Procedimientos de respaldo y restauración para varios componentes Ultra-M

Contenido

[Introducción](#)
[Antecedentes](#)
[Abreviaturas](#)
[Procedimientos de copia de seguridad](#)
[Respaldo OSPD](#)
[Copia de seguridad de AutoDeploy](#)
[Copia de seguridad AutoIT-VNF](#)
[Copia de seguridad AutoVNF](#)
[Copia de seguridad ESC](#)
[Copia de seguridad de EM](#)
[Copia de seguridad de StarOS](#)
[Procedimiento de restauración](#)
[Recuperación de OSPD](#)
[Recuperación de AutoDeploy](#)
[Recuperación de AutoIT-VNF](#)
[Recuperación de AutoVNF](#)
[Recuperación ESC](#)
[Recuperación de EM](#)
[Recuperación de StarOS](#)

Introducción

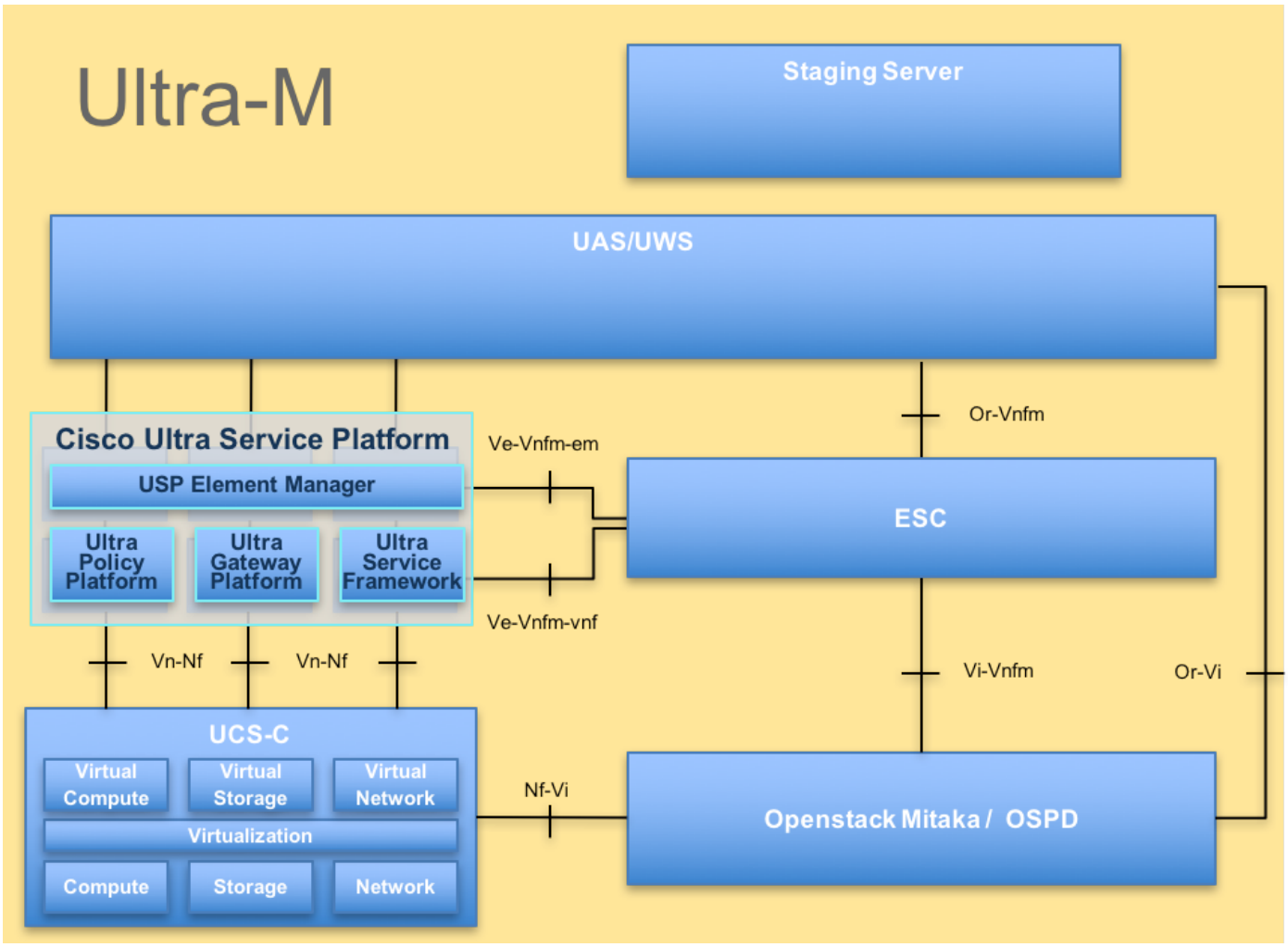
Este documento describe los pasos necesarios para realizar una copia de seguridad y restaurar una máquina virtual (VM) en una configuración Ultra-M que aloja StarOS Virtual Network Functions (VNF).

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 (VM):

- TI automática
- Implementación automática
- Servicios de automatización (UAS)
- Administrador de elementos (EM)
- Controlador de servicios elásticos (ESC)
- Función de control (CF)
- Función de sesión (SF)

La arquitectura de alto nivel de Ultra-M y los componentes involucrados se ilustran en esta imagen:



Este documento está dirigido al personal de Cisco que está familiarizado con la plataforma Cisco Ultra-M.

> **Nota:** Se considera la versión Ultra M 5.1.x para definir los procedimientos en este documento.

Abreviaturas

VNF	Función de red virtual
CF	Función de control
SF	Función de servicio
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

EM	Administrador de elementos
UAS	Servicios de ultra automatización
UUID	Identificador único universal

Procedimientos 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 interna 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 Undercloud a un archivo denominado **undercloud-backup-[timestamp].tar.gz** y transferirlo 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 de AutoDeploy

1. AutoDeploy requiere que se realice una copia de seguridad de estos datos:

- AutoDeploy Confd Configuration Database (CDB)
- Configuración de AutoDeploy
- Registros de AutoDeploy
- Configuración de Syslog

2. Después de cada activación/desactivación se requiere una copia de seguridad de los datos de CDB configurados de AutoDeploy y una configuración en ejecución, así como garantizar que los datos se transfieren a un servidor de respaldo.

3. AutoDeploy se ejecuta en modo independiente y, si se pierden estos datos, no podrá desactivar correctamente la implementación. Por lo tanto, es obligatorio realizar la copia de seguridad de los datos de la configuración y CDB.

```
ubuntu@auto-deploy-iso-2007-uas-0:~$ sudo -i
root@auto-deploy-iso-2007-uas-0:~# service uas-confd stop
uas-confd stop/waiting

root@auto-deploy:/home/ubuntu# service autodeploy status
autodeploy start/running, process 1313

root@auto-deploy:/home/ubuntu# service autodeploy stop
autodeploy stop/waiting

root@auto-deploy-iso-2007-uas-0:~# cd /opt/cisco/usp/uas/confd-6.3.1/var/confd
root@auto-deploy-iso-2007-uas-0:/opt/cisco/usp/uas/confd-6.3.1/var/confd# tar cvf
autodeploy_cdb_backup.tar cdb/

cdb/
cdb/O.cdb
cdb/C.cdb
cdb/aaa_init.xml
cdb/A.cdb
```

4. Copie **autoDeploy_cdb_backup.tar** en el servidor de respaldo.

5. Realice una copia de seguridad de la configuración en ejecución en AutoDeploy y transfiéela a un servidor de respaldo.

```
root@auto-deploy:/home/ubuntu# confd_cli -u admin -C

Welcome to the ConfD CLI

admin connected from 127.0.0.1 using console on auto-deploy

auto-deploy#show running-config | save backup-config-$date.cfg à Replace the $date to
appropriate date and POD reference
auto-deploy#
```

6. Inicie el servicio AutoDeploy Confid.

```
root@auto-deploy-iso-2007-uas-0:~# service uas-confd start
uas-confd start/running, process 13852


root@auto-deploy:/home/ubuntu# service autodeploy start
autodeploy start/running, process 8835
```

7. Navegue hasta el directorio de scripts y recopile los registros de la VM AutoDeploy.

```
cd /opt/cisco/usp/uas/scripts
```

8. Inicie el script **collection-uas-logs.sh** para recolectar los registros.

```
sudo ./collect-uas-logs.sh
```

9. Realice la copia de seguridad de la imagen ISO desde AutoDeploy y transfiéela al servidor de respaldo.

```
root@POD1-5-1-7-2034-auto-deploy-uas-0:/home/ubuntu# /home/ubuntu/isos
root@POD1-5-1-7-2034-auto-deploy-uas-0:/home/ubuntu/isos# ll

total 4430888
drwxr-xr-x 2 root   root         4096 Dec 20 01:17 ./
drwxr-xr-x 5 ubuntu ubuntu       4096 Dec 20 02:31 ../
-rwxr-xr-x 1 ubuntu ubuntu 4537214976 Oct 12 03:34 usp-5_1_7-2034.iso*
```

10. Recopile la configuración de syslog y guárdela en el servidor de respaldo.

```
ubuntu@auto-deploy-vnf-iso-5-1-5-1196-uas-0:~$sudo su
root@auto-deploy-vnf-iso-5-1-5-1196-uas-0:/home/ubuntu#ls /etc/rsyslog.d/00-autodeploy.conf
00-autodeploy.conf
root@auto-deploy-vnf-iso-5-1-5-1196-uas-0:/home/ubuntu#ls /etc/rsyslog.conf
rsyslog.conf
```

Copia de seguridad AutoIT-VNF

AutoIT-VNF es una VM sin estado, por lo que no hay base de datos (DB) a la que se deba realizar una copia de seguridad. AutoIT-VNF es responsable de la administración de paquetes junto con el repositorio de administración de configuración para Ultra-M, por lo tanto, es esencial que se tomen esas copias de seguridad.

1. Realice la copia de seguridad de las configuraciones de StarOS de día 0 y transfiéralas al servidor de respaldo.

```
root@auto-it-vnf-iso-5-8-uas-0:/home/ubuntu# cd /opt/cisco/usp/uploads/
root@auto-it-vnf-iso-5-8-uas-0:/opt/cisco/usp/uploads# ll
total 12
drwxrwxr-x  2 uspadmin usp-data 4096 Nov  8 23:28 ./
drwxr-xr-x 15 root     root     4096 Nov  8 23:53 ../
-rw-rw-r--  1 ubuntu   ubuntu    985 Nov  8 23:28 system.cfg
```

2. Navegue hasta el directorio de scripts y recopile los registros de la VM AutoIT.

```
cd /opt/cisco/usp/uas/scripts
```

3. Inicie el script **collection-uas-logs.sh** para recolectar los registros.

```
sudo ./collect-uas-logs.sh
```

4. Recopile la copia de seguridad de la configuración de syslog y guárdela en el servidor de respaldo.

```
ubuntu@auto-it-vnf-iso-5-1-5-1196-uas-0:~$sudo su

root@auto-it-vnf-iso-5-1-5-1196-uas-0:/home/ubuntu#ls /etc/rsyslog.d/00-autoit-vnf.conf

00-autoit-vnf.conf

root@auto-it-vnf-iso-5-1-5-1196-uas-0:ls /etc/rsyslog.conf

rsyslog.conf
```

Copia de seguridad AutoVNF

AutoVNF es responsable de activar VNFM y VNF individuales. AutoDeploy envía la configuración necesaria para crear instancias de VNFM. y VNF a AutoVNF y AutoVNF realiza esta operación. Para activar VNFM, AutoVNF hablará directamente con VIM/OpenStack y después de que el VNFM esté activo, AutoVNF utiliza VNFM para activar VNF.

AutoVNF tiene redundancia 1:N y en una configuración Ultra-M, hay tres VM AutoVNF ejecutándose. La falla AutoVNF única se soporta en Ultra-M y la recuperación es factible.

> **Nota:** Si hay más de una falla, no se admite y podría requerir la reimplementación del sistema.

Detalles de la copia de seguridad de AutoVNF:

- configuración en ejecución
- Base de datos CDB de ConfD
- Registros AutoVNF (de cada instancia de AutoVNF)
- Configuración de Syslog

Se recomienda realizar copias de seguridad antes de cualquier activación/desactivación en el sitio dado y cargadas en el servidor de respaldo.

1. Inicie sesión en AutoVNF maestro y valide que es **confd-master**.

```
root@auto-testautovnf1-uas-1:/home/ubuntu# confd_cli -u admin -C

Welcome to the ConfD CLI
admin connected from 127.0.0.1 using console on auto-testautovnf1-uas-1
auto-testautovnf1-uas-1#show uas
uas version 1.0.1-1
uas state ha-active
uas ha-vip 172.57.11.101

INSTANCE IP   STATE  ROLE
-----------------------------------
172.57.12.6   alive  CONFD-SLAVE
172.57.12.7   alive  CONFD-MASTER
172.57.12.13  alive  NA

auto-testautovnf1-uas-1#exit

root@auto-testautovnf1-uas-1:/home/ubuntu# ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
1000
   link/ether fa:16:3e:c7:dc:89 brd ff:ff:ff:ff:ff:ff
   inet 172.57.12.7/24 brd 172.57.12.255 scope global eth0
      valid_lft forever preferred_lft forever
```

```
   inet6 fe80::f816:3eff:fec7:dc89/64 scope link
      valid_lft forever preferred_lft forever

3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
1000
   link/ether fa:16:3e:10:29:1b brd ff:ff:ff:ff:ff:ff
   inet 172.57.11.101/24 brd 172.57.11.255 scope global eth1
      valid_lft forever preferred_lft forever
   inet6 fe80::f816:3eff:fe10:291b/64 scope link
      valid_lft forever preferred_lft forever
```

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

```
root@auto-testautovnf1-uas-1:/home/ubuntu# confd_cli -u admin -C
Welcome to the ConfD CLI
admin connected from 127.0.0.1 using console on auto-testautovnf1-uas-1
auto-testautovnf1-uas-1#show running-config | save running-autovnf-12202017.cfg
auto-testautovnf1-uas-1#exit
root@auto-testautovnf1-uas-1:/home/ubuntu# ll running-autovnf-12202017.cfg
-rw-r--r-- 1 root   root   18181 Dec 20 19:03 running-autovnf-12202017.cfg
```

3. Realice una copia de seguridad de CDB y transfiera el archivo al servidor de copia de seguridad.

```
root@auto-testautovnf1-uas-1:/opt/cisco/usp/uas/confd-6.3.1/var/confd# tar cvf
autovnf_cdb_backup.tar cdb/
cdb/
cdb/O.cdb
cdb/C.cdb
cdb/aaa_init.xml
cdb/vpc.xml
cdb/A.cdb
cdb/gilan.xml

root@auto-testautovnf1-uas-1:/opt/cisco/usp/uas/confd-6.3.1/var/confd#
root@auto-testautovnf1-uas-1:/opt/cisco/usp/uas/confd-6.3.1/var/confd# ll autovnf_cdb_backup.tar
-rw-r--r-- 1 root root 1198080 Dec 20 19:08 autovnf_cdb_backup.tar
```

4. Navegue hasta el directorio de scripts, recopile los registros y transfiera al servidor de respaldo.

```
cd /opt/cisco/usp/uas/scripts

sudo ./collect-uas-logs.sh
```

5. Inicie sesión en la instancia en espera de AutoVNF y realice estos pasos para recopilar los registros y transferirlos al servidor de respaldo.

6. Realice una copia de seguridad de la configuración de syslog en las VM de AutoVNF principales y en espera y transfiéalas al servidor de respaldo.

```
ubuntu@auto-testautovnf1-uas-1:~$sudo su
root@auto-testautovnf1-uas-1:/home/ubuntu#ls /etc/rsyslog.d/00-autovnf.conf
00-autovnf.conf
```

```
root@auto-testautovnf1-uas-1:/home/ubuntu#ls /etc/rsyslog.conf
rsyslog.conf
```

Copia de seguridad ESC

1. AutoVNF es responsable de activar ESC en una solución Ultra-M interactuando directamente con VIM. AutoVNF/EM pasa la configuración específica de VNF a ESC y ESC, a su vez, activará VNF interactuando con VIM.

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

> **Nota:** Si hay más de una falla, no se admite y podría requerir la reimplementación del 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 que usted siga las actividades en el VNF/POD/Site dado.

4. Verifique que el estado de ESC sea bueno con el uso de 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 una 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 de copia de seguridad

1. Establezca ESC en modo de mantenimiento.

2. Inicie sesión en ESC VM y ejecute este comando antes de realizar la copia de seguridad.

```
[admin@auto-test-vnfm1-esc-0 admin]# sudo bash
[root@auto-test-vnfm1-esc-0 admin]# cp /opt/cisco/esc/esc-scripts/esc_dbtool.py
/opt/cisco/esc/esc-scripts/esc_dbtool.py.bkup
[root@auto-test-vnfm1-esc-0 admin]# 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@auto-test-vnfm1-esc-0 admin]# escadm op_mode set --mode=maintenance
```

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

```
[root@auto-test-vnfm1-esc-0 admin]# escadm op_mode show
```

4. Base de datos de respaldo con el uso de la herramienta de restauración de respaldo de la base de datos disponible en ESC.

```
[root@auto-test-vnfm1-esc-0 admin]# sudo /opt/cisco/esc/esc-scripts/esc_dbtool.py backup --file
 scp://<username>:<password>@<backup_vm_ip>:<filename>
```

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

```
[root@auto-test-vnfm1-esc-0 admin]# escadm op_mode set --mode=operation

[root@auto-test-vnfm1-esc-0 admin]# escadm op_mode show
```

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

```
[root@auto-test-vnfm1-esc-0 admin]# /opt/cisco/esc/esc-scripts

sudo ./collect_esc_log.sh
```

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

8. Recopile la copia de seguridad de la configuración de syslog en el ESC VMS 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 EM

1. Después de que VNFM/ESC esté activo, AutoVNF utiliza ESC para activar el clúster EM. Una vez que el clúster de EM esté activo, EM interactuará con ESC para activar VNF (VPC/StarOS).

2. EM tiene redundancia 1:N en la solución Ultra-M. Hay un clúster de tres VM EM y Ultra-M admite la recuperación de una única falla de VM.

> **Nota:** Si hay más de una falla, no se admite y podría requerir la reimplementación del sistema.

Detalles de la copia de seguridad de EM:

- Configuración en ejecución
- NCS DB
- Registros de EM (desde las dos VM activas/en espera de NCS)
- Configuración de Syslog

3. La frecuencia de las copias de seguridad de la base de datos de EM es complicada y debe manejarse con cuidado, ya que ESC supervisa y mantiene las diferentes máquinas de estado para diversas VM de VNF implementadas. Se recomienda realizar estas copias de seguridad después de seguir las actividades en un VNF/POD/Site determinado.

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

```
ubuntu@vnfd1deploymentem-0:~$ sudo -i
root@vnfd1deploymentem-0:~# ncs_cli -u admin -C

admin connected from 127.0.0.1 using console on vnfd1deploymentem-0
admin@scm# show running-config | save em-running-12202017.cfg

root@vnfd1deploymentem-0:~# ll em-running-12202017.cfg
-rw-r--r-- 1 root root 19957 Dec 20 23:01 em-running-12202017.cfg
```

5. Realice la copia de seguridad de la base de datos de EM NCS y transfiera el archivo al servidor de copia de seguridad.

```
ubuntu@vnfd1deploymentem-0:~$ sudo -i
root@vnfd1deploymentem-0:~# cd /opt/cisco/em/git/em-scm/ncs-cdb
root@vnfd1deploymentem-0:/opt/cisco/em/git/em-scm/ncs-cdb# ll

total 472716
drwxrwxr-x 2 root root      4096 Dec 20 02:53 ./
drwxr-xr-x 9 root root      4096 Dec 20 19:22 ../
-rw-r--r-- 1 root root       770 Dec 20 02:48 aaa_users.xml
-rw-r--r-- 1 root root     70447 Dec 20 02:53 A.cdb
-rw-r--r-- 1 root root 483927031 Dec 20 02:48 C.cdb
-rw-rw-r-- 1 root root        47 Jul 27 05:53 .gitignore
-rw-rw-r-- 1 root root       332 Jul 27 05:53 global-settings.xml
-rw-rw-r-- 1 root root       621 Jul 27 05:53 jvm-defaults.xml
-rw-rw-r-- 1 root root      3392 Jul 27 05:53 nacm.xml
-rw-r--r-- 1 root root      6156 Dec 20 02:53 O.cdb
-rw-r--r-- 1 root root     13041 Dec 20 02:48 startup-vnfd.xml

root@vnfd1deploymentem-0:/opt/cisco/em/git/em-scm/ncs-cdb#
root@vnfd1deploymentem-0:/opt/cisco/em/git/em-scm# tar cvf em_cdb_backup.tar ncs-cdb

ncs-cdb/
ncs-cdb/O.cdb
ncs-cdb/C.cdb
ncs-cdb/nacm.xml
ncs-cdb/jvm-defaults.xml
ncs-cdb/A.cdb
ncs-cdb/aaa_users.xml
ncs-cdb/global-settings.xml
ncs-cdb/.gitignore
ncs-cdb/startup-vnfd.xml

root@vnfd1deploymentem-0:/opt/cisco/em/git/em-scm# ll em_cdb_backup.tar
-rw-r--r-- 1 root root 484034560 Dec 20 23:06 em_cdb_backup.tar
```

6. Navegue hasta el directorio de scripts, recopile los registros y transfiéelos al servidor de respaldo.

```
/opt/cisco/em-scripts

sudo ./collect-em-logs.sh
```

- Repita el mismo procedimiento para recopilar el registro de la VM en espera de NCS
- Realice una copia de seguridad de la configuración de syslog en todas las VM de EM y transfiéalas al servidor de respaldo

```
root@vnfd1deploymentem-0:/etc/rsyslog.d# pwd
/etc/rsyslog.d

root@vnfd1deploymentem-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@vnfd1deploymentem-0:/etc/rsyslog.d# ls /etc/rsyslog.conf
rsyslog.conf
```

Copia de seguridad de StarOS

Para StarOS, es necesario realizar una copia de seguridad de esta información.

- Es necesario realizar copias de seguridad de los registros de datos (CDR) en un servidor remoto a intervalos regulares
- Configuración de día 0 aplicada en el momento de la implementación del sistema
- Configuración de día N
- SSD
- Configuración de Syslog

Procedimiento de restauración

Recuperación de OSPD

El procedimiento de recuperación de OSPD se realiza en base a estas suposiciones

- La copia de seguridad OSPD está disponible desde el servidor OSPD antiguo
- La recuperación de OSPD se realizará en el nuevo servidor que es el reemplazo del servidor OSPD antiguo en el sistema.

Recuperación de AutoDeploy

1. La VM AutoDeploy se puede recuperar cuando la VM se encuentra en estado de error o apagado, realice un reinicio duro para activar la VM afectada. Ejecute estas comprobaciones para ver si esto ayuda a recuperar AutoDeploy.

```
Checking AutoDeploy Processes
Verify that key processes are running on the AutoDeploy VM:

root@auto-deploy-iso-2007-uas-0:~# initctl status autodeploy
autodeploy start/running, process 1771

root@auto-deploy-iso-2007-uas-0:~# ps -ef | grep java
root      1788  1771  0 May24 ?        00:00:41 /usr/bin/java -jar
/opt/cisco/usp/apps/autodeploy/autodeploy-1.0.jar com.cisco.usp.autodeploy.Application --
autodeploy.transaction-log-store=/var/log/cisco-uas/autodeploy/transactions
Stopping/Restarting AutoDeploy Processes

#To start the AutoDeploy process:
root@auto-deploy-iso-2007-uas-0:~# initctl start autodeploy
autodeploy start/running, process 11094

#To stop the AutoDeploy process:
root@auto-deploy-iso-2007-uas-0:~# initctl stop autodeploy
autodeploy stop/waiting

#To restart the AutoDeploy process:
```

```
root@auto-deploy-iso-2007-uas-0:~# initctl restart autodeploy
autodeploy start/running, process 11049

#If the VM is in ERROR or shutdown state, hard-reboot the AutoDeploy VM

[stack@pod1-ospd ~]$ nova list |grep auto-deploy
| 9b55270a-2dcd-4ac1-aba3-bf041733a0c9 | auto-deploy-ISO-2007-uas-
0                                    | ACTIVE | -          | running     | mgmt=172.16.181.12,
10.84.123.39

[stack@pod1-ospd ~]$ nova reboot –hard 9b55270a-2dcd-4ac1-aba3-bf041733a0c9
```

2. Si AutoDeploy es irrecuperable, siga estos procedimientos para restaurarlo al estado en el que estaba antes. Utilice la copia de seguridad realizada anteriormente.

```
[stack@pod1-ospd ~]$ nova list |grep auto-deploy
| 9b55270a-2dcd-4ac1-aba3-bf041733a0c9 | auto-deploy-ISO-2007-uas-
0                                    | ACTIVE | -          | running     | mgmt=172.16.181.12,
10.84.123.39 [stack@pod1-ospd ~]$ cd /opt/cisco/usp/uas-installer/scripts

[stack@pod1-ospd ~]$ ./auto-deploy-booting.sh --floating-ip 10.1.1.2 --delete
```

3. Después de eliminar AutoDeploy, vuelva a crearlo con la misma dirección **floatingip**.

```
[stack@pod1-ospd ~]$ cd /opt/cisco/usp/uas-installer/scripts

[stack@pod1-ospd scripts]$ ./auto-deploy-booting.sh --floating-ip 10.1.1.2

2017-11-17 07:05:03,038 - INFO: Creating AutoDeploy deployment (1 instance(s)) on
'http://10.1.1.2:5000/v2.0' tenant 'core' user 'core', ISO 'default'
2017-11-17 07:05:03,039 - INFO: Loading image 'auto-deploy-ISO-5-1-7-2007-usp-uas-1.0.1-
1504.qcow2' from '/opt/cisco/usp/uas-installer/images/usp-uas-1.0.1-1504.qcow2'
2017-11-17 07:05:14,603 - INFO: Loaded image 'auto-deploy-ISO-5-1-7-2007-usp-uas-1.0.1-
1504.qcow2'
2017-11-17 07:05:15,787 - INFO: Assigned floating IP '10.1.1.2' to IP '172.16.181.7'
2017-11-17 07:05:15,788 - INFO: Creating instance 'auto-deploy-ISO-5-1-7-2007-uas-0'
2017-11-17 07:05:42,759 - INFO: Created instance 'auto-deploy-ISO-5-1-7-2007-uas-0'
2017-11-17 07:05:42,759 - INFO: Request completed, floating IP: 10.1.1.2]
```

4. Copie el archivo **AutoDeploy.cfg**, ISO y el archivo **confd_backup tar** del servidor de respaldo en la VM AutoDeploy.

5. Restaure los archivos cdb confd desde el archivo .tar de copia de seguridad.

```
ubuntu@auto-deploy-iso-2007-uas-0:~# sudo -i
ubuntu@auto-deploy-iso-2007-uas-0:#  service uas-confd stop
uas-confd stop/waiting

root@auto-deploy-iso-2007-uas-0:# cd /opt/cisco/usp/uas/confd-6.3.1/var/confd
root@auto-deploy-iso-2007-uas-0:/opt/cisco/usp/uas/confd-6.3.1/var/confd# tar xvf
/home/ubuntu/ad_cdb_backup.tar

cdb/
cdb/O.cdb
cdb/C.cdb
cdb/aaa_init.xml
cdb/A.cdb

root@auto-deploy-iso-2007-uas-0~# service uas-confd start
uas-confd start/running, process 2036
```

```
#Restart AutoDeploy process

root@auto-deploy-iso-2007-uas-0~# service autodeploy restart
autodeploy start/running, process 2144


#Check that confd was loaded properly by checking earlier transactions.

root@auto-deploy-iso-2007-uas-0:~# confd_cli -u admin -C
Welcome to the ConfD CLI
admin connected from 127.0.0.1 using console on auto-deploy-iso-2007-uas-0

auto-deploy-iso-2007-uas-0#show transaction

                                  SERVICE
       SITE

                                  DEPLOYMENT
SITE  TX    AUTOVNF  VNF  AUTOVNF

TX ID          TX TYPE             ID          DATE AND TIME
STATUS              ID    ID    ID       ID   TX ID

-------------------------------------------------------------------------------------------------
-----------------------------------
1512571978613  service-deployment  tb5bxb      2017-12-06T14:52:59.412+00:00  deployment-success
```

6. Si la máquina virtual se ha restaurado y se está ejecutando correctamente; asegúrese de que toda la configuración específica de syslog se restaura desde la copia de seguridad conocida anterior exitosa.

```
ubuntu@auto-deploy-vnf-iso-5-1-5-1196-uas-0:~$sudo su
root@auto-deploy-vnf-iso-5-1-5-1196-uas-0:/home/ubuntu#ls /etc/rsyslog.d/00-autodeploy.conf
00-autodeploy.conf

root@auto-deploy-vnf-iso-5-1-5-1196-uas-0:/home/ubuntu#ls /etc/rsyslog.conf
rsyslog.conf
```

Recuperación de AutoIT-VNF

1. La VM AutoIT-VNF es recuperable, si la VM está en estado de error o apagado, realice un reinicio duro para activar la VM afectada. Ejecute estos pasos para recuperar AutoIT-VNF.

```
Checking AutoIT-VNF Processes

Verify that key processes are running on the AutoIT-VNF VM:

root@auto-it-vnf-iso-5-1-5-1196-uas-0:~# service autoit status
AutoIT-VNF is running.

#Stopping/Restarting AutoIT-VNF Processes

root@auto-it-vnf-iso-5-1-5-1196-uas-0:~# service autoit stop
AutoIT-VNF API server stopped.

#To restart the AutoIT-VNF processes:

root@auto-it-vnf-iso-5-1-5-1196-uas-0:~# service autoit restart
AutoIT-VNF API server stopped.
Starting AutoIT-VNF
```

```
/opt/cisco/usp/apps/auto-it/vnf
AutoIT API server started.

#If the VM is in ERROR or shutdown state, hard-reboot the AutoDeploy VM

[stack@pod1-ospd ~]$ nova list |grep auto-it
| 1c45270a-2dcd-4ac1-aba3-bf041733d1a1 | auto-it-vnf-ISO-2007-uas-
0                                    | ACTIVE | -          | running     | mgmt=172.16.181.13,
10.84.123.40

[stack@pod1-ospd ~]$ nova reboot –hard 1c45270a-2dcd-4ac1-aba3-bf041733d1a1
```

2. Si AutoIT-VNF no se puede recuperar, siga estos procedimientos para restaurarlo al estado que estaba antes en. Utilice el archivo de copia de seguridad.

```
 [stack@pod1-ospd ~]$ nova list |grep auto-it
| 580faf80-1d8c-463b-9354-781ea0c0b352 | auto-it-vnf-ISO-2007-uas-
0                                    | ACTIVE | -          | running     | mgmt=172.16.181.3,
10.84.123.42 [stack@pod1-ospd ~]$ cd /opt/cisco/usp/uas-installer/scripts

[stack@pod1-ospd ~]$ ./ auto-it-vnf-staging.sh --floating-ip 10.1.1.3 --delete
```

3. Vuelva a crear Auto-IT ejecutando la secuencia de comandos **auto-it-vnf staging** y asegúrese de utilizar la misma ip flotante que se utilizó anteriormente.

```
[stack@pod1-ospd ~]$ cd /opt/cisco/usp/uas-installer/scripts

[stack@pod1-ospd scripts]$ ./auto-it-vnf-staging.sh --floating-ip 10.1.1.3

2017-11-16 12:54:31,381 - INFO: Creating StagingServer deployment (1 instance(s)) on
'http://10.1.1.3:5000/v2.0' tenant 'core' user 'core', ISO 'default'
2017-11-16 12:54:31,382 - INFO: Loading image 'auto-it-vnf-ISO-5-1-7-2007-usp-uas-1.0.1-
1504.qcow2' from '/opt/cisco/usp/uas-installer/images/usp-uas-1.0.1-1504.qcow2'
2017-11-16 12:54:51,961 - INFO: Loaded image 'auto-it-vnf-ISO-5-1-7-2007-usp-uas-1.0.1-
1504.qcow2'
2017-11-16 12:54:53,217 - INFO: Assigned floating IP '10.1.1.3' to IP '172.16.181.9'
2017-11-16 12:54:53,217 - INFO: Creating instance 'auto-it-vnf-ISO-5-1-7-2007-uas-0'
2017-11-16 12:55:20,929 - INFO: Created instance 'auto-it-vnf-ISO-5-1-7-2007-uas-0'
2017-11-16 12:55:20,930 - INFO: Request completed, floating IP: 10.1.1.3
```

4. Las imágenes ISO utilizadas en el POD deben recargarse en AutoIT-VNF.

```
[stack@pod1-ospd ~]$ cd images/5_1_7-2007/isos

[stack@pod1-ospd isos]$ curl -F file=@usp-5_1_7-2007.iso http://10.1.1.3:5001/isos

{
 "iso-id": "5.1.7-2007"
}

Note: 10.1.1.3 is AutoIT-VNF IP in the above command.

#Validate that ISO is correctly loaded.

[stack@pod1-ospd isos]$ curl http://10.1.1.3:5001/isos

{
 "isos": [
   {
     "iso-id": "5.1.7-2007"
```

```
   }
 ]
}
```

5. Copie los archivos VNF **system.cfg** del servidor remoto a la VM AutoIT-VNF. En este ejemplo, se copia de AutoDeploy a AutoIT-VNF VM.

```
[stack@pod1-ospd autodeploy]$ scp system-vnf* ubuntu@10.1.1.3:.
ubuntu@10.1.1.3's password:

system-
vnf1.cfg
       100% 1197     1.2KB/s   00:00
system-
vnf2.cfg
       100% 1197     1.2KB/s   00:00

ubuntu@auto-it-vnf-iso-2007-uas-0:~$ pwd
/home/ubuntu

ubuntu@auto-it-vnf-iso-2007-uas-0:~$ ls
system-vnf1.cfg  system-vnf2.cfg
```

6. Copie los archivos en una ubicación adecuada en AutoIT-VNF como se hace referencia en la configuración de AutoDeploy. Vea aquí:

```
ubuntu@auto-it-vnf-iso-2007-uas-0:~$ sudo -i
root@auto-it-vnf-iso-2007-uas-0:~$ cp –rp system-vnf1.cfg system-vnf2.cfg
/opt/cisco/usp/uploads/
root@auto-it-vnf-iso-2007-uas-0:~$ls /opt/cisco/usp/uploads/
system-vnf1.cfg  system-vnf2.cfg
```

7. Si la máquina virtual se restaura y se ejecuta correctamente, asegúrese de que se restaura toda la configuración específica de syslog a partir de la copia de seguridad conocida anterior que se ha realizado correctamente.

```
root@auto-deploy-vnf-iso-5-1-5-1196-uas-0:/home/ubuntu#ls /etc/rsyslog.d/00-autoit-vnf.conf
00-autoit-vnf.conf

root@auto-deploy-vnf-iso-5-1-5-1196-uas-0:ls /etc/rsyslog.conf
rsyslog.conf
```

Recuperación de AutoVNF

1. La VM AutoVNF se puede recuperar si la VM está en estado de error o apagado. Realice un reinicio duro para activar la VM afectada. Ejecute estos pasos para recuperar AutoVNF.

2. Identifique la VM que se encuentra en estado Error o Apagar. Reinicie la máquina virtual AutoVNF.

En este ejemplo, reinicie **auto-testautovnf1-uas-2**.

```
[root@tb1-baremetal scripts]# nova list | grep "auto-testautovnf1-uas-[0-2]"

| 3834a3e4-96c5-49de-a067-68b3846fba6b | auto-testautovnf1-uas-
0                                     | ACTIVE | -          | running     | auto-
testautovnf1-uas-orchestration=172.57.12.6; auto-testautovnf1-uas-
management=172.57.11.8
```

```
             |
| 0fbfec0c-f4b0-4551-807b-50c5fe9d3ea7 | auto-testautovnf1-uas-
1                                    | ACTIVE | -          | running     | auto-
testautovnf1-uas-orchestration=172.57.12.7; auto-testautovnf1-uas-management=172.57.11.12
                                                                                 |
| 432e1a57-00e9-4e58-8bef-2a20652df5bf | auto-testautovnf1-uas-
2                                    | ACTIVE | -          | running     | auto-
testautovnf1-uas-orchestration=172.57.12.13; auto-testautovnf1-uas-
management=172.57.11.4
            |

[root@tb1-baremetal scripts]# nova reboot --hard 432e1a57-00e9-4e58-8bef-2a20652df5bf
Request to reboot server <Server: auto-testautovnf1-uas-2> has been accepted.

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

3. Una vez que se activa la máquina virtual, valide que se une al clúster nuevamente.

```
root@auto-testautovnf1-uas-1:/opt/cisco/usp/uas/scripts# confd_cli -u admin -C
Welcome to the ConfD CLI
admin connected from 127.0.0.1 using console on auto-testautovnf1-uas-1

auto-testautovnf1-uas-1#show uas

uas version 1.0.1-1
uas state ha-active
uas ha-vip 172.57.11.101

INSTANCE IP   STATE  ROLE
-----------------------------------

172.57.12.6   alive  CONFD-SLAVE
172.57.12.7   alive  CONFD-MASTER
172.57.12.13  alive  NA
```

4. Si la VM AutoVNF no puede recuperarse mediante el procedimiento mencionado, debe recuperarla con la ayuda de estos pasos.

```
[stack@pod1-ospd ~]$ nova list | grep vnf1-UAS-uas-0
| 307a704c-a17c-4cdc-8e7a-3d6e7e4332fa | vnf1-UAS-uas-
0                                    | ACTIVE | -          | running     | vnf1-
UAS-uas-orchestration=172.168.11.10; vnf1-UAS-uas-management=172.168.10.3

[stack@pod1-ospd ~]$ nova delete vnf1-UAS-uas-0
Request to delete server vnf1-UAS-uas-0 has been accepted.
```

5. Para recuperar la VM **autovnf-uas**, ejecute el script **uas-check** para verificar el estado. Debe informar de un error. A continuación, ejecute de nuevo con la opción **—fix** para recrear la VM UAS faltante.

```
[stack@pod1-ospd ~]$ cd /opt/cisco/usp/uas-installer/scripts/
[stack@pod1-ospd scripts]$ ./uas-check.py auto-vnf vnf1-UAS

2017-12-08 12:38:05,446 - INFO: Check of AutoVNF cluster started
2017-12-08 12:38:07,925 - INFO: Instance 'vnf1-UAS-uas-0' status is 'ERROR'
2017-12-08 12:38:07,925 - INFO: Check completed, AutoVNF cluster has recoverable errors

[stack@tb3-ospd scripts]$ ./uas-check.py auto-vnf vnf1-UAS --fix

2017-11-22 14:01:07,215 - INFO: Check of AutoVNF cluster started
2017-11-22 14:01:09,575 - INFO: Instance vnf1-UAS-uas-0' status is 'ERROR'
```

```
2017-11-22 14:01:09,575 - INFO: Check completed, AutoVNF cluster has recoverable errors
2017-11-22 14:01:09,778 - INFO: Removing instance vnf1-UAS-uas-0'
2017-11-22 14:01:13,568 - INFO: Removed instance vnf1-UAS-uas-0'
2017-11-22 14:01:13,568 - INFO: Creating instance vnf1-UAS-uas-0' and attaching volume ‘vnf1-
UAS-uas-vol-0'
2017-11-22 14:01:49,525 - INFO: Created instance ‘vnf1-UAS-uas-0'

[stack@tb3-ospd scripts]$ ./uas-check.py auto-vnf vnf1-UAS

2017-11-16 13:11:07,472 - INFO: Check of AutoVNF cluster started
2017-11-16 13:11:09,510 - INFO: Found 3 ACTIVE AutoVNF instances
2017-11-16 13:11:09,511 - INFO: Check completed, AutoVNF cluster is fine
```

6. Inicie sesión en la máquina virtual AutoVNF maestra. Pocos minutos después de la recuperación, la instancia recién creada debe unirse al clúster y en estado vivo.

```
tb3-bxb-vnf1-autovnf-uas-0#show uas

uas version 1.0.1-1
uas state ha-active
uas ha-vip 172.17.181.101

INSTANCE IP   STATE  ROLE
-----------------------------------
172.17.180.6  alive  CONFD-SLAVE
172.17.180.7  alive  CONFD-MASTER
172.17.180.9  alive  NA

#if uas-check.py --fix fails, you may need to copy this file and execute again.

[stack@tb3-ospd]$ mkdir -p /opt/cisco/usp/apps/auto-it/common/uas-deploy/
[stack@tb3-ospd]$ cp /opt/cisco/usp/uas-installer/common/uas-deploy/userdata-uas.txt
/opt/cisco/usp/apps/auto-it/common/uas-deploy/
```

7. Si la máquina virtual se restaura y se ejecuta correctamente, asegúrese de que se restaura toda la configuración específica de syslog a partir de la copia de seguridad conocida anterior que se ha realizado correctamente. Asegúrese de que se restaura en todas las VM AutoVNF.

```
ubuntu@auto-testautovnf1-uas-1:~$sudo su
root@auto-testautovnf1-uas-1:/home/ubuntu#ls /etc/rsyslog.d/00-autovnf.conf
00-autovnf.conf

root@auto-testautovnf1-uas-1:/home/ubuntu#ls /etc/rsyslog.conf
rsyslog.conf
```

Recuperación ESC

1. La VM ESC se puede recuperar si la VM se encuentra en estado Error o apagado. Realice un reinicio duro para activar la VM afectada. Ejecute estos pasos para recuperar ESC.

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

```
[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 esta 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. Desde AutoVNF-UAS, busque la transacción de implementación ESC y en el registro de la transacción busque la línea de comandos **boot_vm.py** para crear la instancia ESC.

```
ubuntu@vnf1-uas-uas-0:~$ sudo -i
root@vnf1-uas-uas-0:~# confd_cli -u admin -C
Welcome to the ConfD CLI

admin connected from 127.0.0.1 using console on vnf1-uas-uas-0
vnf1-uas-uas-0#show transaction

TX ID                                  TX TYPE          DEPLOYMENT ID
TIMESTAMP                          STATUS
-------------------------------------------------------------------------------------------------
------------------------------
35eefc4a-d4a9-11e7-bb72-fa163ef8df2b  vnf-deployment   vnf1-DEPLOYMENT  2017-11-
29T02:01:27.750692-00:00  deployment-success
73d9c540-d4a8-11e7-bb72-fa163ef8df2b  vnfm-deployment  vnf1-ESC         2017-11-
29T01:56:02.133663-00:00  deployment-success

vnf1-uas-uas-0#show logs 73d9c540-d4a8-11e7-bb72-fa163ef8df2b | display xml

<config xmlns="http://tail-f.com/ns/config/1.0">
 <logs xmlns="http://www.cisco.com/usp/nfv/usp-autovnf-oper">
   <tx-id>73d9c540-d4a8-11e7-bb72-fa163ef8df2b</tx-id>
   <log>2017-11-29 01:56:02,142 - VNFM Deployment RPC triggered for deployment: vnf1-ESC,
deactivate: 0

2017-11-29 01:56:02,179 - Notify deployment
..
2017-11-29 01:57:30,385 - Creating VNFM 'vnf1-ESC-ESC-1' with [python //opt/cisco/vnf-
staging/bootvm.py vnf1-ESC-ESC-1 --flavor vnf1-ESC-ESC-flavor --image 3fe6b197-961b-4651-af22-
dfd910436689 --net vnf1-UAS-uas-management --gateway_ip 172.168.10.1 --net vnf1-UAS-uas-
orchestration --os_auth_url http://10.1.1.5:5000/v2.0 --os_tenant_name core --os_username ******
--os_password ****** --bs_os_auth_url http://10.1.1.5:5000/v2.0 --bs_os_tenant_name core --
bs_os_username ****** --bs_os_password ****** --esc_ui_startup false --esc_params_file
```

```
/tmp/esc_params.cfg --encrypt_key ****** --user_pass ****** --user_confd_pass ****** --kad_vif
eth0 --kad_vip 172.168.10.7 --ipaddr 172.168.10.6 dhcp --ha_node_list 172.168.10.3 172.168.10.6
--file root:0755:/opt/cisco/esc/esc-
scripts/esc_volume_em_staging.sh:/opt/cisco/usp/uas/autovnf/vnfms/esc-
scripts/esc_volume_em_staging.sh --file root:0755:/opt/cisco/esc/esc-
scripts/esc_vpc_chassis_id.py:/opt/cisco/usp/uas/autovnf/vnfms/esc-scripts/esc_vpc_chassis_id.py
--file root:0755:/opt/cisco/esc/esc-scripts/esc-vpc-di-internal-
keys.sh:/opt/cisco/usp/uas/autovnf/vnfms/esc-scripts/esc-vpc-di-internal-keys.sh]...
```

5. Guarde la línea **boot_vm.py** en un archivo de secuencia de comandos de shell (esc.sh) y actualice todas las líneas de nombre de usuario ***** y contraseña ***** con la información correcta (normalmente, core/Cisco@123). También debe quitar la opción -encrypt_key. Para user_pass y user_confd_pass, debe utilizar el formato -user_passwd username:password (ejemplo - admin:Cisco@123).

Ahora, busque la URL a **bootvm.py** de running-config y obtenga el **archivo bootvm.py** a la máquina virtual autovnf-uas. 10.1.1.3 es la TI automática en este caso.

```
root@vnf1-uas-uas-0:~# confd_cli -u admin -C
Welcome to the ConfD CLI
admin connected from 127.0.0.1 using console on vnf1-uas-uas-0

vnf1-uas-uas-0#show running-config autovnf-vnfm:vnfm
…
configs bootvm
 value http://10.1.1.3:80/bundles/5.1.7-2007/vnfm-bundle/bootvm-2_3_2_155.py
!

root@vnf1-uas-uas-0:~# wget http://10.1.1.3:80/bundles/5.1.7-2007/vnfm-bundle/bootvm-
2_3_2_155.py

--2017-12-01 20:25:52--  http://10.1.1.3/bundles/5.1.7-2007/vnfm-bundle/bootvm-2_3_2_155.py
Connecting to 10.1.1.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 127771 (125K) [text/x-python]
Saving to: ‘bootvm-2_3_2_155.py’

100%[=========================================================================================
==========>] 127,771     --.-K/s   in 0.001s


2017-12-01 20:25:52 (173 MB/s) - ‘bootvm-2_3_2_155.py’ saved [127771/127771
Create a /tmp/esc_params.cfg file.

root@vnf1-uas-uas-0:~# echo "openstack.endpoint=publicURL" > /tmp/esc_params.cfg
```

6. Ejecute el script shell que ejecuta el script **bootvm.py** python con opciones.

```
root@vnf1-uas-uas-0:~# /bin/sh esc.sh
+ python ./bootvm.py vnf1-ESC-ESC-1 --flavor vnf1-ESC-ESC-flavor --image 3fe6b197-961b-4651-
af22-dfd910436689 --net vnf1-UAS-uas-management --gateway_ip 172.168.10.1 --net vnf1-UAS-uas-
orchestration --os_auth_url http://10.1.1.5:5000/v2.0 --os_tenant_name core --os_username core -
-os_password Cisco@123 --bs_os_auth_url http://10.1.1.5:5000/v2.0 --bs_os_tenant_name core --
bs_os_username core --bs_os_password Cisco@123 --esc_ui_startup false --esc_params_file
/tmp/esc_params.cfg --user_pass admin:Cisco@123 --user_confd_pass admin:Cisco@123 --kad_vif eth0
--kad_vip 172.168.10.7 --ipaddr 172.168.10.6 dhcp --ha_node_list 172.168.10.3 172.168.10.6 --
file root:0755:/opt/cisco/esc/esc-
scripts/esc_volume_em_staging.sh:/opt/cisco/usp/uas/autovnf/vnfms/esc-
scripts/esc_volume_em_staging.sh --file root:0755:/opt/cisco/esc/esc-
scripts/esc_vpc_chassis_id.py:/opt/cisco/usp/uas/autovnf/vnfms/esc-scripts/esc_vpc_chassis_id.py
--file root:0755:/opt/cisco/esc/esc-scripts/esc-vpc-di-internal-
```

```
keys.sh:/opt/cisco/usp/uas/autovnf/vnfms/esc-scripts/esc-vpc-di-internal-keys.sh


+-----------------------------------+-------------------------------------------------------
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
-----------------------------------------------+
| Property                          |
Value



+-----------------------------------+-------------------------------------------------------
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
-----------------------------------------------+
| OS-DCF:diskConfig                 |
MANUAL


| OS-EXT-AZ:availability_zone       |
mgmt


| OS-EXT-SRV-ATTR:host              | tb5-ultram-osd-compute-
1.localdomain


| OS-EXT-SRV-ATTR:hypervisor_hostname  | tb5-ultram-osd-compute-
1.localdomain


| OS-EXT-SRV-ATTR:instance_name     | instance-
000001eb

| OS-EXT-STS:power_state            |
1


| OS-EXT-STS:task_state             | -


| OS-EXT-STS:vm_state               |
active


| OS-SRV-USG:launched_at            | 2017-12-
02T13:28:32.000000


| OS-SRV-USG:terminated_at          | -
```

```
| accessIPv4                          |

| accessIPv6
|

| addresses                           | {"vnf1-UAS-uas-orchestration": [{"OS-EXT-IPS-
MAC:mac_addr": "fa:16:3e:d7:c6:19", "version": 4, "addr": "172.168.11.14", "OS-EXT-IPS:type":
"fixed"}], "vnf1-UAS-uas-management": [{"OS-EXT-IPS-MAC:mac_addr": "fa:16:3e:31:ee:cd",
"version": 4, "addr": "172.168.10.6", "OS-EXT-IPS:type": "fixed"}]}
| config_drive                        | True

| created                             | 2017-12-
02T13:27:49Z

| flavor                              | {"id": "457623b6-05d5-403c-b2e4-aa3b6a0c9d32", "links":
[{"href": "http://10.1.1.5:8774/flavors/457623b6-05d5-403c-b2e4-aa3b6a0c9d32", "rel":
"bookmark"}]}
| hostId                              |
f5d2bbf0c5a7df34cf2e6f62ae0702ef120ff82f81c3f7664ffb35e9

| id                                  | 2601b8ec-8ff8-4285-810a-
e859f6642ab6

| image                               | {"id": "3fe6b197-961b-4651-af22-dfd910436689", "links":
[{"href": "http://10.1.1.5:8774/images/3fe6b197-961b-4651-af22-dfd910436689", "rel":
"bookmark"}]}
| key_name                            | -

| metadata                            |
{}

| name                                | vnf1-esc-esc-
1

| os-extended-volumes:volumes_attached | []

| progress                            |
0

| security_groups                     | [{"name": "default"}, {"name":
"default"}]
```

```
                                                    |
| status                                |
ACTIVE


                                      |
| tenant_id                             |
fd4b15df46c6469cbacf5b80dcc98a5c


                                                        |
| updated                               | 2017-12-
02T13:28:32Z


                                        |
| user_id                               |
d3b51d6f705f4826b22817f27505c6cd


                           |
```

7. En OSPD, verifique que la nueva VM ESC esté ACTIVA/en ejecución.

```
[stack@pod1-ospd ~]$ nova list|grep -i esc
| 934519a4-d634-40c0-a51e-fc8d55ec7144 | vnf1-ESC-ESC-
0                                                   | ACTIVE | -          | running     | vnf1-
UAS-uas-orchestration=172.168.11.13; vnf1-UAS-uas-
management=172.168.10.3
                        |
| 2601b8ec-8ff8-4285-810a-e859f6642ab6 | vnf1-ESC-ESC-
1                                                   | ACTIVE | -          | running     | vnf1-
UAS-uas-orchestration=172.168.11.14; vnf1-UAS-uas-
management=172.168.10.6
                        |

#Log in to new ESC and verify Backup state.  You may execute health.sh on ESC Master too.

ubuntu@vnf1-uas-uas-0:~$ ssh admin@172.168.11.14
…
  ################################################################################
  #   ESC on vnf1-esc-esc-1.novalocal is in BACKUP state.
  ################################################################################

[admin@vnf1-esc-esc-1 ~]$ escadm status
0 ESC status=0 ESC Backup Healthy

[admin@vnf1-esc-esc-1 ~]$ health.sh
============== ESC HA (BACKUP) =================
========================================

ESC HEALTH PASSED
[admin@vnf1-esc-esc-1 ~]$ cat /proc/drbd
version: 8.4.7-1 (api:1/proto:86-101)
GIT-hash: 3a6a769340ef93b1ba2792c6461250790795db49 build by mockbuild@Build64R6, 2016-01-12
13:27:11

 1: cs:Connected ro:Secondary/Primary ds:UpToDate/UpToDate C r-----
    ns:0 nr:504720 dw:3650316 dr:0 al:8 bm:0 lo:0 pe:0 ua:0 ap:0 ep:1 wo:f oos:0
```

8. 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.

9. Para restaurar la base de datos ESC, asegúrese de 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
```

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

```
# escadm status
```

11. 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>
```

12. Reinicie el servicio ESC para completar la restauración de la base de datos.

13. Para HA, ejecute en ambas VM, reinicie el servicio keepalived.

```
# service keepalived start
```

14. 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
```

Recuperación de EM

1. Si la VM EM está en estado Ninguno/Error debido a una u otra condición, el usuario puede seguir la secuencia dada para recuperar la VM EM afectada.

2. ESC/VNFM es el componente que monitorea las VM EM, por lo que en el caso de que EM se encuentre en estado de error, ESC intentará recuperar automáticamente la VM EM. Por cualquier razón,n si ESC no puede completar la recuperación correctamente, ESC marcará esa VM en estado de error.

3. En estos escenarios, el usuario puede realizar la recuperación manual de la VM de EM una vez que se solucione el problema de infraestructura subyacente. Es importante ejecutar esta recuperación manual sólo después de solucionar un problema subyacente.

4. Identifique la VM en el estado errado.

```
[stack@pod1-ospd ~]$ source corerc
[stack@pod1-ospd ~]$ nova list --field name,host,status |grep -i err
| c794207b-a51e-455e-9a53-3b8ff3520bb9 | vnf1-DEPLOYMENT-_vnf1-D_0_a6843886-77b4-4f38-b941-
74eb527113a8 | None                                    | ERROR   |
```

5. Inicie sesión en ESC Master, ejecute **recovery-vm-action** para cada EM y VM CF afectadas. Sé paciente. ESC programará la acción de recuperación y puede que no suceda durante unos minutos.

```
ubuntu@vnf1-uas-uas-1:~$ ssh admin@172.168.10.3
…

[admin@vnf1-esc-esc-0 ~]$ sudo /opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli recovery-vm-action DO
vnf1-DEPLOYMENT-_vnf1-D_0_a6843886-77b4-4f38-b941-74eb527113a8
[sudo] password for admin:

Recovery VM Action
/opt/cisco/esc/confd/bin/netconf-console --port=830 --host=127.0.0.1 --user=admin --
privKeyFile=/root/.ssh/confd_id_dsa --privKeyType=dsa --rpc=/tmp/esc_nc_cli.ZpRCGiieuW
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">
 <ok/>
</rpc-reply>
```

6. Monitoree el **/var/log/esc/yangesc.log** hasta que se complete el comando.

```
[admin@vnf1-esc-esc-0 ~]$ tail -f /var/log/esc/yangesc.log

…

14:59:50,112 07-Nov-2017 WARN  Type: VM_RECOVERY_COMPLETE
14:59:50,112 07-Nov-2017 WARN  Status: SUCCESS
14:59:50,112 07-Nov-2017 WARN  Status Code: 200
14:59:50,112 07-Nov-2017 WARN  Status Msg: Recovery: Successfully recovered VM [vnf1-DEPLOYMENT-
_vnf1-D_0_a6843886-77b4-4f38-b941-74eb527113a8]

#Log in to new EM and verify EM state is up.

ubuntu@vnf1vnfddeploymentem-1:~$ /opt/cisco/ncs/current/bin/ncs_cli -u admin -C

admin connected from 172.17.180.6 using ssh on vnf1vnfddeploymentem-1

admin@scm# show ems

EM            VNFM

ID  SLA  SCM  PROXY
----------------------
2   up   up   up
3   up   up   up
```

Cuando ESC no puede iniciar VM

1. 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. El switchover ESC tarda aproximadamente un minuto. Ejecute **health.sh** en el nuevo Master ESC para verificar si está activo. Cuando ESC se convierte en Master, ESC podría 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.

2. Puede supervisar **/var/log/esc/yangesc.log** y **/var/log/esc/escmanager.log**. Si observa que la VM no se recupera después de 5-7 minutos, el usuario debe ir y realizar la recuperación manual de las VM afectadas.

3. 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 StarOS

1. En caso de que una de las VM StarOS aparezca en estado Ninguno/Error debido a una u otras condiciones, el usuario puede seguir esta secuencia para recuperar la VM StarOS afectada.

2. ESC/VNFM es el componente que monitorea las VM de StarOS, por lo que en el caso de que la VM CF/SF esté en estado de error, ESC intentará recuperar automáticamente la VM CF/SF. Por cualquier motivo, si ESC no puede completar la recuperación correctamente, ESC marcará esa VM en estado Error.

3. En estos escenarios, el usuario puede realizar la recuperación manual de la VM CF/SF una vez que se solucione el problema de infraestructura subyacente. Es importante ejecutar esta recuperación manual sólo después de solucionar un problema subyacente.

4. Identifique la VM en el estado Error.

```
[stack@pod1-ospd ~]$ source corerc

[stack@pod1-ospd ~]$ nova list --field name,host,status |grep -i err
| c794207b-a51e-455e-9a53-3b8ff3520bb9 | vnf1-DEPLOYMENT-_s4_0_c2b19084-26b3-4c9c-8639-
62428a4cb3a3 | None                                 | ERROR   |
```

5. Inicie sesión en ESC Master, ejecute **recovery-vm-action** para cada paciente de EM y CF VM.Be afectado. ESC programará la acción de recuperación y puede que no suceda durante

unos minutos.

```
ubuntu@vnf1-uas-uas-1:~$ ssh admin@172.168.10.3
…

[admin@vnf1-esc-esc-0 ~]$ sudo /opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli recovery-vm-action DO
vnf1-DEPLOYMENT-_s4_0_c2b19084-26b3-4c9c-8639-62428a4cb3a3
[sudo] password for admin:

Recovery VM Action

/opt/cisco/esc/confd/bin/netconf-console --port=830 --host=127.0.0.1 --user=admin --
privKeyFile=/root/.ssh/confd_id_dsa --privKeyType=dsa --rpc=/tmp/esc_nc_cli.ZpRCGiieuW
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">
 <ok/>
</rpc-reply>

##Monitor the /var/log/esc/yangesc.log until command completes.

[admin@vnf1-esc-esc-0 ~]$ tail -f /var/log/esc/yangesc.log
…
14:59:50,112 07-Nov-2017 WARN  Type: VM_RECOVERY_COMPLETE
14:59:50,112 07-Nov-2017 WARN  Status: SUCCESS
14:59:50,112 07-Nov-2017 WARN  Status Code: 200
14:59:50,112 07-Nov-2017 WARN  Status Msg: Recovery: Successfully recovered VM [vnf1-DEPLOYMENT-
_s4_0_c2b19084-26b3-4c9c-8639-62428a4cb3a3]
```

6. Además, valide lo mismo ejecutando la **pestaña show card** en StarOS. Si la VM recuperada es SF, el usuario podría tener que activarla si lo desea. Realice los cambios necesarios en la configuración de StarOS.

```
[local]VNF1# show card tab
Saturday December 02 14:40:20 UTC 2017
Slot         Card Type                                Oper State     SPOF  Attach

-----------  ---------------------------------------  -------------  ----  ------

 1: CFC      Control Function Virtual Card            Active         No
2: CFC      Control Function Virtual Card            Standby        -
 3: FC       4-Port Service Function Virtual Card     Active         No
 4: FC       4-Port Service Function Virtual Card     Active         No
 5: FC       4-Port Service Function Virtual Card     Active         No
 6: FC       4-Port Service Function Virtual Card     Standby        -
 7: FC       4-Port Service Function Virtual Card     Active         No
 8: FC       4-Port Service Function Virtual Card     Active         No
 9: FC       4-Port Service Function Virtual Card     Active         No
10: FC       4-Port Service Function Virtual Card     Active         No
```

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. El switchover ESC tarda aproximadamente un minuto. Ejecute **health.sh** en el nuevo Master ESC para verificar que está activo. Cuando ESC se convierte en Master, ESC podría 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 la VM se recupera después de 5-7 minutos, deberá ir y realizar la recuperación manual de las VM afectadas.