 28
drwxr-xr-x  2 root root 4096 Jun  7 18:38 ./
drwxr-xr-x 86 root root 4096 Jun  6 20:33 ../]
-rw-r--r--  1 root root  319 Jun  7 18:36 00-vnmf-proxy.conf
-rw-r--r--  1 root root  317 Jun  7 18:38 01-ncs-java.conf
-rw-r--r--  1 root root  311 Mar 17  2012 20-ufw.conf
-rw-r--r--  1 root root  252 Nov 23  2015 21-cloudinit.conf
-rw-r--r--  1 root root 1655 Apr 18  2013 50-default.conf

root@abautotestvnfm1em-0:/etc/rsyslog.d# ls /etc/rsyslog.conf
rsyslog.conf
```

Recuperación de CPS

Restaurar la VM del Cluster Manager en OpenStack

Paso 1 Copie la instantánea de VM del administrador de clúster al servidor blade del controlador como se muestra en el siguiente comando:

```
ls –ltr *snapshot*

Example output: -rw-r--r--. 1 root root 10429595648 Aug 16 02:39 snapshot.raw
```

Paso 2 Cargue la imagen de instantánea en OpenStack desde el almacén de datos:

```
glance image-create --name --file --disk-format qcow2 --container-format bare
```

Paso 3 Verifique si la instantánea se carga con un comando Nova como se muestra en el siguiente ejemplo:

```
nova image-list
```

Figura 2: Ejemplo de salida

```
+--------------------------------------+-----------------------------------+--------+--------------------------------------+
| ID                                   | Name                              | Status | Server                               |
+--------------------------------------+-----------------------------------+--------+--------------------------------------+
| 146719e8-d8a0-4d5a-9b15-2a669cfab81f | CPS_10.9.9_20160803_100301_112.iso | ACTIVE |                                      |
| 1955d56e-4ecf-4269-b53d-b30e73ad57f0 | base_vm                           | ACTIVE |                                      |
| 2bbfb51c-cd05-4b7c-ad77-8362d76578db | cluman_snapshot                   | ACTIVE | 4842ae5a-83a3-48fd-915b-6ca6361adb2c |
| 5eebff44-658a-49a5-a170-1978f6276d18 | imported_image                    | ACTIVE |                                      |
+--------------------------------------+-----------------------------------+--------+--------------------------------------+
```

Paso 4 Según si la VM del administrador de clúster existe o no, puede elegir crear el clúster o reconstruir el clúster:

·Si la instancia de la VM del Cluster Manager no existe, cree la VM de Cluman con un comando Heat o Nova como se muestra en el siguiente ejemplo:

Creación de la VM Cluman con ESC

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli edit-config /opt/cisco/esc/cisco-cps/config/gr/tmo/gen/<original_xml_filename>
```

El clúster de PCRF se producirá con la ayuda del comando anterior y, a continuación, restaurará las configuraciones del administrador de clúster a partir de las copias de seguridad tomadas con el restore config_br.py, mongorestore from dump tomado en backup

```
delete - nova boot --config-drive true --image "" --flavor "" --nic net-id=",v4-fixed-ip=" --nic net-id="network_id,v4-fixed-ip=ip_address" --block-device-mapping "/dev/vdb=2edbac5e-55de-4d4c-a427-ab24ebe66181:::0" --availability-zone "az-2:megh-os2-compute2.cisco.com" --security-groups cps_secgrp "cluman"
```

· Si existe la instancia de la VM del Cluster Manager, utilice un comando nova build para reconstruir la instancia de la VM de Cluman con la instantánea cargada como se muestra:

```
nova rebuild <instance_name> <snapshot_image_name>
```

Por ejemplo:

```
nova rebuild cps-cluman-5f3tujqvbi67 cluman_snapshot
```

Paso 5 Enumera todas las instancias como se muestra y verifique que se haya creado y ejecutado la nueva instancia del administrador del clúster:

```
nova list
```

Figura 3. Ejemplo de salida

```
+--------------------------------------+---------+--------+------------+-------------+-----------------------------------------------+
| ID                                   | Name    | Status | Task State | Power State | Networks                                      |
+--------------------------------------+---------+--------+------------+-------------+-----------------------------------------------+
| ac3d2dbc-7b0e-4df4-a690-7f84ca3032bd | cluman | ACTIVE | -          | Running     | management=172.20.67.34; internal=172.20.70.34 |
```

Restaurar los últimos parches del sistema

```
1.       Copy the patch files to cluster manager which were backed up in OSPD /home/stack/CPS_BACKUP
2.       Login to the Cluster Manager as a root user.
3.       Untar the patch by executing the following command:  tar -xvzf [patch name].tar.gz
4.       Edit /etc/broadhop/repositories and add the following entry:  file:///$path_to_the plugin/[component name]
```

```
5.       Run build_all.sh script to create updated QPS packages:
/var/qps/install/current/scripts/build_all.sh
6.       Shutdown all software components on the target VMs:  runonall.sh sudo monit stop all
7.       Make sure all software components are shutdown on target VMs:  statusall.sh
```

Nota: Todos los componentes del software deben mostrar No supervisado como estado actual.

```
8.       Update the qns VMs with the new software using reinit.sh script:
/var/qps/install/current/scripts/upgrade/reinit.sh
9.       Restart all software components on the target VMs:  runonall.sh sudo monit start all
10.     Verify that the component is updated, run:  about.sh
```

Restauración de Cronworks

1. Mueva el archivo de copia de seguridad de OSPD a Cluman/Pcrfclient01.

2. Ejecute el comando para activar el cronjob desde la copia de seguridad.

```
#crontab Cron-backup
```

3. Verifique si los trabajos cronjob han sido activados por el siguiente comando.

```
#crontab -l
```

Restauración de VM individuales en el clúster

Para volver a implementar la VM pcrfclient01:

Paso 1 Inicie sesión en la VM Cluster Manager como usuario raíz.

Paso 2 Observe el UUID del repositorio SVN usando el siguiente comando:

```
svn info http://pcrfclient02/repos | grep UUID
```

El comando emitirá el UUID del repositorio.

Por ejemplo: UUID del repositorio: ea50bbd2-5726-46b8-b807-10f4a7424f0e

Paso 3 Importe los datos de configuración del creador de políticas de copia de seguridad en el Administrador de clústeres, como se muestra en el ejemplo siguiente:

```
config_br.py -a import --etc-oam --svn --stats --grafanadb --auth-htpasswd --users
/mnt/backup/oam_backup_27102016.tar.gz
```

Nota: Muchas implementaciones ejecutan un trabajo cron que realiza copias de seguridad de los datos de configuración de forma regular.ConsulteCopia de seguridad del repositorio de subversión para obtener más detalles.

Paso 4 Para generar los archivos de VM en el Cluster Manager utilizando las últimas configuraciones, ejecute el siguiente comando:

```
/var/qps/install/current/scripts/build/build_svn.sh
```

Paso 5 Para implementar la VM pcrfclient01, realice una de las siguientes acciones:

En OpenStack, utilice la plantilla HEAT o el comando Nova para volver a crear la máquina virtual. Para obtener más información, consulte Guía de instalación de CPS para OpenStack.

Paso 6 Vuelva a establecer la sincronización maestra/esclava SVN entre pcrfclient01 y pcrfclient02 con pcrfclient01 como maestro ejecutando la siguiente serie de comandos.

Si SVN ya está sincronizado, no ejecute estos comandos.

Para verificar si SVN está sincronizado, ejecute el siguiente comando desde pcrfclient02.

Si se devuelve un valor, el SVN ya está sincronizado:

```
/usr/bin/svn propget svn:sync-from-url --revprop -r0 http://pcrfclient01/repos
```

Ejecute los siguientes comandos desde pcrfclient01:

```
/bin/rm -fr /var/www/svn/repos

/usr/bin/svnadmin create /var/www/svn/repos

/usr/bin/svn propset --revprop -r0 svn:sync-last-merged-rev 0 http://pcrfclient02/repos-proxy-sync

/usr/bin/svnadmin setuuid /var/www/svn/repos/ "Enter the UUID captured in step 2"

/etc/init.d/vm-init-client /

var/qps/bin/support/recover_svn_sync.sh
```

Paso 7 Si pcrfclient01 es también la VM árbitro, ejecute los siguientes pasos:

a) Cree los scripts de inicio/parada mongodb basándose en la configuración del sistema. No todas las implementaciones tienen todas estas bases de datos configuradas.

> **Nota:** Consulte /etc/broadhop/mongoConfig.cfg para determinar qué bases de datos deben configurarse.

```
cd /var/qps/bin/support/mongo

build_set.sh --session --create-scripts
build_set.sh --admin --create-scripts
build_set.sh --spr --create-scripts
build_set.sh --balance --create-scripts
build_set.sh --audit --create-scripts
build_set.sh --report --create-scripts
```

b) Iniciar el proceso mongo:

```
/usr/bin/systemctl start sessionmgr-XXXXX
```

c) Espere a que se inicie el árbitro y luego ejecute diagnostics.sh —get_réplica_status para verificar el estado del conjunto de réplicas.

Para volver a implementar la VM pcrfclient02:

Paso 1 Inicie sesión en la VM Cluster Manager como usuario raíz

Paso 2 Para generar los archivos de VM en el Cluster Manager utilizando las últimas configuraciones, ejecute el siguiente comando:

```
/var/qps/install/current/scripts/build/build_svn.sh
```

Paso 3 Para implementar la VM pcrfclient02, realice una de las siguientes acciones:
En OpenStack, utilice la plantilla HEAT o el comando Nova para volver a crear la máquina virtual. Para obtener más información, consulte Guía de instalación de CPS para OpenStack.

Paso 4 Secure Shell al pcrfclient01:

```
ssh pcrfclient01
```

Paso 5 Ejecute el siguiente script para recuperar los repos SVN de pcrfclient01:

```
/var/qps/bin/support/recover_svn_sync.sh
```

Para volver a implementar una VM de sessionmgr:

Paso 1 Inicie sesión en la VM Cluster Manager como usuario raíz

Paso 2 Para implementar la VM sessionmgr y reemplazar la VM fallida o corrupta, realice una de las siguientes acciones:

En OpenStack, utilice la plantilla HEAT o el comando Nova para volver a crear la máquina virtual. Para obtener más información, consulte Guía de instalación de CPS para OpenStack

Paso 3 Cree los scripts mongodb start/stop en función de la configuración del sistema.

No todas las implementaciones tienen todas estas bases de datos configuradas. Consulte /etc/broadhop/mongoConfig.cfg para determinar qué bases de datos deben configurarse

```
cd /var/qps/bin/support/mongo

build_set.sh --session --create-scripts
build_set.sh --admin --create-scripts
build_set.sh --spr --create-scripts
build_set.sh --balance --create-scripts
build_set.sh --audit --create-scripts
build_set.sh --report --create-scripts
```

Paso 4 Proteja el shell a la VM sessionmgr e inicie el proceso mongo:

```
ssh sessionmgrXX

/usr/bin/systemctl start sessionmgr-XXXXX
```

Paso 5 Espere a que se inicien los miembros y a que se sincronicen los miembros secundarios y, a continuación, ejecute diagnostics.sh —get_réplica_status para comprobar el estado de la base de datos.

Paso 6 Para restaurar la base de datos de Session Manager, utilice uno de los siguientes comandos de ejemplo dependiendo de si la copia de seguridad se realizó con —mongo-all o con la opción —mongo:

```
• config_br.py -a import --mongo-all --users /mnt/backup/Name of backup

or

• config_br.py -a import --mongo --users /mnt/backup/Name of backup
```

Para volver a implementar la máquina virtual Policy Director (Load Balancer):

Paso 1 Inicie sesión en la VM Cluster Manager como usuario raíz.

Paso 2 Para importar los datos de configuración del creador de políticas de respaldo en el Administrador de clústeres, ejecute el siguiente comando:

```
config_br.py -a import --network --haproxy --users /mnt/backup/lb_backup_27102016.tar.gz
```

Paso 3 Para generar los archivos de VM en el Cluster Manager utilizando las últimas configuraciones, ejecute el siguiente comando:

```
/var/qps/install/current/scripts/build/build_svn.sh
```

Paso 4 Para implementar la máquina virtual lb01, realice una de las siguientes acciones:

En OpenStack, utilice la plantilla HEAT o el comando Nova para volver a crear la máquina virtual. Para obtener más información, consulte Guía de instalación de CPS para OpenStack.

Para volver a implementar la VM de Policy Server (QNS):

Paso 1 Inicie sesión en la VM Cluster Manager como usuario raíz.

Paso 2 Importe los datos de configuración del creador de políticas de copia de seguridad en el Administrador de clústeres, como se muestra en el ejemplo siguiente:

```
config_br.py -a import --users /mnt/backup/qns_backup_27102016.tar.gz
```

Paso 3 Para generar los archivos de VM en el Cluster Manager utilizando las últimas configuraciones, ejecute el siguiente comando:

```
/var/qps/install/current/scripts/build/build_svn.sh
```

Paso 4 Para implementar la VM qns, realice una de las siguientes acciones:
En OpenStack, utilice la plantilla HEAT o el comando Nova para volver a crear la máquina virtual. Para obtener más información, consulte Guía de instalación de CPS para OpenStack

Procedimiento general para restaurar la base de datos

Paso 1 Ejecute el siguiente comando para restaurar la base de datos:

```
config_br.py –a import --mongo-all /mnt/backup/backup_$date.tar.gz where $date is the timestamp when the export was made.
```

Por ejemplo,

```
config_br.py –a import --mongo-all /mnt/backup/backup_27092016.tgz
```

Paso 2 Inicie sesión en la base de datos y verifique si se está ejecutando y si se puede acceder a ella:

1. Inicie sesión en el administrador de sesiones:

```
mongo --host sessionmgr01 --port $port
```

donde $port es el número de puerto de la base de datos para verificar. Por ejemplo, 27718 es el puerto de balance predeterminado.

2. Para mostrar la base de datos, ejecute el siguiente comando:

```
show dbs
```

3. Cambie el shell mongo a la base de datos ejecutando el siguiente comando:

```
use $db
```

donde $db es un nombre de base de datos que se muestra en el comando anterior.

El comando 'use' conmuta el shell mongo a esa base de datos.

Por ejemplo,

```
use balance_mgmt
```

4. Para mostrar las colecciones, ejecute el siguiente comando:

```
show collections
```

5. Para mostrar el número de registros en la colección, ejecute el siguiente comando:

```
db.$collection.count()

For example, db.account.count()
```

El ejemplo anterior mostrará el número de registros en la "cuenta" de la colección en la base de datos Balance (balance_mgmt).

Restauración del repositorio de subversion

Para restaurar los datos de configuración de Policy Builder desde una copia de seguridad, ejecute el siguiente comando:

```
config_br.py -a import --svn /mnt/backup/backup_$date.tgz where, $date is the date when the cron created the backup file.
```

Restaurar panel de Grafana

Puede restaurar el panel Grafana mediante el siguiente comando:

```
config_br.py -a import --grafanadb /mnt/backup/
```

Validación de la restauración

Después de restaurar los datos, verifique el sistema en funcionamiento ejecutando el siguiente comando:

```
/var/qps/bin/diag/diagnostics.sh
```