PCRF-Ersatz für Compute-Server UCS C240 M4

Inhalt

Einführung

Dieses Dokument beschreibt die erforderlichen Schritte zum Ersetzen eines fehlerhaften Computing-Servers in einer Ultra-M-Konfiguration, die Cisco Policy Suite (CPS) Virtual Network Functions (VNFs) hostet.

Hintergrundinformationen

Dieses Dokument richtet sich an Mitarbeiter von Cisco, die mit der Cisco Ultra-M-Plattform vertraut sind. Es enthält eine Beschreibung der Schritte, die auf der Ebene von OpenStack und CPS VNF zum Zeitpunkt des Ersatzes des Compute-Servers ausgeführt werden müssen.

Hinweis: Ultra M 5.1.x wird zur Definition der Verfahren in diesem Dokument berücksichtigt.

Gesundheitskontrolle

Bevor Sie einen Compute-Knoten austauschen, ist es wichtig, den aktuellen Status Ihrer Red Hat OpenStack Platform-Umgebung zu überprüfen. Es wird empfohlen, den aktuellen Zustand zu überprüfen, um Komplikationen zu vermeiden, wenn der Computing-Ersetzungsprozess eingeschaltet ist.

Schritt 1: Von OpenStack Deployment (OSPD).

```
[root@director ~]$ su - stack
[stack@director ~]$ cd ansible
[stack@director ansible]$ ansible-playbook -i inventory-new openstack_verify.yml  -e
platform=pcrf
```

Schritt 2: Überprüfen Sie anhand des alle fünfzehn Minuten generierten Berichts über die Ultramedizin den Zustand des Systems.

```
[stack@director ~]# cd /var/log/cisco/ultram-health
```

Schritt 3: Aktivieren Sie die Datei **ultram_health_os.report**. Die einzigen Dienste, die als **XXX** Status angezeigt werden sollen**, sind Neutron-sriov-nic-agent.service**.

Schritt 4: Um zu überprüfen, ob Rabbitmq für alle Controller ausgeführt von OSPD.

```
[stack@director ~]# for i in $(nova list| grep controller | awk '{print $12}'| sed
's/ctlplane=//g') ; do (ssh -o StrictHostKeyChecking=no heat-admin@$i "hostname;sudo rabbitmqctl
eval 'rabbit_diagnostics:maybe_stuck().'" ) & done
```

Schritt 5: Überprüfen Sie, ob Stonit aktiviert ist.

```
[stack@director ~]# sudo pcs property show stonith-enabled
```

Schritt 6: Bei allen Controllern wird der PCS-Status überprüft.

- Alle Controller-Knoten werden unter dem Proxy-Klon **gestartet**.
- Alle Controller-Knoten sind unter galera **aktiv**.
- Alle Controller-Knoten werden unter Rabbitmq **gestartet**.
- 1 Controller-Knoten ist **aktiv** und 2 **Standby-Knoten** unter Umleitung.

Schritt 7: Aus OSPD.

```
[stack@director ~]$ for i in $(nova list| grep controller | awk '{print $12}'| sed
's/ctlplane=//g') ; do (ssh -o StrictHostKeyChecking=no heat-admin@$i "hostname;sudo pcs status"
) ;done
```

Schritt 8: Überprüfen Sie, ob alle OpenStack-Services aktiv sind. Führen Sie diesen Befehl vom

OSPD aus.

```
[stack@director ~]# sudo systemctl list-units "openstack*" "neutron*" "openvswitch*"
```

Schritt 9: Überprüfen Sie, ob der CEPH-Status für Controller HEALTH_OK lautet.

```
[stack@director ~]# for i in $(nova list| grep controller | awk '{print $12}'| sed
's/ctlplane=//g') ; do (ssh -o StrictHostKeyChecking=no heat-admin@$i "hostname;sudo ceph -s" )
;done
```

Schritt 10: Überprüfen Sie die Protokolle der OpenStack-Komponente. Suchen Sie nach einem Fehler:

```
Neutron:
[stack@director ~]# sudo tail -n 20 /var/log/neutron/{dhcp-agent,l3-agent,metadata-
agent,openvswitch-agent,server}.log

Cinder:
[stack@director ~]# sudo tail -n 20 /var/log/cinder/{api,scheduler,volume}.log

Glance:
[stack@director ~]# sudo tail -n 20 /var/log/glance/{api,registry}.log
```

Schritt 11: Führen Sie vom OSPD diese Überprüfungen für API durch.

```
[stack@director ~]$ source
```

```
[stack@director ~]$ nova list

[stack@director ~]$ glance image-list

[stack@director ~]$ cinder list

[stack@director ~]$ neutron net-list
```

Schritt 12: Überprüfen Sie den Zustand der Services.

```
Every service status should be “up”:
[stack@director ~]$ nova service-list

Every service status should be “ :-)”:
[stack@director ~]$ neutron agent-list

Every service status should be “up”:
[stack@director ~]$ cinder service-list
```

Sicherung

Im Falle einer Wiederherstellung empfiehlt Cisco, eine Sicherung der OSPD-Datenbank mithilfe der folgenden Schritte durchzuführen:

```
[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
```

Dieser Prozess stellt sicher, dass ein Knoten ausgetauscht werden kann, ohne dass die Verfügbarkeit von Instanzen beeinträchtigt wird. Außerdem wird empfohlen, die CPS-Konfiguration zu sichern.

So sichern Sie CPS VMs von Cluster Manager VM:

```
[root@CM ~]# config_br.py -a export --all /mnt/backup/CPS_backup_$(date +\%Y-\%m-\%d).tar.gz

or

[root@CM ~]# config_br.py -a export --mongo-all --svn --etc --grafanadb --auth-htpasswd --
haproxy /mnt/backup/$(hostname)_backup_all_$(date +\%Y-\%m-\%d).tar.gz
```

Identifizieren der im Compute-Knoten gehosteten VMs

Identifizieren Sie die VMs, die auf dem Computing-Server gehostet werden:

```
[stack@director ~]$ nova list --field name,host,networks | grep compute-10
| 49ac5f22-469e-4b84-badc-031083db0533 |  VNF2-DEPLOYM_s9_0_8bc6cc60-15d6-4ead-8b6a-
10e75d0e134d     |  pod1-compute-10.localdomain    | Replication=10.160.137.161;
Internal=192.168.1.131; Management=10.225.247.229; tb1-orch=172.16.180.129
```

> **Hinweis:** In der hier gezeigten Ausgabe entspricht die erste Spalte dem Universally Unique Identifier (UUID), die zweite Spalte dem VM-Namen und die dritte Spalte dem Hostnamen, in dem das virtuelle System vorhanden ist. Die Parameter aus dieser Ausgabe werden in nachfolgenden Abschnitten verwendet.

Deaktivieren Sie das Herunterfahren der PCRF-Services für das virtuelle System.

Schritt 1: Melden Sie sich bei der Management-IP des virtuellen Systems an:

```
[stack@XX-ospd ~]$ ssh root@
```

```
[root@XXXSM03 ~]# monit stop all
```

Schritt 2: Wenn es sich bei dem virtuellen System um ein SM, ein OAM oder einen Schiedsrichter handelt, beenden Sie darüber hinaus die Dienste von sessionmgr:

```
[root@XXXSM03 ~]# cd /etc/init.d
[root@XXXSM03 init.d]# ls -l sessionmgr*
-rwxr-xr-x 1 root root 4544 Nov 29 23:47 sessionmgr-27717
-rwxr-xr-x 1 root root 4399 Nov 28 22:45 sessionmgr-27721
-rwxr-xr-x 1 root root 4544 Nov 29 23:47 sessionmgr-27727
```

Schritt 3: Führen Sie für jede Datei mit dem Titel sessionmgr-xxxxx den Dienst sessionmgr-

xxxxxxx stop aus:

```
[root@XXXSM03 init.d]# service sessionmgr-27717 stop
```

Entfernen des Computing-Knotens aus der Nova Aggregate-Liste

Schritt 1: Listen Sie die nova-Aggregate auf, und identifizieren Sie die Aggregate, die dem von ihm gehosteten VNF-Server entsprechen. In der Regel hat das Format <VNFNAME>-SERVICE<X>:

```
[stack@director ~]$ nova aggregate-list
+----+------------------+-------------------+
| Id | Name             | Availability Zone |
+----+------------------+-------------------+
| 29 | POD1-AUTOIT   | mgmt              |
| 57 | VNF1-SERVICE1 | -                 |
| 60 | VNF1-EM-MGMT1 | -                 |
| 63 | VNF1-CF-MGMT1 | -                 |
| 66 | VNF2-CF-MGMT2 | -                 |
| 69 | VNF2-EM-MGMT2 | -                 |
| 72 | VNF2-SERVICE2 | -                 |
| 75 | VNF3-CF-MGMT3 | -                 |
| 78 | VNF3-EM-MGMT3 | -                 |
| 81 | VNF3-SERVICE3 | -                 |
+----+------------------+-------------------+
```

In diesem Fall gehört der zu ersetzende Computing-Server zu VNF2. Daher ist die entsprechende aggregierte Liste VNF2-SERVICE2.

Schritt 2: Entfernen Sie den Computing-Knoten aus der angegebenen Aggregation (entfernen Sie ihn durch den Hostnamen, der im Abschnitt **Identifizieren Sie die im Compute Node gehosteten VMs angegeben ist ��**

nova aggregate-remove-host

```
[stack@director ~]$ nova aggregate-remove-host VNF2-SERVICE2 pod1-compute-10.localdomain
```

Schritt 3: Überprüfen Sie, ob der Computing-Knoten aus den Aggregaten entfernt wird. Nun darf der Host nicht unter der Aggregatzuordnung aufgeführt werden:

nova aggregate-show

```
[stack@director ~]$ nova aggregate-show VNF2-SERVICE2
```

Löschen von Computing-Knoten

Die in diesem Abschnitt beschriebenen Schritte sind unabhängig von den im Computing-Knoten gehosteten VMs häufig.

Löschen aus der Overcloud

Schritt 1: Erstellen Sie eine Skriptdatei mit dem Namen **delete_node.sh**, die wie hier gezeigt den Inhalt enthält. Stellen Sie sicher, dass die erwähnten Vorlagen mit den Vorlagen übereinstimmen, die im **deploy.sh-**Skript für die Stackbereitstellung verwendet wurden.

delete_node.sh

```
openstack overcloud node delete --templates -e /usr/share/openstack-tripleo-heat-
templates/environments/puppet-pacemaker.yaml -e /usr/share/openstack-tripleo-heat-
templates/environments/network-isolation.yaml -e /usr/share/openstack-tripleo-heat-
templates/environments/storage-environment.yaml -e /usr/share/openstack-tripleo-heat-
templates/environments/neutron-sriov.yaml -e /home/stack/custom-templates/network.yaml -e
/home/stack/custom-templates/ceph.yaml -e /home/stack/custom-templates/compute.yaml -e
/home/stack/custom-templates/layout.yaml -e /home/stack/custom-templates/layout.yaml --stack
```

```
[stack@director ~]$ source stackrc
[stack@director ~]$ /bin/sh delete_node.sh
+ openstack overcloud node delete --templates -e /usr/share/openstack-tripleo-heat-
templates/environments/puppet-pacemaker.yaml -e /usr/share/openstack-tripleo-heat-
templates/environments/network-isolation.yaml -e /usr/share/openstack-tripleo-heat-
templates/environments/storage-environment.yaml -e /usr/share/openstack-tripleo-heat-
templates/environments/neutron-sriov.yaml -e /home/stack/custom-templates/network.yaml -e
/home/stack/custom-templates/ceph.yaml -e /home/stack/custom-templates/compute.yaml -e
/home/stack/custom-templates/layout.yaml -e /home/stack/custom-templates/layout.yaml --stack
pod1 49ac5f22-469e-4b84-badc-031083db0533
Deleting the following nodes from stack pod1:
- 49ac5f22-469e-4b84-badc-031083db0533
Started Mistral Workflow. Execution ID: 4ab4508a-c1d5-4e48-9b95-ad9a5baa20ae

real   0m52.078s
user   0m0.383s
sys    0m0.086s
```

Schritt 2: Warten Sie, bis der OpenStack-Stapelvorgang in den VOLLSTÄNDIGEN Zustand wechselt.

```
[stack@director ~]$  openstack stack list
+--------------------------------------+------------+----------------+----------------------+--
--------------------+
| ID                                   | Stack Name | Stack Status    | Creation Time        |
Updated Time         |
+--------------------------------------+------------+----------------+----------------------+--
--------------------+
| 5df68458-095d-43bd-a8c4-033e68ba79a0 | pod1 | UPDATE_COMPLETE | 2018-05-08T21:30:06Z | 2018-
05-08T20:42:48Z |
```

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

Computing-Knoten aus der Dienstliste löschen

Löschen Sie den Computing-Service aus der Dienstliste:

```
[stack@director ~]$ source corerc
[stack@director ~]$ openstack compute service list | grep compute-8
| 404 | nova-compute     | pod1-compute-8.localdomain     | nova     | enabled | up    | 2018-
05-08T18:40:56.000000 |

openstack compute service delete
```

```
[stack@director ~]$ openstack compute service delete 404
```

Neutrale Agenten löschen

Löschen Sie den alten zugeordneten Neutron-Agent und den offenen Switch-Agent für den Computing-Server:

```
[stack@director ~]$ openstack network agent list | grep compute-8
| c3ee92ba-aa23-480c-ac81-d3d8d01dcc03 | Open vSwitch agent | pod1-compute-8.localdomain     |
None              | False  | UP    | neutron-openvswitch-agent |
| ec19cb01-abbb-4773-8397-8739d9b0a349 | NIC Switch agent   | pod1-compute-8.localdomain     |
None              | False  | UP    | neutron-sriov-nic-agent   |

openstack network agent delete
```

```
[stack@director ~]$ openstack network agent delete c3ee92ba-aa23-480c-ac81-d3d8d01dcc03
[stack@director ~]$ openstack network agent delete ec19cb01-abbb-4773-8397-8739d9b0a349
```

Aus der Ironischen Datenbank löschen

Löschen Sie einen Knoten aus der IronBar-Datenbank, und überprüfen Sie ihn.

```
[stack@director ~]$ source stackrc

nova show
```

```
[stack@director ~]$ nova show pod1-compute-10 | grep hypervisor
| OS-EXT-SRV-ATTR:hypervisor_hostname  | 4ab21917-32fa-43a6-9260-02538b5c7a5a

ironic node-delete
```

```
[stack@director ~]$ ironic node-delete 4ab21917-32fa-43a6-9260-02538b5c7a5a
[stack@director ~]$ ironic node-list (node delete must not be listed now)
```

Installation des neuen Computing-Knotens

Die Schritte zur Installation eines neuen UCS C240 M4 Servers sowie die Schritte zur Ersteinrichtung können wie folgt aufgerufen werden: Cisco UCS C240 M4 Serverinstallations- und Serviceleitfaden

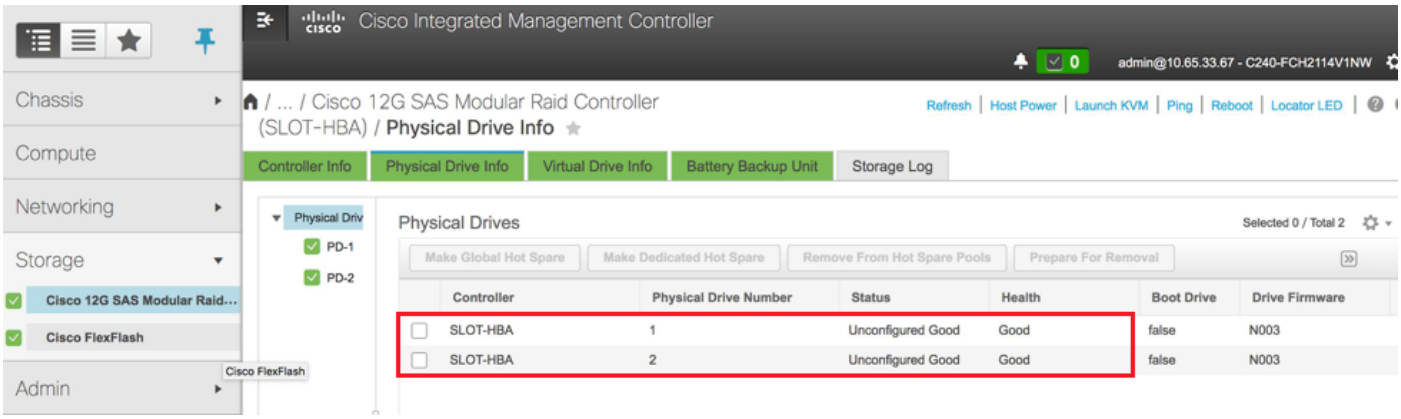
Schritt 1: Nach der Installation des Servers legen Sie die Festplatten in die entsprechenden Steckplätze als alten Server ein.

Schritt 2: Melden Sie sich mit der CIMC IP-Adresse beim Server an.

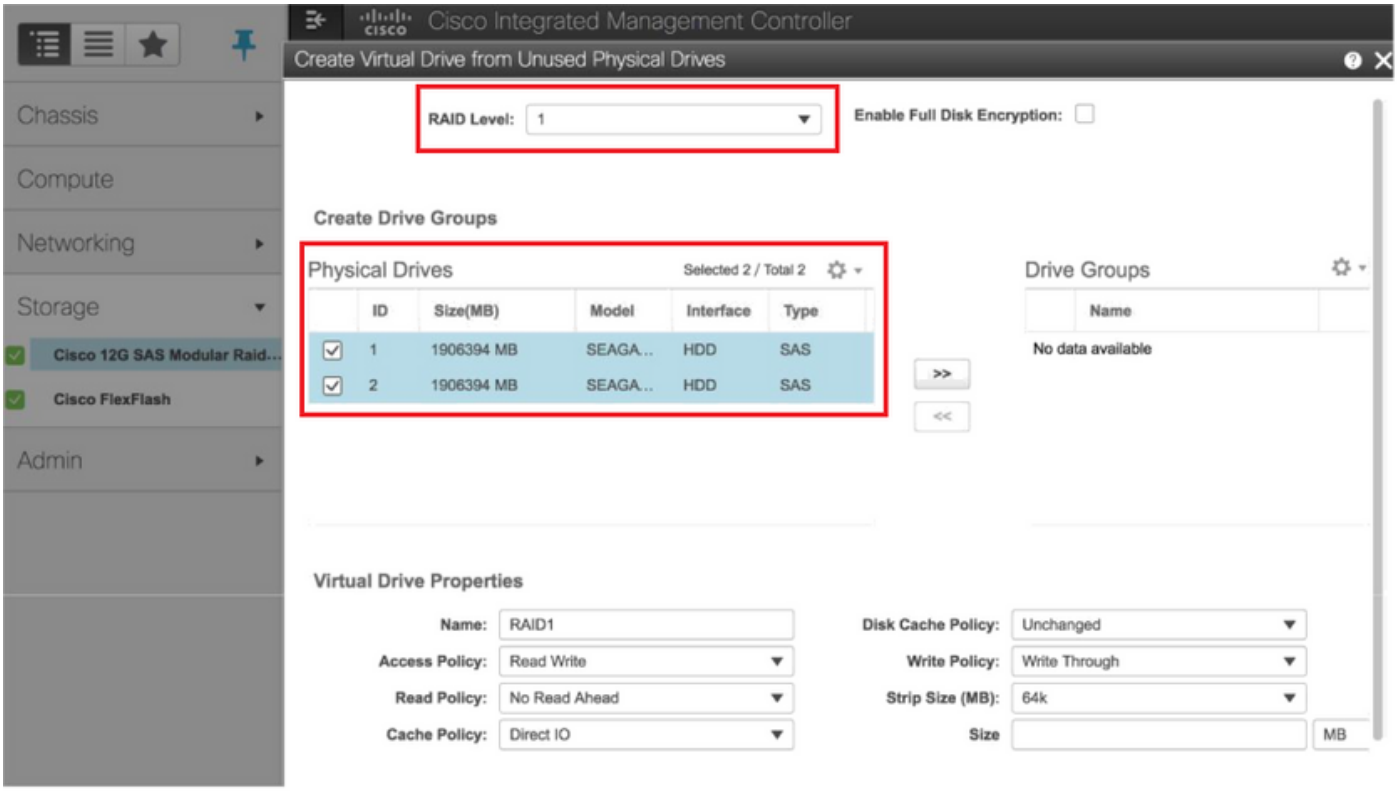
Schritt 3: Führen Sie ein BIOS-Upgrade durch, wenn die Firmware nicht der zuvor verwendeten empfohlenen Version entspricht. Schritte für ein BIOS-Upgrade finden Sie hier: BIOS-Upgrade-Leitfaden für Rackmount-Server der Cisco UCS C-Serie

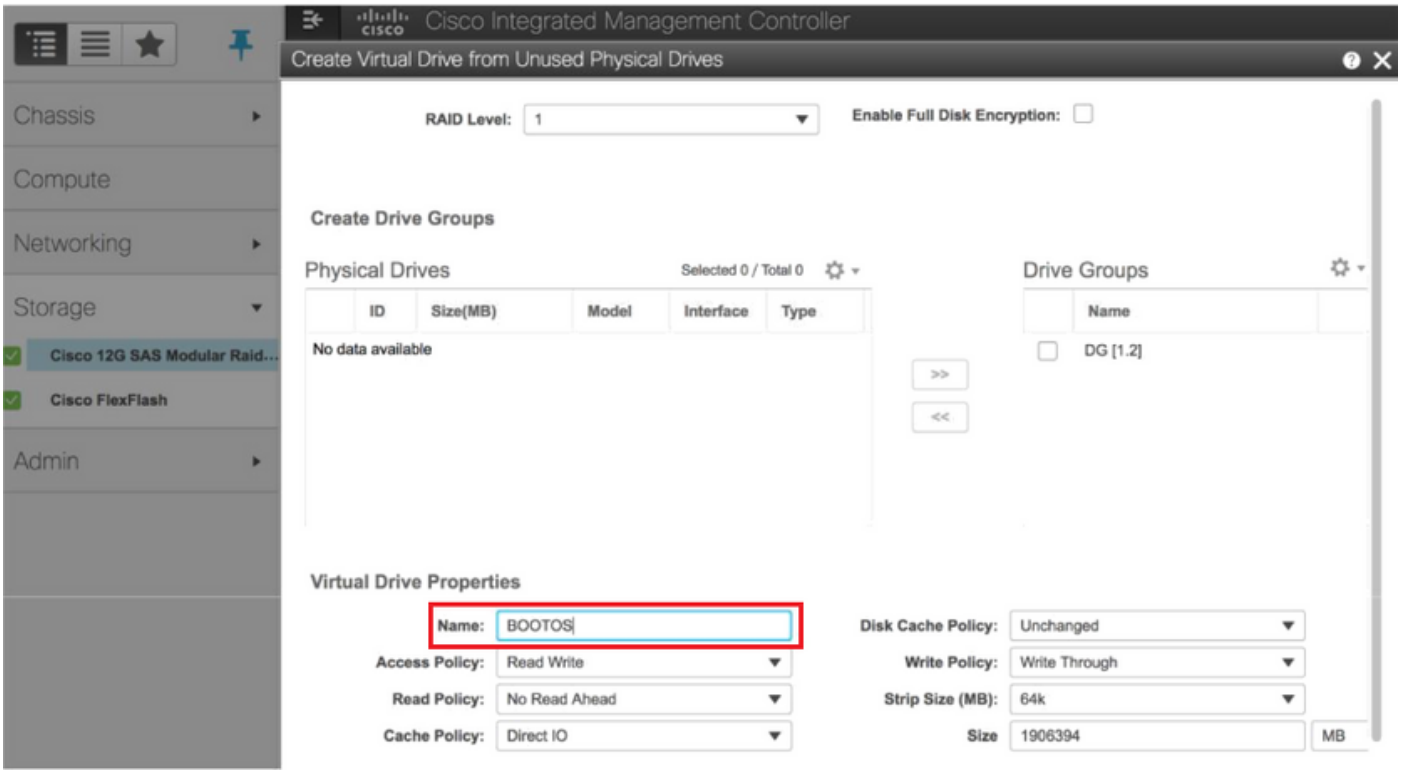
Schritt 4: Um den Status von physischen Laufwerken zu überprüfen, navigieren Sie zu **Storage > Cisco 12G SAS Modular Raid Controller (SLOT-HBA) > Physical Drive Info**. Es muss **nicht konfiguriert** sein**, gut**

Der hier gezeigte Speicher kann ein SSD-Laufwerk sein.

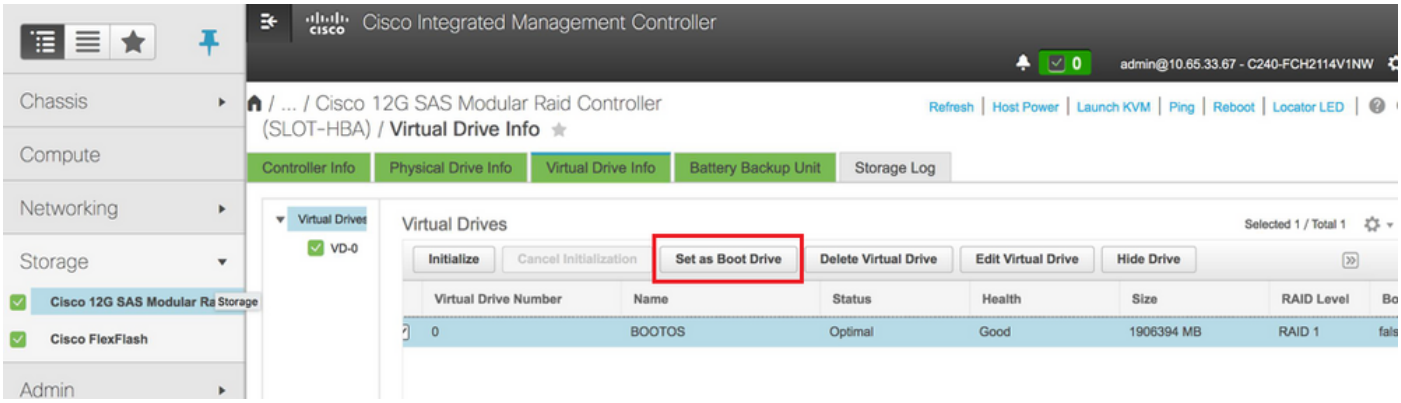


Schritt 5: Um eine virtuelle Festplatte von den physischen Laufwerken mit RAID Level 1 zu erstellen, gehen Sie zu **Storage > Cisco 12G SAS Modular Raid Controller (SLOT-HBA) > Controller Info > Create Virtual Drive from Unused Physical Drives (Virtuelles Laufwerk aus nicht verwendeten physischen Laufwerken erstellen).**

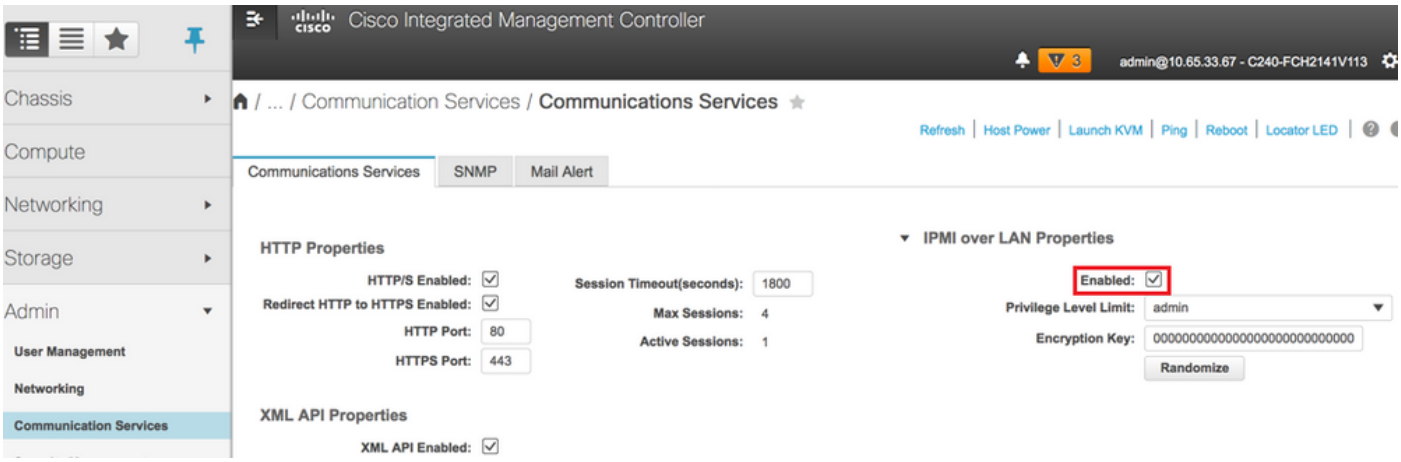




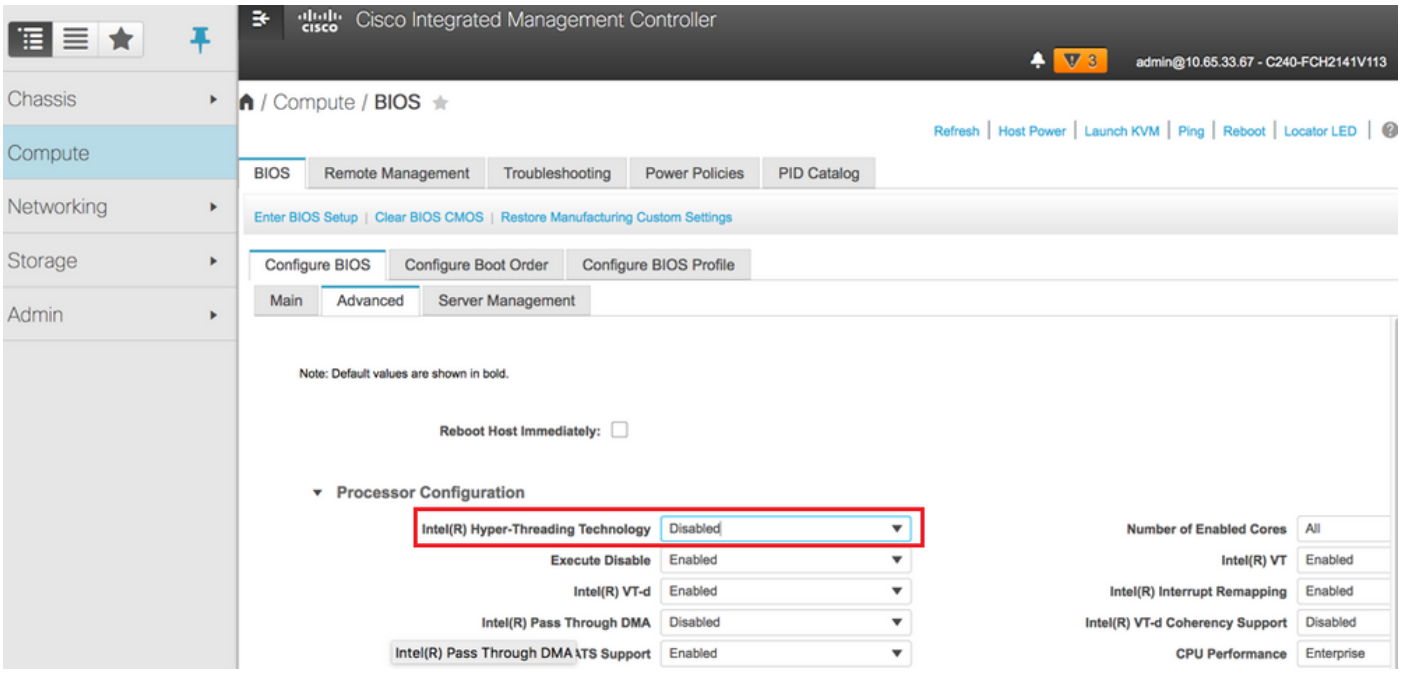
Schritt 6: Wählen Sie die VD aus, und konfigurieren Sie **Set as Boot Drive** (Als Startlaufwerk festlegen), wie im Bild gezeigt.



Schritt 7: Um IPMI über LAN zu aktivieren, navigieren Sie zu **Admin > Communication Services > Communication Services** (**Administrator > Kommunikationsdienste > Kommunikationsdienste**), wie im Bild gezeigt.



Schritt 8: Um Hyperthreading zu deaktivieren, wie im Bild gezeigt, navigieren Sie zu **Compute > BIOS > Configure BIOS > Advanced > Processor Configuration**.



Hinweis: Das hier abgebildete Image und die in diesem Abschnitt beschriebenen Konfigurationsschritte beziehen sich auf die Firmware-Version 3.0(3e). Wenn Sie an anderen Versionen arbeiten, kann es zu geringfügigen Abweichungen kommen.

Hinzufügen des neuen Computing-Knotens zur Overcloud

Die in diesem Abschnitt beschriebenen Schritte sind unabhängig von der vom Computing-Knoten gehosteten VM identisch.

Schritt 1: Hinzufügen eines Compute-Servers mit einem anderen Index

Erstellen Sie eine Datei **add_node.json**, die nur die Details des neuen Computing-Servers enthält, der hinzugefügt werden soll. Stellen Sie sicher, dass die Indexnummer für den neuen Computing-Server nicht zuvor verwendet wurde. Erhöhen Sie in der Regel den nächsthöchsten Rechenwert.

Beispiel: Die höchste vorherige Version wurde deshalb für Computing-17 erstellt. Daher wurde Compute-18 für das 2-VNF-System erstellt.

Hinweis: Achten Sie auf das Json-Format.

```
[stack@director ~]$ cat add_node.json
{
    "nodes":[
        {
            "mac":[
                "

            ],
            "capabilities": "node:compute-18,boot_option:local",
            "cpu":"24",
            "memory":"256000",
            "disk":"3000",
            "arch":"x86_64",
            "pm_type":"pxe_ipmitool",
            "pm_user":"admin",
            "pm_password":"<PASSWORD>",
            "pm_addr":"192.100.0.5"
        }
    ]
}
```

Schritt 2: Importieren Sie die Json-Datei.

```
[stack@director ~]$ openstack baremetal import --json add_node.json
Started Mistral Workflow. Execution ID: 78f3b22c-5c11-4d08-a00f-8553b09f497d
Successfully registered node UUID 7eddfa87-6ae6-4308-b1d2-78c98689a56e
Started Mistral Workflow. Execution ID: 33a68c16-c6fd-4f2a-9df9-926545f2127e
Successfully set all nodes to available.
```

Schritt 3: Führen Sie eine Knotenintrospektion mithilfe der UUID aus, die im vorherigen Schritt angegeben wurde.

```
[stack@director ~]$ openstack baremetal node manage 7eddfa87-6ae6-4308-b1d2-78c98689a56e
[stack@director ~]$ ironic node-list |grep 7eddfa87
| 7eddfa87-6ae6-4308-b1d2-78c98689a56e | None | None                                    | power off
  | manageable         | False       |

[stack@director ~]$ openstack overcloud node introspect 7eddfa87-6ae6-4308-b1d2-78c98689a56e --
provide
Started Mistral Workflow. Execution ID: e320298a-6562-42e3-8ba6-5ce6d8524e5c
Waiting for introspection to finish...
Successfully introspected all nodes.
Introspection completed.
Started Mistral Workflow. Execution ID: c4a90d7b-ebf2-4fcb-96bf-e3168aa69dc9
Successfully set all nodes to available.

[stack@director ~]$ ironic node-list |grep available
| 7eddfa87-6ae6-4308-b1d2-78c98689a56e | None | None                                    | power off
  | available          | False       |
```

Schritt 4: Fügen Sie unter ComputeIPs custom-templates/layout.yml IP-Adressen hinzu. Sie fügen diese Adresse zum Ende der Liste für jeden Typ hinzu, hier als Beispiel Compute-0.

```
ComputeIPs:

    internal_api:

    - 11.120.0.43

    - 11.120.0.44

    - 11.120.0.45

    - 11.120.0.43   <<< take compute-0 .43 and add here

    tenant:

    - 11.117.0.43

    - 11.117.0.44

    - 11.117.0.45

    - 11.117.0.43   << and here

    storage:

    - 11.118.0.43

    - 11.118.0.44

    - 11.118.0.45

    - 11.118.0.43   << and here
```

Schritt 5: Führen Sie deploy.sh-Skript aus, das zuvor für die Bereitstellung des Stacks verwendet wurde, um den neuen Computing-Knoten dem Overcloud-Stack hinzuzufügen.

```
[stack@director ~]$ ./deploy.sh
++ openstack overcloud deploy --templates -r /home/stack/custom-templates/custom-roles.yaml -e
```

```
/usr/share/openstack-tripleo-heat-templates/environments/puppet-pacemaker.yaml -e
/usr/share/openstack-tripleo-heat-templates/environments/network-isolation.yaml -e
/usr/share/openstack-tripleo-heat-templates/environments/storage-environment.yaml -e
/usr/share/openstack-tripleo-heat-templates/environments/neutron-sriov.yaml -e
/home/stack/custom-templates/network.yaml -e /home/stack/custom-templates/ceph.yaml -e
/home/stack/custom-templates/compute.yaml -e /home/stack/custom-templates/layout.yaml --stack
ADN-ultram --debug --log-file overcloudDeploy_11_06_17__16_39_26.log --ntp-server 172.24.167.109
--neutron-flat-networks phys_pcie1_0,phys_pcie1_1,phys_pcie4_0,phys_pcie4_1 --neutron-network-
vlan-ranges datacentre:1001:1050 --neutron-disable-tunneling --verbose --timeout 180
…
Starting new HTTP connection (1): 192.200.0.1
"POST /v2/action_executions HTTP/1.1" 201 1695
HTTP POST http://192.200.0.1:8989/v2/action_executions 201
Overcloud Endpoint: http://10.1.2.5:5000/v2.0
Overcloud Deployed
clean_up DeployOvercloud:
END return value: 0

real    38m38.971s
user    0m3.605s
sys     0m0.466s
```

Schritt 6: Warten Sie, bis der Status des OpenStack-Stacks abgeschlossen ist.

```
[stack@director ~]$ openstack stack list
+--------------------------------------+------------+----------------+----------------------+--
--------------------+
| ID                                   | Stack Name | Stack Status    | Creation Time        |
Updated Time         |
+--------------------------------------+------------+----------------+----------------------+--
--------------------+
| 5df68458-095d-43bd-a8c4-033e68ba79a0 | ADN-ultram | UPDATE_COMPLETE | 2017-11-02T21:30:06Z |
2017-11-06T21:40:58Z |
+--------------------------------------+------------+----------------+----------------------+--
--------------------+
```

Schritt 7: Überprüfen Sie, ob sich der neue Rechenknoten im aktiven Zustand befindet.

```
[stack@director ~]$ source stackrc
[stack@director ~]$ nova list |grep compute-18
| 0f2d88cd-d2b9-4f28-b2ca-13e305ad49ea | pod1-compute-18    | ACTIVE | -          | Running
| ctlplane=192.200.0.117 |

[stack@director ~]$ source corerc
[stack@director ~]$ openstack hypervisor list |grep compute-18
| 63 | pod1-compute-18.localdomain    |
```

Stellen Sie die VMs wieder her

Hinzufügen zur Nova Aggregate-Liste

Fügen Sie den Computing-Knoten dem Aggregat-Host hinzu, und überprüfen Sie, ob der Host hinzugefügt wurde.

```
nova aggregate-add-host
```

```
[stack@director ~]$ nova aggregate-add-host VNF2-SERVICE2 pod1-compute-18.localdomain
```

```
nova aggregate-show
```

```
[stack@director ~]$ nova aggregate-show VNF2-SERVICE2
```

VM-Wiederherstellung vom Elastic Services Controller (ESC)

Schritt 1: Die VM befindet sich in der Nova-Liste im Fehlerstatus.

```
[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     |
```

Schritt 2: Stellen Sie das virtuelle System vom ESC wieder her.

```
[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
```

Schritt 3: Überwachen Sie 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].
```

Überprüfen Sie die Cisco Policy and Charging Rules Function (PCRF) Services, die sich auf VM befinden.

> **Hinweis:** Wenn sich das virtuelle System im "Shutoff"-Zustand befindet, schalten Sie es mithilfe von **esc_nc_cli** vom ESC ein.

Überprüfen Sie die **diagnostics.sh-Datei** von Cluster Manager VM, und ob ein Fehler für die wiederhergestellten VMs gefunden wurde.

Schritt 1: Melden Sie sich bei der entsprechenden VM an.

```
[stack@XX-ospd ~]$ ssh root@
```

```
[root@XXXSM03 ~]# monit start all
```

Schritt 2: Wenn das **virtuelle System** ein **SM**, **OAM** oder **Arbiter** ist, starten Sie zusätzlich die Dienste von sessionmgr, die zuvor gestoppt wurden:

Führen Sie für jede Datei mit dem Titel sessionmgr-xxxxx den Service sessionmgr-xxxxxxx start aus:

```
[root@XXXSM03 init.d]# service sessionmgr-27717 start
```

Wenn die Diagnose weiterhin nicht klar ist, führen Sie **build_all.sh** von Cluster Manager VM aus und führen Sie dann VM-init auf dem jeweiligen VM aus.

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

ssh VM   e.g. ssh pcrfclient01
/etc/init.d/vm-init
```

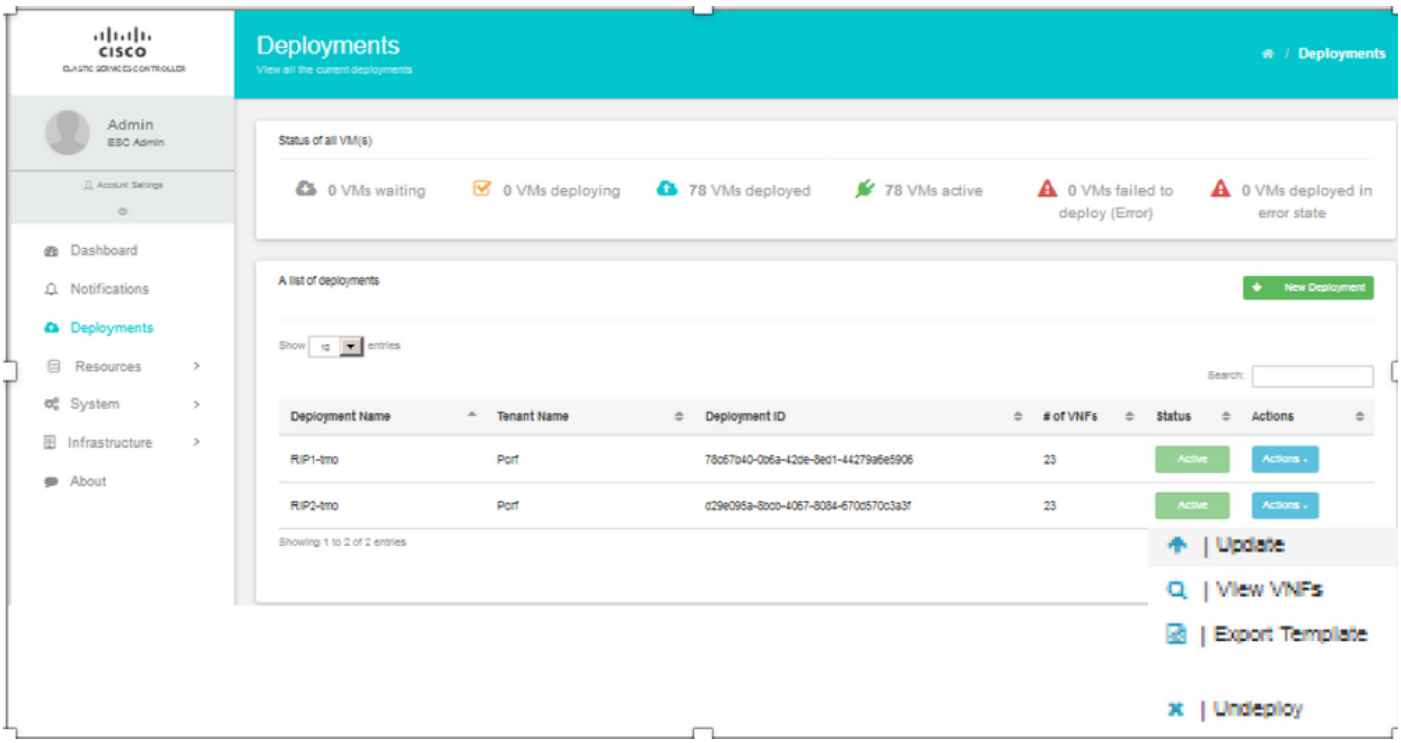
Löschen und erneutes Bereitstellen einer oder mehrerer VMs für den Fall, dass die ESC-Wiederherstellung fehlschlägt

Wenn der ESC-Wiederherstellungsbefehl (oben) nicht funktioniert (VM_RECOVERY_FAILED), löschen und lesen Sie die einzelnen VMs.

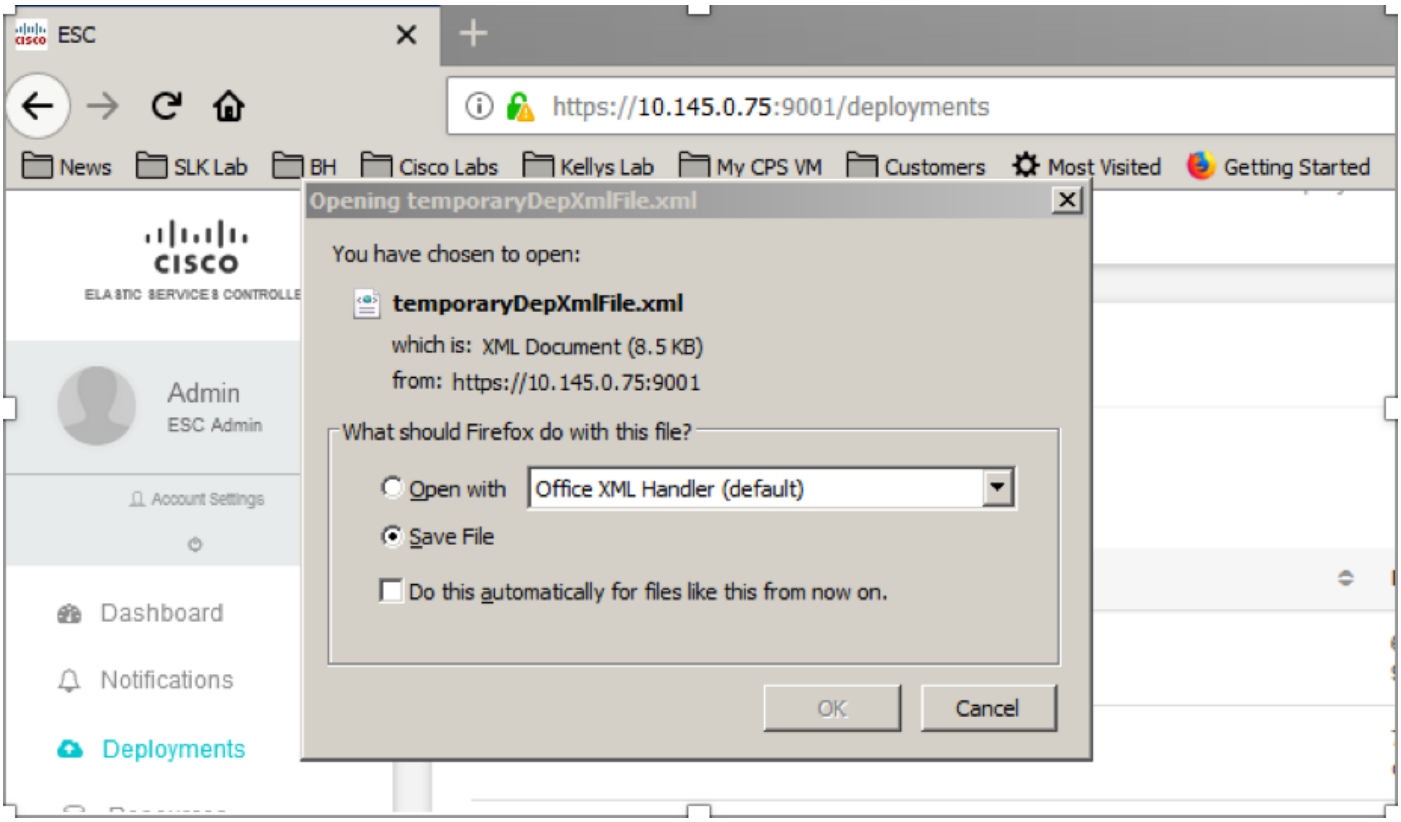
Rufen Sie die neueste ESC-Vorlage für die Site ab.

Von ESC Portal:

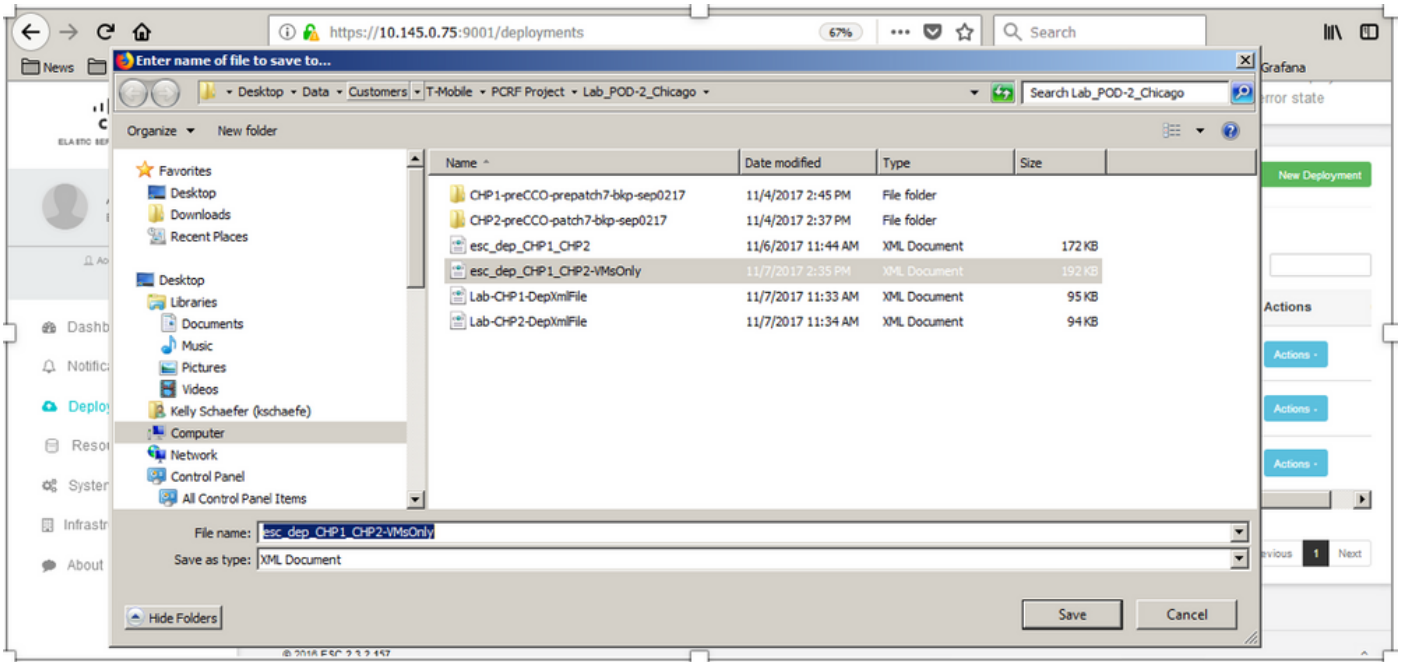
Schritt 1: Platzieren Sie den Cursor über die blaue **Action-**Schaltfläche, ein Popup-Fenster wird geöffnet, und klicken Sie jetzt auf **Vorlage exportieren**, wie im Bild gezeigt.



Schritt 2: Es wird eine Option zum Herunterladen der Vorlage auf den lokalen Computer angezeigt. Aktivieren Sie **Datei speichern**, wie im Bild gezeigt.



Schritt 3: Wählen Sie, wie im Bild gezeigt, einen Speicherort aus, und speichern Sie die Datei zur späteren Verwendung.



Schritt 4: Melden Sie sich beim Active ESC an, damit die Site gelöscht werden kann, und kopieren Sie die oben gespeicherte Datei in diesem Verzeichnis im ESC.

```
/opt/cisco/esc/cisco-cps/config/gr/tmo/gen
```

Schritt 5: Verzeichnis in **/opt/cisco/esc/cisco-cps/config/gr/tmo/gen** ändern:

```
cd /opt/cisco/esc/cisco-cps/config/gr/tmo/gen
```

Verfahren zum Ändern der Datei

Schritt 1: Ändern Sie die Exportvorlagendatei.

In diesem Schritt ändern Sie die Exportvorlagendatei, um die Gruppe(n) der virtuellen Systeme zu löschen, die den wiederherzustellenden virtuellen Systemen zugeordnet sind.

Die Exportvorlagendatei gilt für ein bestimmtes Cluster.

Innerhalb dieses Clusters sind mehrere vm_groups. Für jeden VM-Typ gibt es eine oder mehrere vm_groups (PD, PS, SM, OM).

> **Hinweis:** Einige VM_Groups haben mehr als eine VM. Alle VMs in dieser Gruppe werden gelöscht und neu hinzugefügt.

In dieser Bereitstellung müssen Sie eine oder mehrere der vm_groups zum Löschen markieren.

Beispiel:

```
<vm_group>
  <name>cm</name>
```

Ändern Sie <vm_group>jetzt <vm_group **nc:operation="delete"**>, und speichern Sie die

Änderungen.

Schritt 2: Führen Sie die geänderte Exportvorlagendatei aus.

Aus dem ESC-Ausführen:

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

Im ESC-Portal sollten Sie eine oder mehrere VMs sehen können, die in den **nicht implementierten** Zustand verschoben und dann vollständig verschwunden sind.

Fortschritt kann im WSA unter folgender Adresse nachverfolgt werden: **/var/log/esc/yangesc.log**

Beispiel:

```
09:09:12,608 29-Jan-2018 INFO  ===== UPDATE SERVICE REQUEST RECEIVED(UNDER TENANT) =====
09:09:12,608 29-Jan-2018 INFO  Tenant name: Pcrf
09:09:12,609 29-Jan-2018 INFO  Deployment name: WSP1-tmo
09:09:29,794 29-Jan-2018 INFO
09:09:29,794 29-Jan-2018 INFO  ===== CONFD TRANSACTION ACCEPTED  =====
09:10:19,459 29-Jan-2018 INFO
09:10:19,459 29-Jan-2018 INFO  ===== SEND NOTIFICATION STARTS =====
09:10:19,459 29-Jan-2018 INFO  Type: VM_UNDEPLOYED
09:10:19,459 29-Jan-2018 INFO  Status: SUCCESS
09:10:19,459 29-Jan-2018 INFO  Status Code: 200
|
|
|
09:10:22,292 29-Jan-2018 INFO  ===== SEND NOTIFICATION STARTS =====
09:10:22,292 29-Jan-2018 INFO  Type: SERVICE_UPDATED
09:10:22,292 29-Jan-2018 INFO  Status: SUCCESS
09:10:22,292 29-Jan-2018 INFO  Status Code: 200
```

Schritt 3: Ändern Sie die Exportvorlagendatei, um die VMs hinzuzufügen.

In diesem Schritt ändern Sie die Exportvorlagendatei, um die Gruppe(n) der virtuellen Systeme, die wiederhergestellt werden, erneut hinzuzufügen.

Die Exportvorlagendatei ist in die beiden Bereitstellungen (Cluster1/Cluster2) aufgeteilt.

Innerhalb jedes Clusters befindet sich eine vm_group. Für jeden VM-Typ gibt es eine oder mehrere vm_groups (PD, PS, SM, OM).

> **Hinweis:** Einige VM_Groups haben mehr als eine VM. Alle VMs in dieser Gruppe werden neu hinzugefügt.

Beispiel:

```
<vm_group nc:operation="delete">
```

<name>cm</name>

Ändern Sie die **<vm_group nc:operation="delete">** in just **<vm_group>**.

> **Hinweis:** Wenn die VMs neu erstellt werden müssen, weil der Host ersetzt wurde, hat sich möglicherweise der Hostname des Hosts geändert. Wenn der Hostname des HOST geändert wurde, muss der Hostname im **Platzierungsabschnitt** der **vm_group** aktualisiert werden.

<Platzierung>

<type>zone_host</type>

<Enforcement>strict</Enforcement>

<host>**wsstackovs-compute-4.localdomain**</host>

</placement>

Aktualisieren Sie den im vorherigen Abschnitt gezeigten Hostnamen auf den neuen Hostnamen, wie er vom Ultra-M-Team vor der Ausführung dieses MOP bereitgestellt wurde. Speichern Sie die Änderungen nach der Installation des neuen Hosts.

Schritt 4: Führen Sie die geänderte Exportvorlagendatei aus.

Aus dem ESC-Ausführen:

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

Im ESC-Portal sollten Sie sehen können, dass eine oder mehrere VMs wieder angezeigt werden, und dann in den Active-Status wechseln.

Fortschritt kann im WSA unter folgender Adresse nachverfolgt werden: **/var/log/esc/yangesc.log**

Beispiel:

```
09:14:00,906 29-Jan-2018 INFO  ===== UPDATE SERVICE REQUESTRECEIVED (UNDER TENANT) =====
09:14:00,906 29-Jan-2018 INFO  Tenant name: Pcrf
09:14:00,906 29-Jan-2018 INFO  Deployment name: WSP1-tmo
09:14:01,542 29-Jan-2018 INFO
09:14:01,542 29-Jan-2018 INFO  ===== CONFD TRANSACTION ACCEPTED  =====
09:16:33,947 29-Jan-2018 INFO
09:16:33,947 29-Jan-2018 INFO  ===== SEND NOTIFICATION STARTS =====
09:16:33,947 29-Jan-2018 INFO  Type: VM_DEPLOYED
09:16:33,947 29-Jan-2018 INFO  Status: SUCCESS
09:16:33,947 29-Jan-2018 INFO  Status Code: 200
|
```

```
|
|
09:19:00,148 29-Jan-2018 INFO  ===== SEND NOTIFICATION STARTS =====
09:19:00,148 29-Jan-2018 INFO  Type: VM_ALIVE
09:19:00,148 29-Jan-2018 INFO  Status: SUCCESS
09:19:00,148 29-Jan-2018 INFO  Status Code: 200
|
|
|
09:19:00,275 29-Jan-2018 INFO  ===== SEND NOTIFICATION STARTS =====
09:19:00,275 29-Jan-2018 INFO  Type: SERVICE_UPDATED
09:19:00,275 29-Jan-2018 INFO  Status: SUCCESS
09:19:00,275 29-Jan-2018 INFO  Status Code: 200
```

Schritt 5: Überprüfen Sie die PCRF-Services, die sich auf dem VM befinden.

Überprüfen Sie, ob die PCRF-Dienste deaktiviert sind, und starten Sie sie.

```
[stack@XX-ospd ~]$ ssh root@
```

```
[root@XXXSM03 ~]# monsum
[root@XXXSM03 ~]# monit start all
```

Wenn das **VM** ein **SM**, **OAM** oder **Arbiter** ist, starten Sie zusätzlich die Dienste von sessionmgr, die zuvor gestoppt wurden:

Für jede Datei mit dem Titel sessionmgr-xxxxx führen Sie den Dienst sessionmgr-xxxxxxx aus:

```
[root@XXXSM03 init.d]# service sessionmgr-27717 start
```

Wenn die Diagnose immer noch nicht geklärt ist, führen Sie **build_all.sh** von Cluster Manager VM aus und führen Sie dann VM-init auf der entsprechenden VM aus.

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

ssh VM e.g. ssh pcrfclient01
/etc/init.d/vm-init
```

Schritt 6: Führen Sie die Diagnose aus, um den Systemstatus zu überprüfen.

```
[root@XXXSM03 init.d]# diagnostics.sh
```

Zugehörige Informationen

- https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/10/html/director_installati..
- https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/10/html/director_installati..
- Technischer Support und Dokumentation für Cisco Systeme