Componenti modulari RMA-PCRF

Sommario

Introduzione

Questo documento descrive i passaggi necessari per sostituire i componenti guasti menzionati qui in un server Cisco Unified Computing System (UCS) in una configurazione Ultra-M che ospita le funzioni di rete virtuale (VNF) di Cisco Policy Suite (CPS).

- Modulo di memoria DIMM (Dual In-line Memory Module) sostitutivo
- Errore del controller FlexFlash
- Errore unità a stato solido (SSD)
- Errore del TPM (Trusted Platform Module)
- Errore cache RAID
- Errore del controller RAID/HBA (Hot Bus Adapter)
- Errore riser PCI
- Scheda PCIe Intel X520 10G guasto
- Errore MLOM (Modular LAN-on Motherboard)

- Vassoio ventola RMA
- Errore CPU

Contributo di Nitesh Bansal, Cisco Advance Services.

Premesse

Ultra-M è una soluzione virtualizzata preconfezionata e convalidata, progettata per semplificare l'installazione di VNF. OpenStack è Virtualized Infrastructure Manager (VIM) per Ultra-M ed è costituito dai seguenti tipi di nodi:

- Calcola
- Disco Object Storage - Compute (OSD - Compute)
- Controller
- Piattaforma OpenStack - Director (OSPD)
- Per la definizione delle procedure descritte in questo documento, viene presa in considerazione la release Ultra M 5.1.x.
- Questo documento è destinato al personale Cisco che ha familiarità con la piattaforma Cisco Ultra-M e descrive i passaggi richiesti per essere eseguiti a livello di OpenStack e CPS VNF al momento della sostituzione del componente nel server.

Prima di sostituire un componente difettoso, è importante verificare lo stato corrente dell'ambiente della piattaforma Red Hat Open Stack. Si consiglia di controllare lo stato corrente per evitare complicazioni quando il processo di sostituzione è attivo.

In caso di ripristino, Cisco consiglia di eseguire il backup del database OSPD eseguendo i seguenti passaggi:

```
[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
```

Questo processo assicura che un nodo possa essere sostituito senza influire sulla disponibilità delle istanze.

> **Nota:** Se un server è un nodo di controller, passare alla sezione, altrimenti passare alla sezione successiva.

Abbreviazioni

VNF	Funzione di rete virtuale
PD	Policy Director (servizio di bilanciamento del carico)
PS	Server dei criteri (pcrfclient)
ESC	Elastic Service Controller
MOP	Metodo
OSD	Dischi Object Storage
HDD	Unità hard disk
SSD	Unità a stato solido

VIM	Virtual Infrastructure Manager
VM	Macchina virtuale
SM	Gestione sessioni
QNS	Quantum Name Server
UUID	Identificatore univoco universale

Risoluzione dei problemi relativi al componente RMA - Nodo di calcolo/OSD-calcolo

Passaggio 1. Chiusura normale

Identificare le VM ospitate nel nodo di calcolo/calcolo OSD

Compute/OSD-Compute può ospitare più tipi di VM. Identificare tutti i passaggi e procedere con i singoli passaggi insieme al nodo baremetale specifico e per i nomi di VM specifici ospitati in questo calcolo:

```
[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    |
```

Per lo spegnimento regolare della VM di Cluster Manager

Passaggio 1. Creare una copia istantanea e inviare il file tramite FTP in un'altra posizione all'esterno del server o, se possibile, all'esterno del rack stesso.

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

Passaggio 2. Arrestare la macchina virtuale da ESC.

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

Passaggio 3. Verificare se la macchina virtuale è arrestata.

```
[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
```

Per il PD/loadbalancer attivo VM Arresto normale

Passaggio 1. Accedere ad Active Lab e interrompere i servizi come indicato di seguito

- Passare dalla modalità attiva alla modalità standby

```
service corosync restart
```

- arresta servizi su lb standby

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

Passaggio 2. Dal master ESC.

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

Passaggio 3. Verificare se la macchina virtuale è arrestata.

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

Per il PD di standby/loadbalancer VM Spegnimento regolare

Passaggio 1. Accedere a standby lb e arrestare i servizi.

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

Passaggio 2. Dal master ESC.

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

Passaggio 3. Verificare se la macchina virtuale è arrestata.

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

Per PS/QNS VM Arresto normale

Passaggio 1. Arrestare il servizio:

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

Passaggio 2. Dal master ESC.

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

Passaggio 3. Verificare se la macchina virtuale è arrestata.

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

Per lo spegnimento regolare di VM SM

Passaggio 1. Arrestare tutti i servizi mongo presenti in sessionmgr.

```
 [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  ]
```

Passaggio 2. Dal master ESC.

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

Passaggio 3. Verificare se la macchina virtuale è arrestata.

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

Per OAM/pcrfclient VM Arresto normale

Passaggio 1. Verificare se il criterio SVN è sincronizzato tramite questi comandi. Se viene restituito un valore, il criterio SVN è già sincronizzato e non è necessario sincronizzarlo da PCRFCLIENT02. Se necessario, è comunque possibile ignorare il ripristino dall'ultimo backup.

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

Passaggio 2. Ristabilire la sincronizzazione master/slave SVN tra pcrfclient01 e pcrfclient02 con pcrfclient01 come master eseguendo la serie di comandi su 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
```

Passaggio 3. Eseguire un backup della SVN in Gestione cluster.

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

Passaggio 4. Arrestare i servizi in pcrfclient.

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

Passaggio 5. Dal master ESC:

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

Passaggio 6. Verificare se la macchina virtuale è arrestata.

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

Per la VM arbitro

Passaggio 1. Accedere per arbitrare e arrestare i servizi.

```
[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.
```

Passaggio 2.1 Dal master ESC.

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

Passaggio 3. Verificare se la macchina virtuale è arrestata.

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

Per Elastic Services Controller (ESC)

Passaggio 1. Le configurazioni di ESC-HA devono essere sottoposte a backup mensilmente, prima/dopo qualsiasi operazione di scalabilità verticale o orizzontale con VNF e prima/dopo le modifiche della configurazione con ESC. È necessario eseguire un backup di tale operazione per eseguire in modo efficace il ripristino di emergenza dei ESC

1. Accedere a ESC utilizzando le credenziali di amministratore ed esportare i dati opat in XML.

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

2. Scaricare il file nel computer locale di ftp/sftp in un server esterno al cloud.

Passaggio 2. Eseguire il backup della configurazione del cloud PCRF Tutti gli script e i file di dati utente a cui si fa riferimento nei file XML di distribuzione.

1. Trova tutti i file di dati utente a cui viene fatto riferimento nei file XML di distribuzione di tutte le VNF dai dati opdata esportati nel passaggio precedente.Output di esempio.

2. Trova tutti gli script post-distribuzione utilizzati per inviare l'API di orchestrazione CPS.

3. Frammenti di esempio di script post-distribuzione in esc opdata.

Campione 1:

Esempio 2:

Se i dati operativi ESC di distribuzione (estratti nel passaggio precedente) contengono uno dei file evidenziati, eseguire il backup.

Comando Backup di esempio:

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

Scaricare il file nel computer locale di ftp/sftp in un server esterno al cloud.

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.

Passaggio 2. Backup del database ESC.

Passaggio 1. Raccogliere i registri dalle VM di entrambe le VM ESC ed eseguirne il backup.

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

Passaggio 2. Eseguire il backup del database dal nodo ECS principale.

Passaggio 3. Passare all'utente root e controllare lo stato dell'ESC primario e verificare che il valore di output sia **Master**.

```
 $ sudo bash
 $ escadm status
```

```
Set ESC to maintenance mode & verify
```

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

Passaggio 4. Utilizzare una variabile per impostare il nome del file e includere le informazioni sulla data, chiamare lo strumento di backup e fornire la variabile filename del passaggio precedente.

```
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
```

Passaggio 5. Controllare il file di backup nell'archivio di backup e verificare che il file sia presente.

Passaggio 6. Ripristinare la modalità di funzionamento normale di Esc master.

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

Se l'utilità di backup dbtool non riesce, applicare la seguente soluzione una volta nel nodo ESC. Ripetere quindi il punto 6.

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

Passaggio 3. Migrare ESC alla modalità Standby.

Passaggio 1. Accedere all'ESC ospitato nel nodo e verificare se si trova nello stato master. In caso affermativo, passare alla modalità di standby.

```
[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!
```

Passaggio 2. Una volta che la VM è in modalità di standby ESC, arrestarla con il comando shutdown -r now

> **Nota:** Se il componente difettoso deve essere sostituito sul nodo OSD-Compute, attivare la manutenzione CEPH sul server prima di procedere con la sostituzione 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
```

Passaggio 4. Sostituire il componente difettoso dal nodo di calcolo/calcolo OSD-A.

Spegnere il server specificato. Per sostituire un componente guasto su un server UCS C240 M4, è possibile seguire la procedura descritta di seguito:

Sostituzione dei componenti server

Fare riferimento alla procedura Log persistente nella procedura riportata di seguito ed eseguire se necessario

Passaggio 5. Ripristinare le VM.

Ripristino VM da ESC

1. La macchina virtuale si troverebbe in stato di errore nell'elenco delle macchine virtuali.

```
[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. Ripristinare le VM dalla 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. Monitorare **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. Verificare tutti i servizi nelle VM in fase di avvio.

Ripristino di VM ESC

1. Accedere a ESC tramite la console e verificare lo stato.

2. Avvia i processi se non sono già stati avviati

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

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

Gestisci errore di ripristino ESC

Nei casi in cui ESC non riesca ad avviare la macchina virtuale a causa di uno stato imprevisto, Cisco consiglia di eseguire un passaggio ESC riavviando la macchina virtuale master. Il passaggio al CES richiede circa un minuto. Eseguire lo script "health.sh" sul nuovo Master ESC per verificare se lo stato è attivo. Master ESC per avviare la macchina virtuale e correggere lo stato della macchina virtuale. L'attività di ripristino può richiedere fino a 5 minuti.

Èpossibile monitorare /var/log/esc/yangesc.log e /var/log/esc/escmanager.log. Se NON si vede che la VM viene ripristinata dopo 5-7 minuti, l'utente deve procedere al ripristino manuale delle VM interessate.

Se la VM ESC non viene ripristinata, seguire la procedura per distribuire una nuova VM ESC. Contattare il supporto Cisco per informazioni sulla procedura.

Risoluzione dei problemi relativi al componente RMA - Controller Node

Passaggio 1. Controller - Controlli preliminari

Da OSPD, effettuare il login al controller e verificare che il pc sia in uno stato valido - tutti e tre i controller sono online e galera mostrano tutti e tre i controller come master.

> **Nota:** Un cluster integro richiede 2 controller attivi, quindi verificare che gli altri due controller siano online e attivi.

```
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
```

Passaggio 2. Spostare il cluster di controller in modalità di manutenzione.

1. Posizionare il cluster pcs sul controller da aggiornare in standby.

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

2. Controllare di nuovo lo stato dei pc e verificare che il cluster di pc sia stato arrestato in questo 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. Anche lo stato del pcs sugli altri 2 controller deve mostrare il nodo come in standby.

Passaggio 3. Sostituire il componente difettoso dal nodo del controller.

Spegnere il server specificato. È possibile fare riferimento alla procedura per sostituire un componente guasto sul server UCS C240 M4 da:

Sostituzione dei componenti server

Passaggio 4. Accendere il server.

1. Accendere il server e verificarne l'accensione.

```
[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. Accedere al controller interessato, rimuovere la modalità standby impostando **unstandby**. Verificare che il controller sia online con il cluster e che galera mostri tutti e tre i controller come Master. L'operazione potrebbe richiedere alcuni minuti.

```
[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. Èpossibile verificare che alcuni servizi di monitoraggio, ad esempio ceph, siano in stato integro.

```
[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
```