Componentes modulares RMA-PCRF

Contenido

Introducción

Este documento describe los pasos necesarios para sustituir los componentes defectuosos mencionados aquí en un servidor Cisco Unified Computing System (UCS) en una configuración Ultra-M que aloja Cisco Policy Suite (CPS) Virtual Network Functions (VNF).

- MOP de sustitución del módulo de memoria en línea dual (DIMM)
- Falla del controlador FlexFlash
- Falla de unidad de estado sólido (SSD)
- Falla del módulo de plataforma de confianza (TPM)
- Error de caché Raid
- Falla del controlador Raid/adaptador de bus caliente (HBA)
- Falla de la tarjeta vertical PCI
- Falla del adaptador PCIe Intel X520 10G
- Falla en la placa base LAN-on modular (MLOM)

- RMA de bandeja de ventilador
- Falla de CPU

Colaborado por Nitesh Bansal, Cisco Advance Services.

Antecedentes

Ultra-M es una solución virtualizada validada y empaquetada previamente diseñada para simplificar la implementación de VNF. OpenStack es el Virtualized Infrastructure Manager (VIM) para Ultra-M y consta de estos tipos de nodos:

- Informática
- Disco de almacenamiento de objetos - Compute (OSD - Compute)
- Controlador
- Plataforma OpenStack: Director (OSPD)
- La versión Ultra M 5.1.x se considera para definir los procedimientos en este documento.
- Este documento está dirigido al personal de Cisco familiarizado con la plataforma Cisco Ultra-M y detalla los pasos necesarios para llevarse a cabo en el nivel de VNF de OpenStack y CPS en el momento del reemplazo de componentes en el servidor.

Antes de reemplazar un componente defectuoso, es importante verificar el estado actual del entorno de plataforma Red Hat Open Stack. Se recomienda que verifique el estado actual para evitar complicaciones cuando el proceso de reemplazo está activado.

En caso de recuperación, Cisco recomienda realizar la copia de seguridad de la base de datos OSPD con la ayuda de estos pasos:

```
[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
```

Este proceso asegura que un nodo se pueda reemplazar sin afectar la disponibilidad de las instancias.

> **Nota:** Si un servidor es un nodo de controlador, vaya a la sección , de lo contrario continúe con la siguiente sección.

Abreviaturas

VNF	Función de red virtual
PD	Director de políticas (equilibrador de carga)
PS	Servidor de políticas (pcrfclient)
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
SM	Administrador de sesiones
QNS	Quantum Name Server
UUID	Identificador único universal

Solución de problemas de RMA de componentes - Nodo Compute/OSD-Compute

Paso 1. Apagado Graceful

Identificación de las VM alojadas en el nodo de informática/informática OSD

La Compute/OSD-Compute puede alojar varios tipos de VM. Identifique todos y continúe con los pasos individuales junto con el nodo individual concreto y con los nombres de VM específicos alojados en este equipo:

```
[stack@director ~]$ nova list --field name,host | grep compute-10
| 49ac5f22-469e-4b84-badc-031083db0533 |  SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634
|
pod1-compute-10.localdomain    |
| 49ac5f22-469e-4b84-badc-031083db0533 |  SVS1-tmo_sm-s3_0_05966301-bd95-4071-817a-
0af43757fc88     |
pod1-compute-10.localdomain    |
```

Para el cierre de cortesía de VM del Cluster Manager

Paso 1. Cree una instantánea y envíe el archivo por FTP a otra ubicación fuera del servidor o, si es posible, fuera del propio rack.

```
openstack image create --poll
```

Paso 2. Detenga la VM de ESC.

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

Paso 3. Verifique si la VM está detenida.

```
[admin@esc ~]$ cd /opt/cisco/esc/esc-confd/esc-cli
[admin@esc ~]$ ./esc_nc_cli get esc_datamodel | egrep --color
"<state>|<vm_name>|<vm_id>|<deployment_name>"
<snip>
<state>SERVICE_ACTIVE_STATE</state>
                    SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634
                    VM_SHUTOFF_STATE
```

Para el cierre de cortesía de VM activo PD/equilibrador de carga

Paso 1. Inicie sesión en Active LB y detenga los servicios como se indica a continuación

- Cambie el lb de activo a inactivo

```
service corosync restart
```

- stop services on standby lb

```
service monit stop
service qns stop
```

Paso 2. Desde ESC Master.

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

Paso 3. Verifique si la VM está detenida.

```
admin@esc ~]$ cd /opt/cisco/esc/esc-confd/esc-cli
[admin@esc ~]$ ./esc_nc_cli get esc_datamodel | egrep --color "
```

Para el apagado Graceful de VM PD/equilibrador de carga en espera

Paso 1. Inicie sesión en standby lb y detenga los servicios.

```
service monit stop
service qns stop
```

Paso 2. Desde ESC Master.

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

Paso 3. Verifique si la VM está detenida.

```
[admin@esc ~]$ cd /opt/cisco/esc/esc-confd/esc-cli
[admin@esc ~]$ ./esc_nc_cli get esc_datamodel | egrep --color "
```

Para el cierre de cortesía de VM PS/QNS

Paso 1. Detenga el servicio:

```
service monit stop
service qns stop
```

Paso 2. Desde ESC Master.

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

Paso 3. Verifique si la VM está detenida.

```
[dmin@esc ~]$ cd /opt/cisco/esc/esc-confd/esc-cli
[dmin@esc ~]$ ./esc_nc_cli get esc_datamodel | egrep --color "
```

Para el cierre de cortesía de VM SM

Paso 1. Detenga todos los servicios de mongo presentes en la sesión mgr.

```
 [root@sessionmg01 ~]# cd /etc/init.d
[root@sessionmg01 init.d]# ls -l sessionmgr*

[root@sessionmg01 ~]# /etc/init.d/sessionmgr-27717 stop Stopping mongod: [  OK  ]
[root@ sessionmg01 ~]# /etc/init.d/sessionmgr-27718 stop Stopping mongod: [  OK  ]
[root@ sessionmg01 ~]# /etc/init.d/sessionmgr-27719 stop Stopping mongod: [  OK  ]
```

Paso 2. Desde ESC Master.

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

Paso 3. Verifique si la VM está detenida.

```
[admin@esc ~]$ cd /opt/cisco/esc/esc-confd/esc-cli
[admin@esc ~]$ ./esc_nc_cli get esc_datamodel | egrep --color "
```

Para OAM/pcrfclient VM Graceful Shutdown

Paso 1. Verifique si la política SVN está sincronizada a través de estos comandos. Si se devuelve un valor, SVN ya está sincronizada y no necesita sincronizarla desde PCRFCLIENT02. Debe omitir la recuperación de la última copia de seguridad que se puede seguir utilizando si es

necesario.

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

Paso 2. Vuelva a establecer la sincronización maestro/esclavo de SVN entre pcrfclient01 y pcrfclient02 con pcrfclient01 como maestro ejecutando la serie de comandos en 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 3. Realice una copia de seguridad del SVN en el cluster manager.

```
config_br.py -a export --svn /mnt/backup/svn_backup_pcrfclient.tgz
```

Paso 4. Cierre los servicios en pcrfclient.

```
service monit stop
service qns stop
```

Paso 5. Desde ESC Master:

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

Paso 6. Verifique si la VM está detenida.

```
[admin@esc ~]$ cd /opt/cisco/esc/esc-confd/esc-cli
[admin@esc ~]$ ./esc_nc_cli get esc_datamodel | egrep --color "
```

Para la máquina virtual del árbitro

Paso 1. Inicie sesión en el árbitro y cierre los servicios.

```
[root@SVS1OAM02 init.d]# ls -lrt sessionmgr*
-rwxr-xr-x 1 root root 4382 Jun 21 07:34 sessionmgr-27721
-rwxr-xr-x 1 root root 4406 Jun 21 07:34 sessionmgr-27718
-rwxr-xr-x 1 root root 4407 Jun 21 07:34 sessionmgr-27719
-rwxr-xr-x 1 root root 4429 Jun 21 07:34 sessionmgr-27717
-rwxr-xr-x 1 root root 4248 Jun 21 07:34 sessionmgr-27720

service monit stop
service qns stop
/etc/init.d/sessionmgr-[portno.] stop , where port no is the db port in the arbiter.
```

Paso 2.Desde ESC Master.

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

Paso 3. Verifique si la VM está detenida.

```
[admin@esc ~]$ cd /opt/cisco/esc/esc-confd/esc-cli
[admin@esc ~]$ ./esc_nc_cli get esc_datamodel | egrep --color "
```

Para el controlador de servicios elásticos (ESC)

Paso 1. Las configuraciones en ESC-HA se deben realizar una copia de seguridad mensual, antes/después de cualquier operación de ampliación o reducción con el VNF y antes/después de los cambios de configuración en ESC. Se debe realizar una copia de seguridad de esta información para poder realizar una recuperación ante desastres de ESC de manera eficaz

1. Inicie sesión en ESC mediante Credenciales de administración y Exportar datos opdata a XML.

```
/opt/cisco/esc/confd/bin/netconf-console --host 127.0.0.1 --port 830 -u
```

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

Paso 2. Realice una copia de seguridad de la configuración de nube de PCRF Todos los scripts y archivos de datos de usuario a los que se hace referencia en XML de implementación.

1. Busque todos los archivos de datos de usuario a los que se hace referencia en XML de implementación de todas las VNF de los datos opdata exportados en el paso anterior.Ejemplo de resultado.

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

3. Fragmentos de ejemplo de script posterior a la implementación en esc opdata.

Ejemplo 1:

Ejemplo 2:

Si la implementación ESC opdata (extraída en el paso anterior) contiene alguno de los archivos resaltados, realice la copia de seguridad.

Ejemplo de comando Backup:

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

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

```
Note:- Although opdata is synced between ESC master and slave, directories containing user-data, xml and post deploy scripts are not synced across both instances. It is suggested that customers can push the contents of directory containing these files using scp or sftp, these files should be constant across ESC-Master and ESC-Standby in order to recover a deployment when ESC VM which was master during deployment is not available do to any unforeseen circumstances.
```

Paso 2. Copia de seguridad de la base de datos ESC.

Paso 1. Recopile los registros de las VM ESC y realice una copia de seguridad.

```
$ collect_esc_log.sh
$ scp /tmp/
```

Paso 2. Realice una copia de seguridad de la base de datos desde el nodo ECS maestro.

Paso 3. Cambie al usuario raíz y verifique el estado del ESC primario y valide que el valor de salida sea Master.

```
 $ sudo bash
 $ escadm status

Set ESC to maintenance mode & verify

$ sudo escadm op_mode set --mode=maintenance
$ escadm op_mode show
```

Paso 4. Utilice una variable para establecer el nombre del archivo e incluir información de fecha y Llamar a la herramienta de copia de seguridad y proporcionar la variable de nombre de archivo del paso anterior.

```
fname=esc_db_backup_$(date -u +"%y-%m-%d-%H-%M-%S")

$ sudo /opt/cisco/esc/esc-scripts/esc_dbtool.py backup -- file /tmp/atlpod-esc-master-$fname.tar
```

Paso 5. Compruebe el archivo de copia de seguridad en el almacenamiento de copia de seguridad y asegúrese de que el archivo está allí.

Paso 6. Vuelva a poner Master ESC en el modo de funcionamiento normal.

```
$ sudo escadm op_mode set --mode=operation
```

Si falla la utilidad de copia de seguridad dbtool, aplique la siguiente solución una vez en el nodo ESC. A continuación, repita el paso 6.

```
$ sudo sed -i "s,'pg_dump,'/usr/pgsql-9.4/bin/pg_dump,"
/opt/cisco/esc/esc-scripts/esc_dbtool.py
```

Paso 3. Migrar ESC al modo en espera.

Paso 1. Inicie sesión en el ESC alojado en el nodo y verifique si está en el estado principal. Si la respuesta es sí, cambie el modo ESC al modo en espera.

```
[admin@VNF2-esc-esc-0 esc-cli]$ escadm status
0 ESC status=0 ESC Master Healthy

[admin@VNF2-esc-esc-0 ~]$ sudo service keepalived stop Stopping
keepalived:
[  OK  ]
[admin@VNF2-esc-esc-0 ~]$ escadm status
1 ESC status=0 In SWITCHING_TO_STOP state. Please check status after a while.

[admin@VNF2-esc-esc-0 ~]$ sudo reboot
Broadcast message from admin@vnf1-esc-esc-0.novalocal
       (/dev/pts/0) at 13:32 ...
The system is going down for reboot NOW!
```

Paso 2. Una vez que la VM esté en espera ESC, apague la VM mediante el comando: **shutdown -r now**

> **Nota:** Si se va a sustituir el componente defectuoso en el nodo OSD-Compute, coloque el CEPH en Mantenimiento en el servidor antes de continuar con el reemplazo del componente.

```
[admin@osd-compute-0 ~]$ sudo ceph osd set norebalance
set norebalance
[admin@osd-compute-0 ~]$ sudo ceph osd set noout
```

```
set noout
[admin@osd-compute-0 ~]$ sudo ceph status
    cluster eb2bb192-b1c9-11e6-9205-525400330666
     health HEALTH_WARN
            noout,norebalance,sortbitwise,require_jewel_osds flag(s) set
     monmap e1: 3 mons at {tb3-ultram-pod1-controller-0=11.118.0.40:6789/0,tb3-ultram-pod1-
controller-1=11.118.0.41:6789/0,tb3-ultram-pod1-controller-2=11.118.0.42:6789/0}
            election epoch 58, quorum 0,1,2 tb3-ultram-pod1-controller-0,tb3-ultram-pod1-
controller-1,tb3-ultram-pod1-controller-2
     osdmap e194: 12 osds: 12 up, 12 in
            flags noout,norebalance,sortbitwise,require_jewel_osds
      pgmap v584865: 704 pgs, 6 pools, 531 GB data, 344 kobjects
            1585 GB used, 11808 GB / 13393 GB avail
                 704 active+clean
  client io 463 kB/s rd, 14903 kB/s wr, 263 op/s rd, 542 op/s wr
```

Paso 4. Reemplace el componente defectuoso del nodo de cómputo/OSD-Compute.

Apague el servidor especificado. Los pasos para reemplazar un componente defectuoso en el servidor UCS C240 M4 se pueden derivar de:

Sustitución de los componentes del servidor

Consulte Registro persistente en el siguiente procedimiento y ejecute según sea necesario

Paso 5. Restaure las VM.

Recuperación de VM desde ESC

1. La VM se encontraría en estado de error en la lista nova.

```
[stack@director  ~]$ nova list |grep VNF2-DEPLOYM_s9_0_8bc6cc60-15d6-4ead-8b6a-10e75d0e134d
| 49ac5f22-469e-4b84-badc-031083db0533 | VNF2-DEPLOYM_s9_0_8bc6cc60-15d6-4ead-8b6a-
10e75d0e134d     | ERROR  | -          | NOSTATE     |
```

2. Recupere las VM de ESC.

```
[admin@VNF2-esc-esc-0 ~]$ sudo /opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli recovery-vm-
action DO VNF2-DEPLOYM_s9_0_8bc6cc60-15d6-4ead-8b6a-10e75d0e134d
[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
```

3. Supervisar el yangesc.log

```
admin@VNF2-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 [VNF2-
DEPLOYM_s9_0_8bc6cc60-15d6-4ead-8b6a-10e75d0e134d].
```

4. Verifique todos los servicios en las VM que se están iniciando.

Recuperación de VM ESC

1. Inicie sesión en ESC a través de la consola y verifique el estado.

2. Iniciar los procesos si aún no se han iniciado

```
 [admin@esc ~]$ sudo service keepalived start

[admin@esc ~]$ escadm status 0 ESC status=0 ESC Slave Healthy
```

Controlar la falla de recuperación ESC

En los casos en los que ESC no puede iniciar la VM debido a un estado inesperado, Cisco recomienda realizar un switchover ESC reiniciando el ESC maestro. La conmutación ESC tardaría aproximadamente un minuto. Ejecute la secuencia de comandos "health.sh" en el nuevo Master ESC para comprobar si el estado está activo. Master ESC para iniciar la VM y corregir el estado de la VM. Esta tarea de recuperación tardaría hasta 5 minutos en completarse.

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.

En caso de que no se recupere la VM ESC, siga el procedimiento para implementar una nueva VM ESC. Póngase en contacto con el servicio de asistencia de Cisco para obtener información sobre el procedimiento.

Solución de problemas de RMA de componentes - Nodo controlador

Paso 1. Controlador - Precomprobaciones

Desde OSPD, inicie sesión en el controlador y verifique que los pc estén en buen estado - los tres controladores Online y galera muestran los tres controladores como maestro.

> **Nota:** Un clúster saludable requiere 2 controladores activos para verificar que los dos controladores restantes estén en línea y activos.

```
heat-admin@pod1-controller-0 ~]$ sudo pcs status
Cluster name: tripleo_cluster
Stack: corosync
Current DC: pod1-controller-2 (version 1.1.15-11.el7_3.4-e174ec8) - partition with quorum
Last updated: Mon Dec  4 00:46:10 2017                          Last change: Wed Nov 29 01:20:52
2017 by hacluster via crmd on pod1-controller-0
3 nodes and 22 resources configured
Online: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
Full list of resources:
 ip-11.118.0.42  (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 ip-11.119.0.47  (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 ip-11.120.0.49  (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 ip-192.200.0.102          (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 Clone Set: haproxy-clone [haproxy]
     Started: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
 Master/Slave Set: galera-master [galera]
     Masters: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
 ip-11.120.0.47  (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 Clone Set: rabbitmq-clone [rabbitmq]
     Started: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
 Master/Slave Set: redis-master [redis]
     Masters: [ pod1-controller-2 ]
     Slaves: [ pod1-controller-0 pod1-controller-1 ]
 ip-10.84.123.35            (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 openstack-cinder-volume          (systemd:openstack-cinder-volume):            Started pod1-
controller-2
 my-ipmilan-for-pod1-controller-0        (stonith:fence_ipmilan):  Started pod1-controller-0
 my-ipmilan-for-pod1-controller-1        (stonith:fence_ipmilan):  Started pod1-controller-0
 my-ipmilan-for-pod1-controller-2        (stonith:fence_ipmilan):  Started pod1-controller-0
Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

Paso 2. Mueva el clúster del controlador al modo de mantenimiento.

1. Ponga el clúster de pcs en el controlador que se actualiza en espera.

```
[heat-admin@pod1-controller-0 ~]$ sudo pcs cluster standby
```

2. Vuelva a comprobar el estado de los pc y asegúrese de que el clúster de pcs se ha detenido en este nodo.

```
[heat-admin@pod1-controller-0 ~]$ sudo pcs status
Cluster name: tripleo_cluster
```

```
Stack: corosync
Current DC: pod1-controller-2 (version 1.1.15-11.el7_3.4-e174ec8) - partition with quorum
Last updated: Mon Dec  4 00:48:24 2017                    Last change: Mon Dec  4
00:48:18 2017 by root via crm_attribute on pod1-controller-0
3 nodes and 22 resources configured
Node pod1-controller-0: standby
Online: [ pod1-controller-1 pod1-controller-2 ]
Full list of resources:
 ip-11.118.0.42  (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 ip-11.119.0.47  (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 ip-11.120.0.49  (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 ip-192.200.0.102          (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 Clone Set: haproxy-clone [haproxy]
     Started: [ pod1-controller-1 pod1-controller-2 ]
     Stopped: [ pod1-controller-0 ]
 Master/Slave Set: galera-master [galera]
     Masters: [ pod1-controller-1 pod1-controller-2 ]
     Slaves: [ pod1-controller-0 ]
 ip-11.120.0.47  (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 Clone Set: rabbitmq-clone [rabbitmq]
     Started: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
 Master/Slave Set: redis-master [redis]
     Masters: [ pod1-controller-2 ]
     Slaves: [ pod1-controller-1 ]
     Stopped: [ pod1-controller-0 ]
 ip-10.84.123.35            (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 openstack-cinder-volume          (systemd:openstack-cinder-volume):            Started
pod1-controller-2
 my-ipmilan-for-pod1-controller-0        (stonith:fence_ipmilan):  Started pod1-controller-
1
 my-ipmilan-for-pod1-controller-1        (stonith:fence_ipmilan):  Started pod1-controller-
1
 my-ipmilan-for-pod1-controller-2        (stonith:fence_ipmilan):  Started pod1-controller-
2
Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

3. Además, el estado de pcs en los otros 2 controladores debe mostrar el nodo como en espera.

Paso 3. Reemplace el componente defectuoso del nodo del controlador.

Apague el servidor especificado. Los pasos para reemplazar un componente defectuoso en el servidor UCS C240 M4 se pueden derivar de:

Sustitución de los componentes del servidor

Paso 4. Encienda el servidor.

1. Encienda el servidor y verifique que el servidor se active.

```
[stack@tb5-ospd ~]$ source stackrc
[stack@tb5-ospd ~]$ nova list |grep pod1-controller-0
| 1ca946b8-52e5-4add-b94c-4d4b8a15a975 | pod1-controller-0   | ACTIVE | -          |
```

```
Running     | ctlplane=192.200.0.112 |
```

2. Inicie sesión en el controlador afectado, quite el modo en espera configurando **unstandby**. Verify controller viene Online con cluster y galera muestra los tres controladores como Master. Esto puede tardar unos minutos.

```
[heat-admin@pod1-controller-0 ~]$ sudo pcs cluster unstandby
[heat-admin@pod1-controller-0 ~]$ sudo pcs status
Cluster name: tripleo_cluster
Stack: corosync
Current DC: pod1-controller-2 (version 1.1.15-11.el7_3.4-e174ec8) - partition with quorum
Last updated: Mon Dec  4 01:08:10 2017                          Last change: Mon Dec  4
01:04:21 2017 by root via crm_attribute on pod1-controller-0
3 nodes and 22 resources configured
Online: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
Full list of resources:
 ip-11.118.0.42  (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 ip-11.119.0.47  (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 ip-11.120.0.49  (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 ip-192.200.0.102          (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 Clone Set: haproxy-clone [haproxy]
     Started: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
 Master/Slave Set: galera-master [galera]
     Masters: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
 ip-11.120.0.47  (ocf::heartbeat:IPaddr2):           Started pod1-controller-2
 Clone Set: rabbitmq-clone [rabbitmq]
     Started: [ pod1-controller-0 pod1-controller-1 pod1-controller-2 ]
 Master/Slave Set: redis-master [redis]
     Masters: [ pod1-controller-2 ]
     Slaves: [ pod1-controller-0 pod1-controller-1 ]
 ip-10.84.123.35            (ocf::heartbeat:IPaddr2):           Started pod1-controller-1
 openstack-cinder-volume          (systemd:openstack-cinder-volume):            Started
pod1-controller-2
 my-ipmilan-for-pod1-controller-0        (stonith:fence_ipmilan):  Started pod1-controller-
1
 my-ipmilan-for-pod1-controller-1        (stonith:fence_ipmilan):  Started pod1-controller-
1
 my-ipmilan-for-pod1-controller-2        (stonith:fence_ipmilan):  Started pod1-controller-
2

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

3. Puede comprobar algunos de los servicios de supervisión como si se encuentran en un estado saludable.

```
[heat-admin@pod1-controller-0 ~]$ sudo ceph -s
    cluster eb2bb192-b1c9-11e6-9205-525400330666
     health HEALTH_OK
     monmap e1: 3 mons at {pod1-controller-0=11.118.0.10:6789/0,pod1-controller-
1=11.118.0.11:6789/0,pod1-controller-2=11.118.0.12:6789/0}
            election epoch 70, quorum 0,1,2 pod1-controller-0,pod1-controller-1,pod1-
controller-2
     osdmap e218: 12 osds: 12 up, 12 in
            flags sortbitwise,require_jewel_osds
      pgmap v2080888: 704 pgs, 6 pools, 714 GB data, 237 kobjects
            2142 GB used, 11251 GB / 13393 GB avail
```

```
              704 active+clean
client io 11797 kB/s wr, 0 op/s rd, 57 op/s wr
```