PCRF VM-Wiederherstellungsverfahren - OpenStack

Inhalt

Einführung

In den Dokumenten wird beschrieben, wie die Instanzen Virtual Cisco Policy and Charging Rules Function (vPCRF) in einer Ultra-M/OpenStack-Umgebung wiederhergestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- OpenStack
- Cisco Policy Suite (CPS)
- Computing für die betroffenen Instanzen ist jetzt verfügbar
- Rechenressourcen sind in derselben Verfügbarkeitszone verfügbar wie die betroffene Instanz.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Sicherungsverfahren

Schritt 1: Elastic Services Controller (ESC)

Die Konfigurationen in ESC-HA müssen monatlich gesichert werden, vor/nach einem Scale-Up-

oder Scale-Down-Vorgang mit dem VNF und vor/nach Konfigurationsänderungen beim ESC. Es muss gesichert werden, um eine effektive Notfallwiederherstellung des ESC zu erreichen.

ESC opdata als XML

Führen Sie diese Schritte aus, um die ESC-**opdata** als XML zu exportieren:

1. Melden Sie sich mithilfe von Administratoranmeldeinformationen beim ESC an.

2. Exportieren **von Opdaten** in XML:

```
/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
```

3. Laden Sie diese Datei auf Ihren lokalen Computer von **ftp/sftp** auf einen Server außerhalb der Cloud herunter.

4. Alle Skripts und Benutzerdatendateien, auf die in Bereitstellungs-XMLs verwiesen wird. Suchen Sie alle Benutzerdatendateien, auf die in Bereitstellungs-XMLs aller VNFs verwiesen wird, aus den im vorherigen Schritt exportierten Opdata.

```
grep "file://" /home/admin/ESC_config.xml | sort | uniq
```

Beispielausgabe:

```
<file>file://opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-cm_cloud.cfg</file>

<file>file://opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-oam_cloud.cfg</file>

<file>file://opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-pd_cloud.cfg</file>

<file>file://opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-qns_cloud.cfg</file>

<file>file://opt/cisco/esc/cisco-cps/config/gr/cfg/std/pcrf-sm_cloud.cfg</file>
```

5. Suchen Sie nach allen Skripts, die nach der Bereitstellung zum Senden der CPS-Orchestrierungs-API verwendet werden.

6. Beispielausschnitte des **Post_deploy-**Skripts in **ESC opdata**

Beispielausgabe:

```
<policies>
      <policy>
         <name>PCRF_POST_DEPLOYMENT</name>
       <conditions>
          <condition>
            <name>LCS::POST_DEPLOY_ALIVE</name>
           </condition>
         </conditions>
```

```
            <actions>
               <action>
                 <name>FINISH_PCRF_INSTALLATION</name>
                 <type>SCRIPT</type>
                 <properties>
 ----------
<property>
                  <name>script_filename</name>
                        <value>/opt/cisco/esc/cisco-cps/config/gr/tmo/cfg/../cps_init.py</value>
                        </property>
                        <property>
                          <name>script_timeout</name>
                          <value>3600</value>
                        </property>
                      </properties>
                    </action>
                  </actions>
                </policy>
              </policies>
```

Beispiel 2:

```
<policy>
  <name>PCRF_POST_DEPLOYMENT</name>
  <conditions>
    <condition>
      <name>LCS::POST_DEPLOY_ALIVE</name>
    </condition>
  </conditions>
  <actions>
     <action>
       <name>FINISH_PCRF_INSTALLATION</name>
       <type>SCRIPT</type>
       <properties>
         <property>
            <name>CLUMAN_MGMT_ADDRESS</name>
            <value>10.174.132.46</value>
          </property>
          <property>
            <name>CLUMAN_YAML_FILE</name>
            <value>/opt/cisco/esc/cisco-cps/config/vpcrf01/ cluman_orch_config.yaml</value>
          </property>
          <property>
            <name>script_filename</name>
            <value>/opt/cisco/esc/cisco-
cps/config/vpcrf01/vpcrf_cluman_post_deployment.py</value>
          </property>
          <property>
            <name>wait_max_timeout</name>
            <value>3600</value>
          </property>
        </properties>
      </action>
    </actions>
</policy>
```

Wenn die Bereitstellung von **ESC Opdata** (die im vorherigen Schritt extrahiert wurde) die hervorgehobenen Dateien enthält, sichern Sie diese mithilfe dieses Befehls.

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

Laden Sie diese Datei auf Ihren lokalen Computer von **ftp/sftp** auf einen Server außerhalb der Cloud herunter.

> **Hinweis**: Obwohl **opdata** zwischen ESC Primary und Standby synchronisiert wird, werden Verzeichnisse, die Benutzerdaten, XML- und Nachbereitungsskripts enthalten, nicht in beiden Instanzen synchronisiert. Es wird empfohlen, dass Kunden den Inhalt des Verzeichnisses, das diese Dateien enthält, mithilfe von SCP oder SFTP verschieben. Diese Dateien sollten über ESC-Primary und ESC-Standby konstant sein, um eine Bereitstellung wiederherzustellen, wenn ein zum Zeitpunkt der Bereitstellung primäres ESC VM nicht verfügbar ist.

Vorgeschlagener Sicherungszeitplan im ESC

Dies sind empfohlene Crontab-Einträge für den Root-Benutzer, die in ESC Primary und ESC Standby hinzugefügt werden sollen. Sie können jedoch die Stunden/den Tag/Monat entsprechend den Anforderungen und der Häufigkeit von Änderungen im Netzwerk ändern.

```
30 01 * * * tar –zcf /home/admin/esc_files_backup_$(date +"\%Y-\%m-\%d").tgz
/opt/cisco/esc/cisco-cps/config/
00 02 * * * /opt/cisco/esc/confd/bin/netconf-console --host 127.0.0.1 --port 830 -u <admin-user>
-p <admin-password> --get-config > /home/admin/ESC_config_$(date +"\%Y-\%m-\%d").xml
```

Schritt 2: Cisco Policy Suite-Backup

Cluster Manager fungiert als primäre Marionette für ein CPS-Cluster. Daher ist es notwendig, einen Snapshot dieser Instanz zu erstellen. Das von Cisco bereitgestellte Sicherungs- und Wiederherstellungs-Dienstprogramm kann auch zum Erfassen von Backups von mongoDB, Richtlinienkonfiguration, Pfropfen-DB, Benutzern, Netzwerken und anderen pcrf-Konfigurationsdateien verwendet werden. Diese Dateien sollten häufig mithilfe des CPS-Sicherungs-Dienstprogramms gesichert und an einem Ort außerhalb der Ultra-M-Cloud gespeichert werden.

Snapshot des Cluster Manager VM

Cluster Manager Instance Snapshot muss monatlich gesichert werden, auch vor und nach Konfigurationsänderungen, Patch-Updates und Upgrades. Alte Snapshots können nach erfolgreichen Aktivitäten gelöscht werden, um Speicherplatz zu sparen. Dieses Verfahren beschreibt die Schritte zum Sichern der Cluster-Manager-Instanz als Snapshot:

1. Mit diesem Befehl können Sie die nova-Instanzen anzeigen und den Namen der Cluster Manager VM-Instanz beachten:

```
nova list
```

2. Erstellen Sie ein nova-Snapshot-Image, wie hier gezeigt:

```
nova image-create --poll <cluman_instance_name> <cluman_snapshot_name>
```

Beispielausgabe:

```
Server snapshotting... 100% complete

Finished
```

> **Hinweis**: Stellen Sie sicher, dass Sie über genügend Speicherplatz für den Snapshot verfügen. Der Cluster Manager ist zum Zeitpunkt der Erstellung des Snapshots manchmal nicht erreichbar und wird nach dem Erstellen des Snapshots wieder fortgesetzt. Wenn die Instanz selbst nach Abschluss des Snapshot-Prozesses nicht erreichbar bleibt, überprüfen Sie den Status der VM mithilfe des Befehls **nova list**. Wenn es sich im **SHUTOFF**-Zustand befindet, müssen Sie das virtuelle System manuell starten, wobei der **nova start-**Befehl verwendet wird.

3. Stellen Sie sicher, dass das Snapshot-Image mit diesem Befehl erstellt wird.

```
glance image-list
```

Beispielausgabe:

```
+--------------------------------------+--------------------------------------+
| ID                                   | Name                                 |
+--------------------------------------+--------------------------------------+
| 1683d05f-2a9f-46d8-877d-10982ee819e1 | cluman_backup_image                  |
| 30f2ece1-6438-4ef7-b4cf-44a0e7de183e | CPS_13.1.1.release.iso               |
| d38321a1-27c1-4c47-bc0f-24aedab5867a | CPS_13.1.1_Base                      |
+--------------------------------------+--------------------------------------+
```

4. Wenn Sie Plattformänderungen durchführen, bei denen Ceph betroffen sein könnte, wird immer empfohlen, den Snapshot von Cluster Manager in eine QCOW-Datei zu konvertieren und an einem Remote-Speicherort zu speichern.

```
glance image-download --file /var/Pcrf/cluman_snapshot.raw <image-id of the snapshot>
```

5. Laden Sie diese Datei auf Ihren lokalen Computer von **ftp/sftp** auf einen Server außerhalb der Cloud herunter.

Sicherung von CPS-Konfigurationen und Datenbanken

1. Für die Sicherung von CPS-Konfigurationen und Datenbankinhalten ist das Dienstprogramm **config_br.py** in der CPS-Plattform integriert. Details zur Verwendung des Dienstprogramms **config_br.py** finden Sie im CPS-Sicherungs- und Wiederherstellungsleitfaden. Dies ist ein Beispiel-Crontab im Cluster-Manager, um alle Konfigurationen und Datenbanken täglich um 100 Uhr zu sichern.

```
00 01 * * * /var/platform/modules/config_br.py -a export --all /mnt/backup/backup_$(date +\%Y-\%m-\%d).tar
```

2. MongoDB kann alternativ durch den Einsatz von **mongodump** gesichert werden.

```
30 01 * * * mongodump --host sessionmgr01 –port 27721 --out /mnt/backup/mongo_admin_27721_$(date +\%Y-\%m-\%d)/

30 01 * * * mongodump --host sessionmgr01 –port 27720 --out /mnt/backup/mongo_spr_27720_$(date +\%Y-\%m-\%d)/
```

```
30 01 * * * mongodump --host sessionmgr01 –port 27718 --out /mnt/backup/mongo_bal_27718_$(date
+\%Y-\%m-\%d)/

30 01 * * * mongodump --host sessionmgr01 –port 27719 --out
/mnt/backup/mongo_report_27721_$(date +\%Y-\%m-\%d)/
```

3. Backup-Orchestrierung YAML.

```
curl -i -X GET http://<Cluster Manager IP>:8458/api/system/config -H "Content-Type:
application/yaml" > /mnt/backup/CPS_orc_$(date +\%Y-\%m-\%d).yaml
```

Wenn das System über eine CPS-Orchestrierungs-API konfiguriert wird, wird empfohlen, auch diese Konfiguration zu sichern.

> **Hinweis**: Alle Backups müssen außerhalb von CPS VNF und vorzugsweise außerhalb der Cloud, auf der CPS bereitgestellt wird, gespeichert/übertragen werden.

Fehlerbehebung

Wiederherstellungsverfahren für CPS-VNF-Instanzen

Schalten Sie jede Instanz aus dem SHUTOFF-Zustand 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 im ESC.

1. Überprüfen Sie den Zustand einer Instanz über OpenStack.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f| destackovs-
compute-2  | SHUTOFF|
```

2. Überprüfen Sie, ob Compute verfügbar ist, und stellen Sie sicher, dass der Status aktiv ist.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f| destackovs-
compute-2  | SHUTOFF|
```

3. Melden Sie sich als Admin-Benutzer beim ESC Primary an, und überprüfen Sie den Zustand der Instanz in **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
```

4. Schalten Sie die Instanz über OpenStack ein.

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

nova start cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

5. Warten Sie fünf Minuten, bis die Instanz hochgefahren ist, und gehen Sie zum **AKTIVEN** Status.

```
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 |
```

6. Aktivieren Sie VM Monitor im ESC, nachdem sich die Instanz im **AKTIVEN** Zustand befindet.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR cm_0_170d9c14-0221-4609-
87e3-d752e636f57f
```

Weitere Informationen zum Wiederherstellen von Instanzkonfigurationen finden Sie in den hier bereitgestellten **gerätespezifischen** Prozeduren.

Stellen Sie alle Instanzen aus dem FEHLERzustand wieder her.

Die folgende Prozedur kann verwendet werden, wenn der Zustand der CPS-Instanz in OpenStack FEHLER ist:

1. Überprüfen Sie den Zustand einer Instanz in OpenStack.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f| destackovs-
compute-2Â  | ERROR|
```

2. Überprüfen Sie, ob Compute verfügbar ist und fehlerfrei ausgeführt wird.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep cm
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | cm_0_170d9c14-0221-4609-87e3-d752e636f57f| destackovs-
compute-2  | ERROR|
```

3. Melden Sie sich als Administrator beim ESC Primary an, und überprüfen Sie den Zustand einer Instanz in **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
```

4. Setzen Sie den Zustand der Instanz zurück, um die Instanz auf einen **AKTIVEN** Zustand anstelle eines Fehlerzustands zurückzusetzen. Starten Sie anschließend die Instanz neu.

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

nova reset-state –active cm_0_170d9c14-0221-4609-87e3-d752e636f57f
nova reboot –-hard  cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

5. Warten Sie fünf Minuten, bis die Instanz hochgefahren ist, und gehen Sie in den **AKTIVEN** Zustand.

```
source /home/stack/destackovsrc-Pcrf
nova list â€“fields name,status | grep cm
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 |cm_0_170d9c14-0221-4609-87e3-d752e636f57f| ACTIVE |
```

6. Wenn Cluster Manager den Status nach dem Neustart in **ACTIVE** ändert, aktivieren Sie VM Monitor in ESC.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR
cm_0_170d9c14-0221-4609-87e3-d752e636f57f
```

7. Wenn nach der Wiederherstellung der Status "RUNNING/ACTIVE" aktiviert ist, verweisen Sie auf eine instanzenspezifische Prozedur, um die Konfiguration/Daten aus der Sicherung wiederherzustellen.