Sicherungs- und Wiederherstellungsverfahren für verschiedene Ultra-M-Komponenten - CPS

Inhalt

Einführung

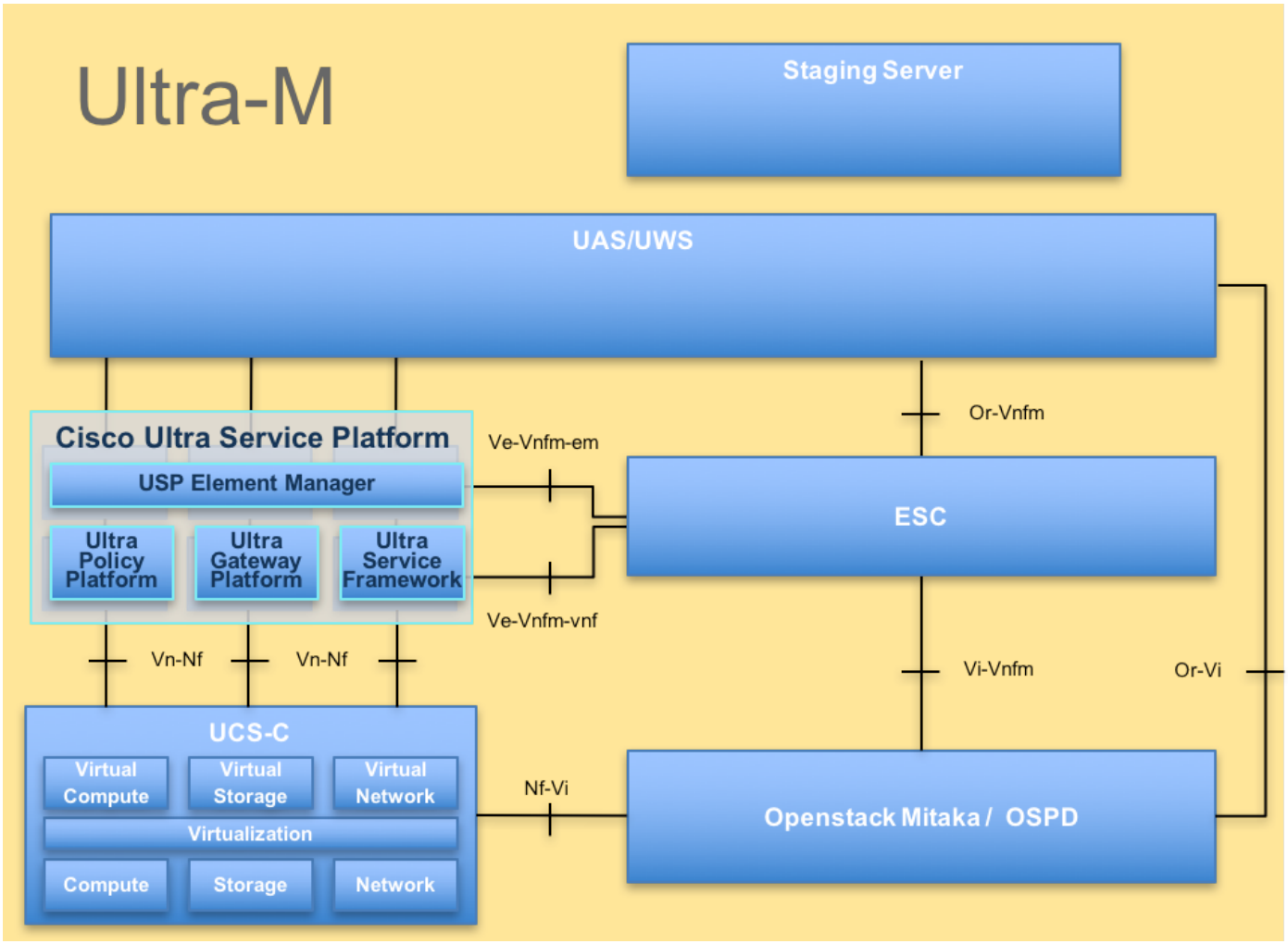
Dieses Dokument beschreibt die erforderlichen Schritte zum Sichern und Wiederherstellen eines virtuellen Systems (VM) in einer Ultra-M-Konfiguration, die CPS Virtual Network Functions (VNFs) hostet.

Hintergrundinformationen

Ultra-M ist eine vorkonfigurierte und validierte Kernlösung für virtualisierte mobile Pakete, die die Bereitstellung von VNFs vereinfacht. Die Ultra-M-Lösung besteht aus den folgenden VM-Typen:

- Elastic Services Controller (ESC)
- Cisco Policy Suite (CPS)

Die High-Level-Architektur von Ultra-M und die beteiligten Komponenten sind in diesem Bild dargestellt.



Hinweis: Ultra M 5.1.x wird zur Definition der Verfahren in diesem Dokument berücksichtigt. Dieses Dokument richtet sich an Mitarbeiter von Cisco, die mit der Cisco Ultra-M-Plattform vertraut sind.

Abkürzungen

VNF	Virtuelle Netzwerkfunktion
WSA	Elastic Service Controller
MOP	Verfahrensweise
OSD	Objektspeicherdatenträger
HDD	Festplattenlaufwerk
SSD	Solid-State-Laufwerk
VIM	Virtueller Infrastrukturmanager
VM	Virtuelles System
UUID	Universell eindeutige IDentifier

Sicherungsverfahren

OSPD-Sicherung

1. Überprüfen Sie den Status des OpenStack-Stacks und der Knotenliste.

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

2. Überprüfen Sie, ob alle unterCloud-Services über den OSP-D-Knoten im Status "load", "active" und "running" sind.

```
[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. Vergewissern Sie sich, dass genügend Speicherplatz verfügbar ist, bevor Sie den Sicherungsvorgang durchführen. Dieser Tarball soll mindestens 3,5 GB umfassen.

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

4. Führen Sie diese Befehle als Root-Benutzer aus, um die Daten vom unterCloud-Knoten in eine Datei mit dem Namen **undercloud-backup-[timestamp].tar.gz zu** sichern und auf den Backup-Server zu übertragen.

```
[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
```

ESC-Sicherung

1. ESC wiederum ruft Virtual Network Function (VNF) durch Interaktion mit VIM auf.

2. ESC bietet 1:1-Redundanz in der Ultra-M-Lösung. In Ultra-M werden 2 ESC-VMs bereitgestellt, die einen Ausfall unterstützen, d. h. das System wiederherstellen, wenn nur ein Systemfehler auftritt.

> **Hinweis**: Wenn mehr als ein Fehler vorliegt, wird dieser nicht unterstützt und erfordert möglicherweise eine Neubereitstellung des Systems.

ESC-Sicherungsdetails:

- Konfiguration wird ausgeführt
- ConfD CDB DB
- ESC-Protokolle
- Syslog-Konfiguration

3. Die Häufigkeit der ESC DB-Backups ist schwierig und muss sorgfältig behandelt werden, da der ESC die verschiedenen Statuscomputer für verschiedene bereitgestellte VNF VMs überwacht und verwaltet. Es wird empfohlen, dass diese Sicherungen nach den folgenden Aktivitäten in der gegebenen VNF/POD/Site durchgeführt werden

4. Stellen Sie sicher, dass der Zustand von ESC mit health.sh-Skript einwandfrei ist.

```
[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. Sichern Sie die Running-Konfiguration, und übertragen Sie die Datei auf den Backup-Server.

```
[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
```

Backup ESC-Datenbank

1. Melden Sie sich bei ESC VM an, und führen Sie den folgenden Befehl aus, bevor Sie die Sicherung durchführen.

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

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

2. Prüfen Sie den ESC-Modus, und vergewissern Sie sich, dass er sich im Wartungsmodus

befindet.

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

3. Backup-Datenbank mithilfe des in ESC verfügbaren Tools zur Wiederherstellung der Datenbanksicherung.

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

4. Setzen Sie ESC zurück in den Betriebsmodus, und bestätigen Sie den Modus.

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

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

5. Navigieren Sie zum Verzeichnis Scripts, und sammeln Sie die Protokolle.

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

sudo ./collect_esc_log.sh
```

6. So erstellen Sie einen Snapshot des ESC, um den ESC zuerst herunterzufahren.

```
shutdown -r now
```

7. Erstellen eines Image-Snapshots aus dem OSPD-Diagramm

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

8. Überprüfen, ob der Snapshot erstellt wird

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

9. ESC vom OSPD starten

```
nova start esc1
```

10. Wiederholen Sie das gleiche Verfahren für das Standby-ESC-VM, und übertragen Sie die Protokolle auf den Backup-Server.

11. Sichern der Syslog-Konfiguration auf beiden ESC VMS und Übertragen dieser auf den Backup-Server

```
[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
```

CPS-Sicherung

1. Erstellen einer Sicherung des CPS Cluster Manager

Verwenden Sie diesen Befehl, um die nova-Instanzen anzuzeigen und den Namen der Cluster Manager VM-Instanz zu beachten:

```
nova list
```

Stoppen des Clumans aus dem ESC

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

Schritt 2: Überprüfen Sie Cluster Manager im SHUTOFF-Status.

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

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

Schritt 3: Erstellen Sie ein nova-Snapshot-Image, wie im folgenden Befehl gezeigt:

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

> **Hinweis**: Stellen Sie sicher, dass Sie über genügend Speicherplatz für den Snapshot verfügen.

Wichtig - Falls VM nach der Snapshot-Erstellung nicht erreichbar ist, überprüfen Sie den Status von VM mithilfe des nova-Listenbefehls. Wenn der Status "SHUTOFF" lautet, müssen Sie das virtuelle System manuell starten.

Schritt 4: Zeigen Sie die Bildliste mit dem folgenden Befehl an: nova-Bildliste Abbildung 1: Beispielausgabe

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

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

Schritt 5: Wenn ein Snapshot erstellt wird, wird das Snapshot-Image in OpenStack Glance gespeichert. Um den Snapshot in einem Remote-Datenspeicher zu speichern, laden Sie den Snapshot herunter und übertragen Sie die Datei in OSPD an (/home/stack/CPS_BACKUP)

Um das Bild herunterzuladen, verwenden Sie den folgenden Befehl in OpenStack:

```
glance image-download –-file For example: glance image-download –-file snapshot.raw 2bbfb51c-cd05-4b7c-ad77-8362d76578db
```

Schritt 6: Führen Sie die heruntergeladenen Bilder wie im folgenden Befehl gezeigt auf:

```
ls –ltr *snapshot*

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

Schritt 7: Speichern Sie den Snapshot des Cluster Manager VM, der später wiederhergestellt werden soll.

2. Sichern Sie die Konfiguration und die Datenbank.

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

Überprüfen Sie auf der Crontab -l, ob eine andere Sicherung erforderlich ist.

Übertragen Sie alle Sicherungen auf das OSPD /home/stack/CPS_BACKUP

3. Sicherungsdatei von ESC Master

```
/opt/cisco/esc/confd/bin/netconf-console --host 127.0.0.1 --port 830 -u <admin-user> -p <admin-password> --get-config > /home/admin/ESC_config.xml
```

Übertragen Sie die Datei in OSPD /home/stack/CPS_BACKUP

4. Sichern von Crontab-l-Einträgen

Erstellen Sie eine TXT-Datei mit crontab -l und ftp it to remote location (in OSPD /home/stack/CPS_BACKUP).

5. Sicherung der Routendateien von LB und PCRF-Client

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

Wiederherstellungsverfahren

OSPD-Wiederherstellung

Das OSPD-Wiederherstellungsverfahren wird auf der Grundlage der folgenden Annahmen durchgeführt:

1. Die OSPD-Sicherung ist über den alten OSPD-Server verfügbar.

2. OSPD Recovery wird auf dem neuen Server durchgeführt, der den alten OSPD-Server im System ersetzt. .

ESC-Wiederherstellung

1. Wenn sich das virtuelle System im Fehlermodus oder im heruntergefahrenen Zustand befindet, kann das virtuelle System erneut gestartet werden. Führen Sie diese Schritte aus, um ESC wiederherzustellen.

2. Identifizieren Sie die VM, die sich im FEHLER- oder Herunterfahren-Zustand befindet, nachdem Sie einen harten Neustart der ESC VM identifiziert haben. In diesem Beispiel starten Sie auto-test-vnfm1-ESC-0 neu.

```
[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. Wenn ESC VM gelöscht wird und wieder aktiviert werden muss. Führen Sie die folgenden Schritte aus:

```
[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. Wenn ESC VM nicht wiederherstellbar ist und die Wiederherstellung der Datenbank erfordert, stellen Sie die Datenbank aus der zuvor durchgeführten Sicherung wieder her.

5. Für die Wiederherstellung der ESC-Datenbank muss vor der Wiederherstellung der Datenbank sichergestellt werden, dass der Dienst esc beendet wird. Führen Sie für ESC HA zunächst eine sekundäre VM und dann die primäre VM aus.

```
# service keepalived stop
```

6. Überprüfen Sie den ESC-Dienststatus, und stellen Sie sicher, dass alle Vorgänge sowohl in primären als auch in sekundären VMs für HA beendet werden.

```
# escadm status
```

7. Führen Sie das Skript aus, um die Datenbank wiederherzustellen. Im Rahmen der Wiederherstellung der DB zur neu erstellten ESC-Instanz fördert das Tool auch eine der Instanzen als primären ESC, mountet ihren DB-Ordner auf dem laufenden Gerät und startet die PostgreSQL-Datenbank.

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

8. Starten Sie den ESC-Dienst neu, um die Datenbankwiederherstellung abzuschließen. Wenn HA in beiden VMs ausgeführt wird, starten Sie den Keepalived Service neu.

```
# service keepalived start
```

9. Sobald die VM erfolgreich wiederhergestellt und ausgeführt wurde, Stellen Sie sicher, dass alle Syslog-spezifischen Konfigurationen aus der vorherigen erfolgreichen, bekannten Sicherung wiederhergestellt werden. Stellen Sie sicher, dass es in allen ESC VMs wiederhergestellt wird.

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

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

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

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

10. Wenn der ESC aus dem OSPD-Snapshot neu erstellt werden muss, verwenden Sie diesen Befehl unter Verwendung des während des Backups erstellten Snapshots.

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

11. Überprüfen Sie den Status des ESC nach Abschluss der Wiederherstellung.

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

12. Überprüfen Sie den ESC-Status mit dem folgenden Befehl

```
health.sh

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

Wenn ESC zum Starten von VM fehlschlägt

- In einigen Fällen kann ESC aufgrund eines unerwarteten Zustands nicht die VM starten. Eine Problemumgehung besteht darin, einen ESC-Switchover durchzuführen, indem der Master-ESC neu gestartet wird. Der ESC-Switchover dauert etwa eine Minute. Führen Sie health.sh auf dem neuen Master-ESC aus, um zu überprüfen, ob er aktiviert ist. Wenn der ESC Master wird, kann ESC den VM-Status reparieren und das virtuelle System starten. Da dieser Vorgang geplant ist, müssen Sie 5-7 Minuten warten, bis er abgeschlossen ist.
- Sie können /var/log/esc/yangesc.log und /var/log/esc/escmanager.log überwachen. Wenn Sie NICHT sehen, dass VM nach 5-7 Minuten wiederhergestellt wird, muss der Benutzer die manuelle Wiederherstellung der betroffenen VM(s) durchführen.
- Sobald die VM erfolgreich wiederhergestellt und ausgeführt wurde, Stellen Sie sicher, dass alle Syslog-spezifischen Konfigurationen aus der vorherigen erfolgreichen, bekannten Sicherung wiederhergestellt werden. Stellen Sie sicher, dass es in allen ESC VMs wiederhergestellt ist.

```
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
```

CPS-Wiederherstellung

Stellen Sie Cluster Manager VM in OpenStack wieder her

Schritt 1 Kopieren Sie den Snapshot des Cluster Manager VM auf den Controller-Blade, wie in folgendem Befehl gezeigt:

```
ls –ltr *snapshot*

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

Schritt 2 Laden Sie das Snapshot-Image aus dem Datenspeicher in OpenStack hoch:

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

Schritt 3 Überprüfen Sie, ob der Snapshot mit einem Nova-Befehl hochgeladen wird, wie im folgenden Beispiel gezeigt:

```
nova image-list
```

Abbildung 2: Beispielausgabe

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

Schritt 4 Je nachdem, ob die Cluster-Manager-VM vorhanden ist oder nicht, können Sie den Cluman erstellen oder den Cluman neu erstellen:

·Wenn die Cluster Manager VM-Instanz nicht vorhanden ist, erstellen Sie die Cluman VM mit einem Heat- oder Nova-Befehl, wie im folgenden Beispiel gezeigt:

Erstellen einer Cluman VM mit ESC

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

Der PCRF-Cluster wird mithilfe des obigen Befehls ausgelöst und stellt dann die Cluster-Manager-Konfigurationen aus den Backups wieder her, die mit config_br.py-Wiederherstellung erstellt wurden, sowie die Mongorestore aus dem in der Sicherung übernommenen Dump.

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

· Wenn die Instanz der Cluster Manager VM vorhanden ist, verwenden Sie einen nova rebuild-Befehl, um die Cluman VM-Instanz mit dem hochgeladenen Snapshot wie folgt neu zu erstellen:

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

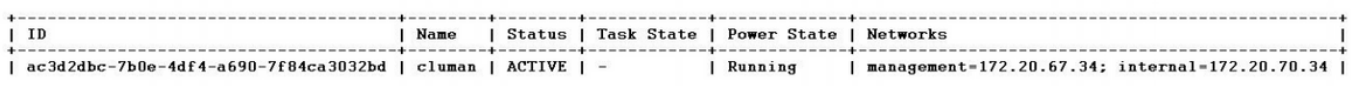
Beispiel:

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

Schritt 5 Listen Sie alle Instanzen wie gezeigt auf, und überprüfen Sie, ob die neue Instanz des Cluster-Managers erstellt und ausgeführt wird:

```
nova list
```

Abbildung 3: Beispielausgabe



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

Stellen Sie die neuesten Patches auf dem System wieder her

```
1.	Copy the patch files to cluster manager which were backed up in OSPD /home/stack/CPS_BACKUP
2.	Login to the Cluster Manager as a root user.
```

```
3.       Untar the patch by executing the following command:  tar -xvzf [patch name].tar.gz
4.       Edit /etc/broadhop/repositories and add the following entry:  file:///$path_to_the
plugin/[component name]
5.       Run build_all.sh script to create updated QPS packages:
/var/qps/install/current/scripts/build_all.sh
6.       Shutdown all software components on the target VMs:  runonall.sh sudo monit stop all
7.       Make sure all software components are shutdown on target VMs:  statusall.sh
```

Hinweis: Die Softwarekomponenten müssen als aktuellen Status "Nicht überwacht" anzeigen.

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

Wiederherstellen von Cronjobs

1. Verschieben Sie die gesicherte Datei von OSPD in den Cluman/Crfclient01.

2. Führen Sie den Befehl aus, um den Cronjob von der Sicherung aus zu aktivieren.

```
#crontab Cron-backup
```

3. Überprüfen Sie, ob die Cronjobs mit dem folgenden Befehl aktiviert wurden.

```
#crontab -l
```

Wiederherstellen einzelner VMs im Cluster

So stellen Sie die VM pcrfclient01 erneut bereit:

Schritt 1 Melden Sie sich als Root-Benutzer beim Cluster Manager VM an.

Schritt 2 Notieren Sie die UUID des SVN-Repositorys mit dem folgenden Befehl:

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

Der Befehl gibt die UUID des Repositorys aus.

Beispiel: Repository-UUID: ea50bd2-5726-46b8-b807-10f4a7424f0e

Schritt 3 Importieren Sie die Konfigurationsdaten für den Backup Policy Builder im Cluster Manager, wie im folgenden Beispiel gezeigt:

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

Hinweis: Viele Bereitstellungen führen einen Cron-Auftrag aus, der Konfigurationsdaten regelmäßig sichert.Weitere Einzelheiten finden Sie unter Subversion Repository Backup.

Schritt 4 Führen Sie den folgenden Befehl aus, um die VM-Archivdateien im Cluster Manager mit den neuesten Konfigurationen zu generieren:

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

Schritt 5 Führen Sie zum Bereitstellen des virtuellen Systems pcrfclient01 einen der folgenden Schritte aus:

Verwenden Sie in OpenStack die HEAT-Vorlage oder den Befehl Nova, um die VM neu zu erstellen. Weitere Informationen finden Sie in der CPS-Installationsanleitung für OpenStack.

Schritt 6 Erneutes Herstellen der SVN-Master-/Slave-Synchronisierung zwischen pcrfclient01 und pcrfclient02 mit pcrfclient01 als Master durch Ausführen der folgenden Befehlsreihe.

Wenn SVN bereits synchronisiert ist, geben Sie diese Befehle nicht aus.

Um zu überprüfen, ob SVN synchronisiert ist, führen Sie den folgenden Befehl von pcrfclient02 aus.

Wenn ein Wert zurückgegeben wird, ist das SVN bereits synchronisiert:

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

Führen Sie die folgenden Befehle aus pcrfclient01 aus:

```
/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
```

Schritt 7 Wenn pcrfclient01 auch die beliebige VM ist, führen Sie die folgenden Schritte aus:

a) Erstellen Sie die mongodb start/stop Skripts auf Basis der Systemkonfiguration. Nicht in allen Bereitstellungen sind alle Datenbanken konfiguriert.

Hinweis: Unter /etc/broadhop/mongoConfig.cfg können Sie ermitteln, welche Datenbanken eingerichtet werden müssen.

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

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

b) Starten des Mongo-Prozesses:

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

c) Warten Sie, bis der Schiedsrichter startet, und führen Sie dann diagnostics.sh —get_replica_status aus, um den Zustand des Replikationssatzes zu überprüfen.

So stellen Sie die VM pcrfclient02 erneut bereit:

Schritt 1 Melden Sie sich als Root-Benutzer bei der Cluster Manager VM an.

Schritt 2 Führen Sie den folgenden Befehl aus, um die VM-Archivdateien im Cluster Manager mit den neuesten Konfigurationen zu generieren:

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

Schritt 3 Führen Sie einen der folgenden Schritte aus, um die VM pcrfclient02 bereitzustellen: Verwenden Sie in OpenStack die HEAT-Vorlage oder den Befehl Nova, um die VM neu zu erstellen. Weitere Informationen finden Sie in der CPS-Installationsanleitung für OpenStack.

Schritt 4 Sichern Sie die Shell zum pcrfclient01:

```
ssh pcrfclient01
```

Schritt 5 Führen Sie das folgende Skript aus, um die SVN-Repos von pcrfclient01 wiederherzustellen:

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

So stellen Sie eine sitzungsmgr VM wieder bereit:

Schritt 1 Melden Sie sich als Root-Benutzer bei der Cluster Manager VM an.

Schritt 2 Führen Sie einen der folgenden Schritte durch, um die sitzungsmgr VM bereitzustellen und die ausgefallene oder beschädigte VM zu ersetzen:

Verwenden Sie in OpenStack die HEAT-Vorlage oder den Befehl Nova, um die VM neu zu erstellen. Weitere Informationen finden Sie in der CPS-Installationsanleitung für OpenStack.

Schritt 3 Erstellen Sie die mongodb start/stop-Skripts, die auf der Systemkonfiguration basieren.

Nicht in allen Bereitstellungen sind alle Datenbanken konfiguriert. Unter /etc/broadhop/mongoConfig.cfg können Sie ermitteln, welche Datenbanken eingerichtet werden müssen.

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

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

Schritt 4 Sichern Sie die Shell zum sitzungsmgr VM, und starten Sie den Mongo-Prozess:

```
ssh sessionmgrXX

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

Schritt 5 Warten Sie, bis die Member gestartet sind und die sekundären Member synchronisiert werden, und führen Sie dann diagnostics.sh —get_replica_status aus, um den Zustand der Datenbank zu überprüfen.

Schritt 6 Um die Session Manager-Datenbank wiederherzustellen, verwenden Sie einen der folgenden Beispielbefehle, je nachdem, ob die Sicherung mit der Option —mongo-all oder —mongo durchgeführt wurde:

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

or

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

So stellen Sie die VM Policy Director (Load Balancer) erneut bereit:

Schritt 1 Melden Sie sich als Root-Benutzer beim Cluster Manager VM an.

Schritt 2 Führen Sie den folgenden Befehl aus, um die Backup Policy Builder-Konfigurationsdaten im Cluster Manager zu importieren:

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

Schritt 3 Führen Sie den folgenden Befehl aus, um die VM-Archivdateien im Cluster Manager mit den neuesten Konfigurationen zu generieren:

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

Schritt 4 Führen Sie zum Bereitstellen des virtuellen Systems lb01 einen der folgenden Schritte aus:

Verwenden Sie in OpenStack die HEAT-Vorlage oder den Befehl Nova, um die VM neu zu erstellen. Weitere Informationen finden Sie in der CPS-Installationsanleitung für OpenStack.

So stellen Sie die Policy Server (QNS) VM wieder bereit:

Schritt 1 Melden Sie sich als Root-Benutzer beim Cluster Manager VM an.

Schritt 2 Importieren Sie die Backup Policy Builder-Konfigurationsdaten auf den Cluster Manager, wie im folgenden Beispiel gezeigt:

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

Schritt 3 Führen Sie den folgenden Befehl aus, um die VM-Archivdateien im Cluster Manager mit den neuesten Konfigurationen zu generieren:

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

Schritt 4 Führen Sie zum Bereitstellen der qns VM einen der folgenden Schritte aus:
Verwenden Sie in OpenStack die HEAT-Vorlage oder den Befehl Nova, um die VM neu zu erstellen. Weitere Informationen finden Sie in der CPS-Installationsanleitung für OpenStack.

Allgemeine Vorgehensweise für die Datenbankwiederherstellung

Schritt 1 Führen Sie den folgenden Befehl aus, um die Datenbank wiederherzustellen:

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

Beispiel:

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

Schritt 2 Melden Sie sich bei der Datenbank an, und überprüfen Sie, ob diese ausgeführt wird und darauf zugegriffen werden kann:

1. Melden Sie sich beim Sitzungsmanager an:

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

wobei "$port" die Portnummer der zu überprüfenden Datenbank ist. Zum Beispiel ist 27718 der Standard-Balance-Port.

2. Zeigen Sie die Datenbank an, indem Sie den folgenden Befehl ausführen:

```
show dbs
```

3. Wechseln Sie die Mongo-Shell zur Datenbank, indem Sie den folgenden Befehl ausführen:

```
use $db
```

wobei $db ein im vorherigen Befehl angezeigter Datenbankname ist.

Der Befehl 'use' schaltet die Mongo-Shell auf diese Datenbank.

Beispiel:

```
use balance_mgmt
```

4. Um die Auflistungen anzuzeigen, führen Sie den folgenden Befehl aus:

```
show collections
```

5. Um die Anzahl der Datensätze in der Auflistung anzuzeigen, führen Sie den folgenden Befehl aus:

```
db.$collection.count()

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

Im obigen Beispiel wird die Anzahl der Datensätze in der Sammelanschlussdatenbank (balance_mgmt) angezeigt.

Subsystemwiederherstellung

Führen Sie den folgenden Befehl aus, um die Policy Builder-Konfigurationsdaten aus einer Sicherung wiederherzustellen:

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

Grafana Dashboard wiederherstellen

Sie können das Grafana-Dashboard mit dem folgenden Befehl wiederherstellen:

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

Überprüfen der Wiederherstellung

Nachdem Sie die Daten wiederhergestellt haben, überprüfen Sie das Betriebssystem, indem Sie den folgenden Befehl ausführen:

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