

Fehlerbehebung: PCRF-Cluster-Manager VM-Wiederherstellung - OpenStack

Inhalt

[Einführung](#)

[Fehlerbehebung](#)

[Schalten Sie Cluster Manager im SHUTOFF-Status ein.](#)

[Stellen Sie alle Instanzen aus dem FEHLERzustand wieder her.](#)

[CPS Cluster Manager durch Snapshot neu erstellen](#)

[Neubereitstellung von CPS Cluster Manager über Snapshot](#)

[Überprüfen](#)

Einführung

Dieses Dokument beschreibt die Schritte zur Wiederherstellung von vPCRF-Instanzen (Virtual Policy and Charging Rules Function) von Cisco, die in einer Ultra-M/OpenStack-Bereitstellung bereitgestellt werden.

Fehlerbehebung

Schalten Sie Cluster Manager im SHUTOFF-Status ein.

Wenn sich eine Instanz aufgrund eines geplanten Herunterfahrens oder aus einem anderen Grund im SHUTOFF-Zustand befindet, starten Sie die Instanz mit diesem Verfahren, und aktivieren Sie die Überwachung in Elastic Services Controller (ESC).

Schritt 1: Überprüfen Sie den Status der Instanz über OpenStack.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm_0
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634 |
destackovs-compute-2 | SHUTOFF|
```

Schritt 2: Überprüfen Sie, ob der Computer verfügbar ist, und stellen Sie sicher, dass der Status aktiv ist.

```
source /home/stack/destackovsrc
nova hypervisor-show destackovs-compute-2 | egrep 'status|state'
| state | up |
| status | enabled |
```

Schritt 3: Melden Sie sich als Admin-Benutzer beim ESC Master an, und überprüfen Sie den Zustand der Instanz in opdata.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli get esc_datamodel/opdata | grep cm_0
SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634 VM_ERROR_STATE
```

Schritt 4: Schalten Sie die Instanz von OpenStack ein.

```
source /home/stack/destackovsrc-Pcrf
nova start SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634
```

Schritt 5: Warten Sie fünf Minuten, bis die Instanz gestartet ist, und gehen Sie in den aktiven Zustand über.

```
source /home/stack/destackovsrc-Pcrf
nova list -fields name,status | grep cm_0
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634 |
ACTIVE
```

Schritt 6: Aktivieren Sie VM Monitor im ESC, nachdem die Instanz im aktiven Zustand ist.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634
```

Weitere Informationen zum Wiederherstellen von Instanzkonfigurationen finden Sie in den hier bereitgestellten Instanztypspezifischen Verfahren.

Stellen Sie alle Instanzen aus dem FEHLERzustand wieder her.

Dieses Verfahren kann verwendet werden, wenn der Zustand der CPS-Instanz in OpenStack FEHLER ist:

Schritt 1: Überprüfen Sie den Status der Instanz in OpenStack.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm_0
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634 |
destackovs-compute-2 | ERROR|
```

Schritt 2: Überprüfen Sie, ob der Computer verfügbar ist und fehlerfrei ausgeführt wird.

```
source /home/stack/destackovsrc
nova hypervisor-show destackovs-compute-2 | egrep 'status|state'
| state | up |
| status | enabled |
```

Schritt 3: Melden Sie sich als Admin-Benutzer beim ESC Master an, und überprüfen Sie den Zustand der Instanz in opdata.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli get esc_datamodel/opdata | grep cm_0
SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634 VM_ERROR_STATE
```

Schritt 4: Setzen Sie den Status der Instanz zurück, um die Instanz wieder in einen aktiven Zustand zu versetzen, anstatt einen Fehlerzustand. Starten Sie anschließend die Instanz neu.

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

```
nova reset-state --active SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634
nova reboot --hard SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634
```

Schritt 5: Warten Sie fünf Minuten, bis die Instanz gestartet ist, und gehen Sie in den aktiven Zustand über.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,status | grep cm_0
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634 |
ACTIVE |
```

Schritt 6: Wenn Cluster Manager den Status nach dem Neustart in AKTIV ändert, aktivieren Sie VM Monitor im ESC, nachdem die Cluster Manager-Instanz im aktiven Zustand ist.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR SVS1-tmo_cm_0_e3ac7841-7f21-45c8-9f86-3524541d6634
```

Verwenden Sie nach der Wiederherstellung in den aktiven Status bzw. in den Ausführungsstatus die Prozedur für den Instanztyp, um Konfigurationen/Daten aus der Sicherung wiederherzustellen.

CPS Cluster Manager durch Snapshot neu erstellen

Wenn die Cisco Policy Suite (CPS) im FEHLER-Status fixiert ist und die bereits beschriebenen Verfahren nicht eingeschaltet werden kann und die Instanz in OpenStack verfügbar ist. Es wird empfohlen, die Instanz durch ein Snapshot-Image neu zu erstellen.

Schritt 1: Stellen Sie sicher, dass der Snapshot der zuletzt bekannten guten Konfiguration als QCOW-Datei vorhanden ist. Verwenden Sie diese zuvor generierte Datei während des Backups, scp/sftp sie zurück zum OpenStack Platform-Director (OSPD)-Computing. Mit diesem Verfahren konvertieren Sie das Bild in ein Übersichtsbild:

```
source /home/stack/destackovsrc-Pcrf
glance image-create --name CPS_Cluman_13.1.1 --disk-format "qcow2" --container "bare" --file
/var/Pcrf/cluman_snapshot.raw
```

Alternativ,

```
glance image-create --name rebuild_cluman --file /home/stack/cluman_snapshot.raw --disk-format
qcow2 --container-format bare
```

Schritt 2: Verwenden Sie einen nova rebuild-Befehl auf OSPD, um die Cluman VM-Instanz mit dem hochgeladenen Snapshot wie gezeigt neu zu erstellen.

```
nova rebuild
```

Schritt 3: Warten Sie fünf Minuten, bis die Instanz gestartet ist, und gehen Sie in den aktiven Zustand über.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,status | grep cm
```

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

Schritt 4: Wenn Cluster Manager den Status nach der Wiederherstellung in "ACTIVE" ändert, überprüfen Sie den Zustand der Instanz in ESC und aktivieren Sie ggf. VM Monitor in ESC.

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

Schritt 5: Überprüfen Sie, ob das mit dem ursprünglichen ISO-Image des Cluster Manager verknüpfte Cinder-Volumen nach der Neubereitstellung mit der aktuellen Uhrzeit aktualisiert wird:

```
cinder list | grep tmobile-pcrf-13.1.1-1.iso  
| 2f6d7deb-60d6-40fa-926f-a88536cf98a3 | in-use | tmobile-pcrf-13.1.1-1.iso | 3 | -  
| true | a3f3bc62-0195-483a-bbc0-692bccd37307 |  
cinder show 2f6d7deb-60d6-40fa-926f-a88536cf98a3 | grep updated_at  
| updated_at | 2018-06-18T08:54:59.000000
```

```
updated_at | 2018-06-18T08:54:59.000000
```

Schritt 6: Schließen Sie Sicherungsdatenträger oder andere, zuvor an die Cluster Manager-Instanz angeschlossene Cinder-Volumen an, wenn diese nicht in vorherigen Schritten automatisch angeschlossen wurden.

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

```
cinder list
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
| ID | Status | Name | Size | Volume  
Type | Bootable | Attached to | |  
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
| 0e7ec662-b59e-4e3a-91a9-35c4ed3f51d7 | available | pcrf-atp1-mongo02 | 3 | -  
| false | | | |  
| 2f6d7deb-60d6-40fa-926f-a88536cf98a3 | in-use | tmobile-pcrf-13.1.1-1.iso | 3 | -  
| true | a3f3bc62-0195-483a-bbc0-692bccd37307 | | |  
| 4c553948-df75-4f0b-bf7b-0e64127dfda3 | available | pcrf-atp1-svn01 | 3 | -  
| false | | | |  
| 594c052e-aaa3-4c82-867d-3b36162244b3 | available | tmobile-pcrf-13.1.1-2.iso | 3 | -  
| true | | | |  
| 64953713-de86-40d5-a0e5-07db22d692f2 | in-use | tmobile-pcrf-13.1.1-1.iso | 3 | -  
| true | 80a93e90-59e2-43bd-b67e-5d766d0a2f11 | | |
```

```
openstack server add volume
```

Schritt 7: Wenn der Cluman-Snapshot alt ist und die Datensicherung `config_br.py` verfügbar ist, wurde ein Datums-Snapshot erstellt. Importieren Sie die Konfiguration aus der Sicherung, und überspringen Sie andernfalls diesen Schritt.

ssh

Schritt 8: Erstellen Sie alle VM-Images aus dem Backup über `config_br.py` im Cluster-Manager neu:

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

Neubereitstellung von CPS Cluster Manager über Snapshot

Wenn der CPS Cluster Manager VM verloren geht (kann nicht wiederhergestellt werden) und der Wiederherstellungsprozess (wie in 2.3 beschrieben) ebenfalls fehlgeschlagen ist, müssen Sie die Instanz über ESC erneut bereitstellen. Dieses Verfahren beschreibt den Prozess für die gleiche:

Schritt 1: Stellen Sie sicher, dass der Snapshot der zuletzt bekannten guten Konfiguration als QCOW-Datei vorhanden ist. Verwenden Sie diese zuvor generierte Datei während des Backups, scp/sftp sie zurück zum OSPD-Computing.

```
ls -ltr /var/Pcrf/cluman_snapshot.qcow  
-rw-r--r--. 1 root root 328514100 May 18 16:59 cluman_snapshot.qcow
```

Schritt 2: Mit diesem Verfahren konvertieren Sie das Bild in ein Übersichtsbild.

```
source /home/stack/destackovsrc-Pcrf  
glance image-create --name CPS_Cluman_13.1.1 --disk-format "qcow2" --container "bare" --file  
/var/Pcrf/cluman_snapshot.qcow
```

Schritt 3: Sobald das Bild verfügbar ist, melden Sie sich beim ESC an, und überprüfen Sie den Zustand der Cluster Manager-Instanz in ESC opdata.

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

Schritt 4: Stellen Sie sicher, dass die `/home/admin/PCRF_config.xml`-Datei wie in 2.1.1 gesichert vorhanden ist.

Schritt 5: Rufen Sie den Namen der Bereitstellung, den Tenant und die `vm_group` für Cluster-Manager ab, die wiederhergestellt werden sollen.

Beispiel für einen Ausschnitt:

Schritt 6: Löschen von Cluster Manager vm aus ESC:

Warnung: Der Befehl zum Entfernen der Instanz aus opdata sollte abgeschlossen sein, unvollständige Befehl kann die gesamte Bereitstellung löschen. Seien Sie vorsichtig! Der Befehl sollte immer alle Parameter enthalten, d. h. Tenant-Name, Bereitstellungsname und vm_group-Name.

```
/opt/cisco/esc/confd/bin/confd_cli -u admin -C
esc-ha-01# config
esc-ha-01(config)# no esc_datamodel tenants tenant Pcrf deployments deployment DEP1 vm_group cm
esc-ha-01(config)# commit
esc-ha-01(config)# exit
```

Der obige Schritt sollte die Instanz aus OpenStack sowie aus ESC Opdata entfernen. Mit anderen Worten, der Cluster Manager ist jetzt kein Teil der Bereitstellung.

Schritt 7: Stellen Sie sicher, dass die Cluster-Manager-Instanz aus der Bereitstellung von **yangesc.log**, **escmanager.log** in ESC- und Nova-Liste im OSPD-Knoten entfernt wird.

Schritt 8: Ändern Sie die in Schritt 2.1.1 gesicherte Datei **PCRF_config.xml** und ändern Sie den Namen des Cluster-Manager-Image in das neu erstellte Image aus dem Snapshot in den oben beschriebenen Schritten:

Vor der Änderung

```
<vm_group>
<name>cm</name>
<image>pcrf-13.1.1.qcow2</image>
```

Nach Änderung

```
<vm_group>
<name>cm</name>
<image>CPS_Cluman_13.1.1</image>
```

Schritt 9: Ändern Sie die Datei **PCRF_config.xml**, und entfernen Sie die Cloud-Benutzerdatendatei für die Cluster Manager-vm-Gruppe. Ein Beispiel für einen XML-Ausschnitt, der entfernt werden soll, ist hier dargestellt:

Schritt 10: Kopieren Sie die Datei **PCRF_config.xml** in den **/opt/cisco/esc/cisco-cps/config/Ordner**, in dem alle anderen Konfigurationsdateien vorhanden sind.

Schritt 11: Laden Sie die neue Konfigurationsdatei in ESC opdata zusammenführen.

```
/opt/cisco/esc/confd/bin/confd_cli -u admin -C
esc-ha-01# config
esc-ha-01(config)# load merge /opt/cisco/esc/cisco-cps/config/PCRF_config.xml
esc-ha-01(config)# commit
esc-ha-01(config)# exit
```

Schritt 12: Überwachen Sie die Liste `yangesc.log`, `escmanager.log` auf ESC und Nova im OSPD, um die Bereitstellung von Cluster Manager zu überprüfen.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,status| grep cm
| 96a5647e-9970-4e61-ab5c-5e7285543a09 | cm_0_a11a9068-df37-4974-9bd8-566f825d5e39 | ACTIVE
```

Schritt 13: Wenn Cluster Manager den Status nach der Wiederherstellung in "ACTIVE" ändert, überprüfen Sie den Zustand der Instanz in ESC und aktivieren Sie ggf. VM Monitor in ESC.

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

Schritt 14: Schließen Sie Sicherungsdatenträger oder andere Cinder-Volumes an, die zuvor an die Cluster Manager-Instanz angehängt wurden und nicht im vorherigen Schritt automatisch über EMC angehängt wurden.

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

ID	Status	Name	Size	Volume Type
4c478cce-c746-455a-93f1-3f360acb87ce	in-use	CPS_14.0.0.release.iso	3	-
7e5573d9-29bc-4ea0-b046-c666bb1f7e06	in-use	PCRF_backup	1024	-
d5ab1991-3e09-41f2-89f5-dd1cf8a9e172	in-use	svn01	2	-
d74988a7-1f59-4241-9777-fc4f2d4f3e78	in-use	svn02	2	-

```
openstack server add volume
```

Schritt 15: Wenn der Cluman-Snapshot alt ist und die Datensicherung `config_br.py` verfügbar ist, wurde ein Datums-Snapshot erstellt. Importieren Sie die Konfiguration aus der Sicherung, wenn nicht, überspringen Sie diesen Schritt.

ssh

Schritt 16: Erstellen Sie alle VM-Images aus dem Backup über **config_br.py** im Cluster-Manager neu:

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

Überprüfen

- Pingen Sie die Cluster-Manager-IP, um sicherzustellen, dass die Verbindung aktiv ist.
- SSH den Cluster-Manager, um die Zugänglichkeit zu überprüfen.
- Überprüfen Sie die Diagnose vom Cluster Manager, um sicherzustellen, dass der Systemstatus anderer VMs von CPS nicht beeinflusst wird.