Ersatz von Compute-Server UCS C240 M4 - CPAR

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte, die erforderlich sind, um einen fehlerhaften Computing-Server in einer Ultra-M-Konfiguration zu ersetzen.

Dieses Verfahren gilt für eine OpenStack-Umgebung mit NEWTON-Version, in der der Elastic Serives Controller (ESC) Cisco Prime Access Registrar (CPAR) nicht verwaltet und CPAR direkt auf dem auf OpenStack bereitgestellten virtuellen System installiert wird.

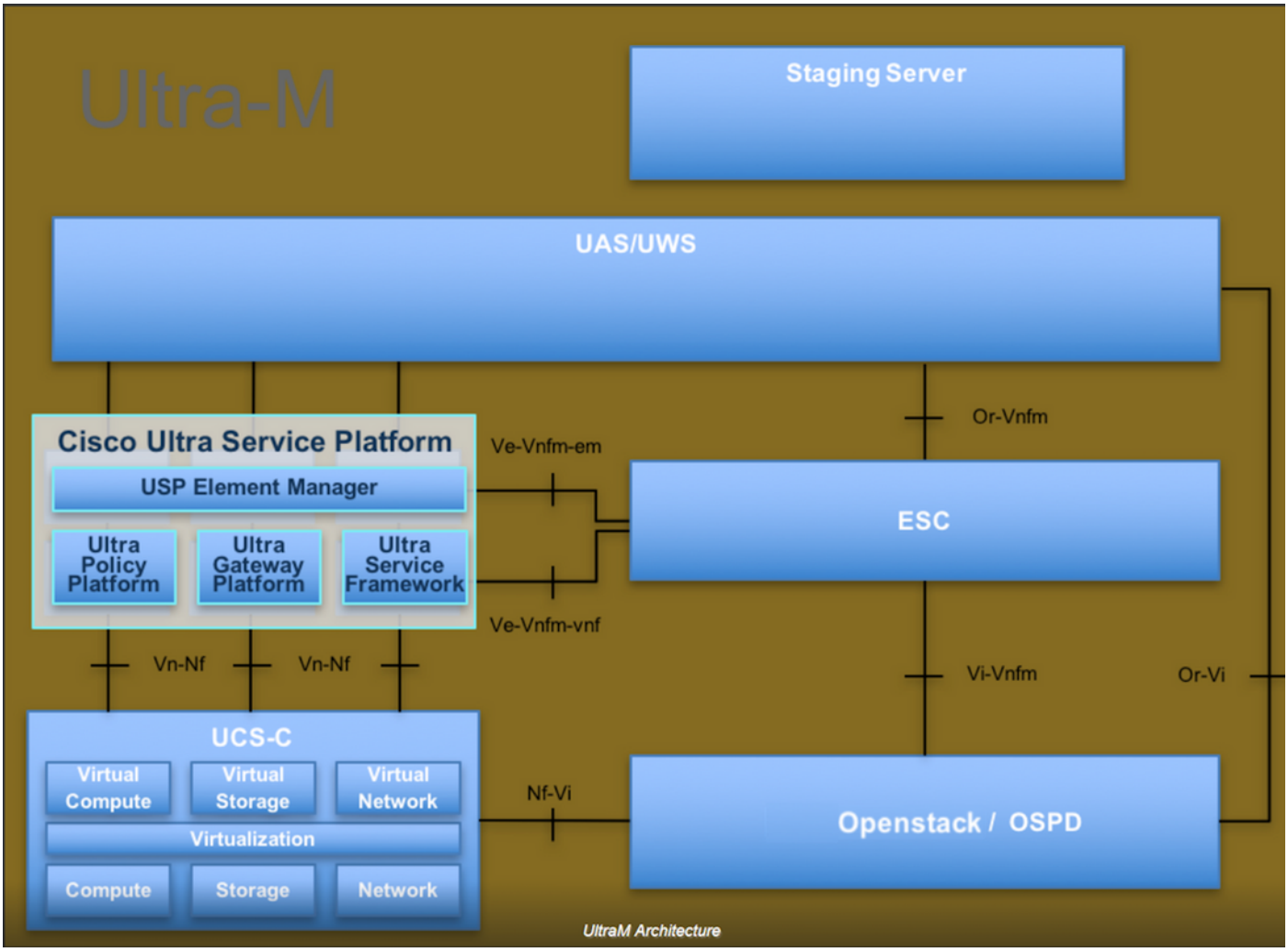
Hintergrundinformationen

Ultra-M ist eine vorkonfigurierte und validierte Kernlösung für virtualisierte mobile Pakete, die die

Bereitstellung von VNFs vereinfacht. OpenStack ist der Virtualized Infrastructure Manager (VIM) für Ultra-M und besteht aus den folgenden Knotentypen:

- Computing
- Object Storage Disk - Computing (OSD - Computing)
- Controller
- OpenStack-Plattform - Director (OSPD)

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



Dieses Dokument richtet sich an Mitarbeiter von Cisco, die mit der Cisco Ultra-M-Plattform vertraut sind. Es beschreibt die Schritte, die für OpenStack und Redhat OS erforderlich sind.

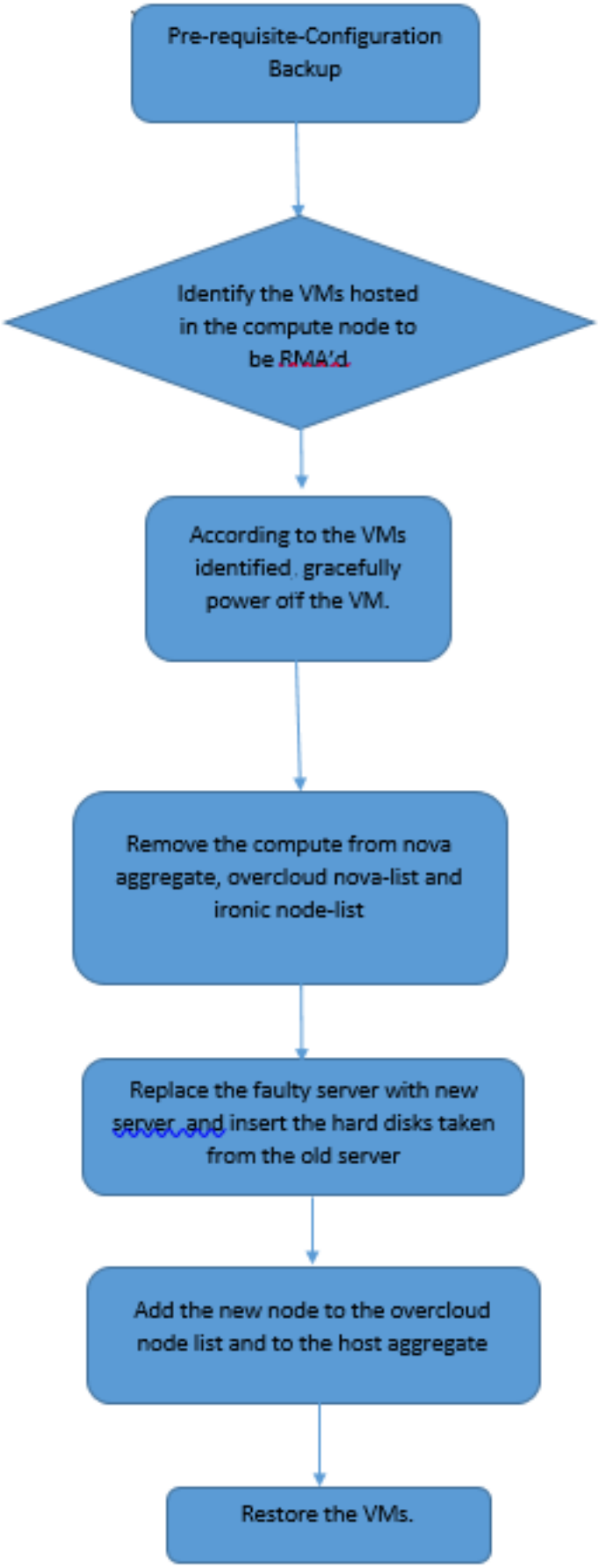
Hinweis: Ultra M 5.1.x wird zur Definition der Verfahren in diesem Dokument berücksichtigt.

Abkürzungen

MOP	Verfahrensweise
OSD	Objektspeicherdatenträger
OSPD	OpenStack Platform Director

HDD	Festplattenlaufwerk
SSD	Solid-State-Laufwerk
VIM	Virtueller Infrastrukturmanager
VM	Virtuelles System
EM	Element Manager
USA	Ultra-Automatisierungsservices
UUID	Universell eindeutige IDentifier

Workflow des MoP



Voraussetzungen

Sicherung

Bevor Sie einen **Compute-**Knoten ersetzen, müssen Sie den aktuellen Zustand Ihrer Red Hat OpenStack Platform-Umgebung überprüfen. Es wird empfohlen, den aktuellen Zustand zu überprüfen, um Komplikationen zu vermeiden, wenn der Ersetzungsprozess **Compute** aktiviert ist. Sie kann durch diesen Austausch erreicht werden.

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

```
[root@ al03-pod2-ospd ~]# mysqldump --opt --all-databases > /root/undercloud-all-databases.sql
[root@ al03-pod2-ospd ~]# 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.

> **Hinweis**: Stellen Sie sicher, dass Sie über den Snapshot der Instanz verfügen, sodass Sie das virtuelle System bei Bedarf wiederherstellen können. Gehen Sie wie folgt vor, um einen Snapshot der VM zu erstellen.

Identifizieren der im Compute-Knoten gehosteten VMs

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

```
[stack@al03-pod2-ospd ~]$ nova list --field name,host

+--------------------------------------+--------------------------+-----------------------------
------+

| ID                                   | Name                     |
Host                              |

+--------------------------------------+--------------------------+-----------------------------
------+

| 46b4b9eb-a1a6-425d-b886-a0ba760e6114 | AAA-CPAR-testing-instance | pod2-stack-compute-
4.localdomain |

| 3bc14173-876b-4d56-88e7-b890d67a4122 | aaa2-21                   | pod2-stack-compute-
3.localdomain |

| f404f6ad-34c8-4a5f-a757-14c8ed7fa30e | aaa21june                 | pod2-stack-compute-
3.localdomain |

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

> **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 den nachfolgenden Abschnitten verwendet.

Snapshot-Prozess

Herunterfahren der CPAR-Anwendung

Schritt 1: Öffnen Sie einen mit dem Netzwerk verbundenen SSH-Client, und stellen Sie eine Verbindung zur CPAR-Instanz her.

Es ist wichtig, nicht alle vier AAA-Instanzen an einem Standort gleichzeitig herunterzufahren, sondern dies einzeln zu tun.

Schritt 2: CPAR-Anwendung mit dem folgenden Befehl herunterfahren:

```
/opt/CSCOar/bin/arserver stop
```

In einer Meldung wird die Meldung "Abgeschlossen der Cisco Prime Access Registrar Server Agent" angezeigt. sollte erscheinen.

> **Hinweis**: Wenn ein Benutzer eine CLI-Sitzung geöffnet hat, funktioniert der Befehl arserver stop nicht, und die folgende Meldung wird angezeigt:

```
ERROR:    You can not shut down Cisco Prime Access Registrar while the
          CLI is being used.   Current list of running
          CLI with process id is:
2903 /opt/CSCOar/bin/aregcmd -s
```

In diesem Beispiel muss die hervorgehobene Prozess-ID 2903 beendet werden, bevor CPAR beendet werden kann. Beenden Sie in diesem Fall den Vorgang mit dem folgenden Befehl:

```
kill -9 *process_id*
```

Wiederholen Sie anschließend Schritt 1.

Schritt 3: Stellen Sie sicher, dass die CPAR-Anwendung mit diesem Befehl tatsächlich heruntergefahren wurde:

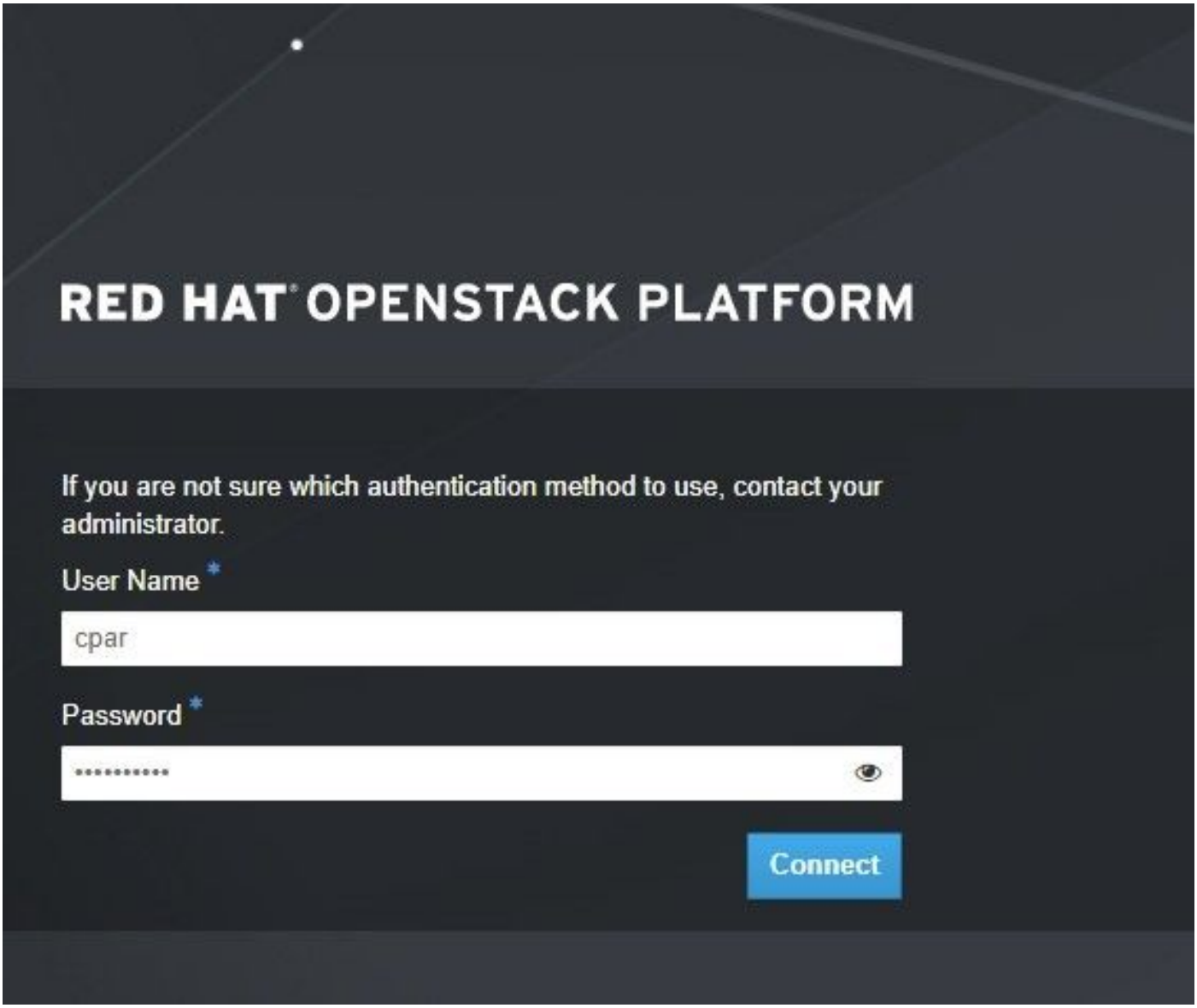
```
/opt/CSCOar/bin/arstatus
```

Diese Meldungen sollten angezeigt werden:

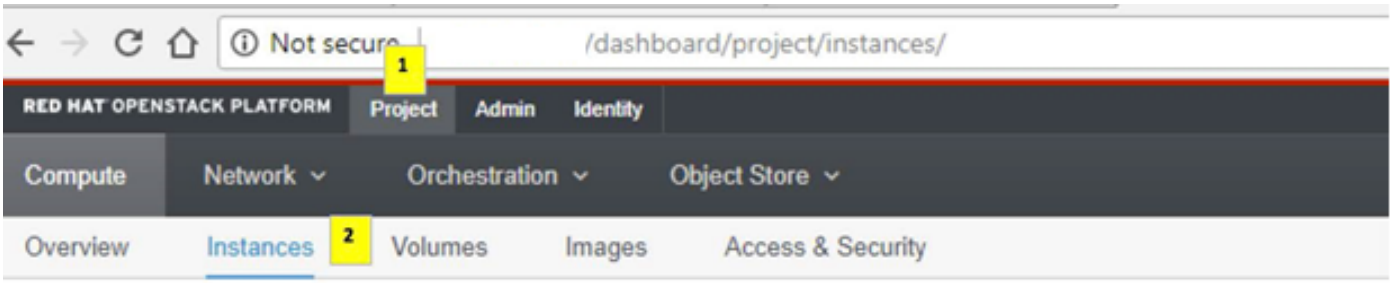
```
Cisco Prime Access Registrar Server Agent not running
Cisco Prime Access Registrar GUI not running
```

VM-Snapshot-Aufgabe

Schritt 1: Geben Sie die Horizon GUI-Website ein, die der aktuell bearbeiteten Website (Stadt) entspricht. Beim Zugriff auf den Horizont wird der im Bild angezeigte Bildschirm angezeigt:

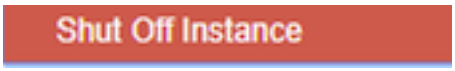


Schritt 2: Navigieren Sie, wie im Bild gezeigt, zu **Projekt > Instanzen**.



Wenn der Benutzer cpar verwendet hat, werden in diesem Menü nur die 4 AAA-Instanzen angezeigt.

Schritt 3: Fahren Sie jeweils nur eine Instanz herunter, und wiederholen Sie den gesamten Vorgang in diesem Dokument. Um das virtuelle System herunterzufahren, navigieren Sie zu **Aktionen > Deaktivierte Instanz** ausschalten, und bestätigen Sie Ihre Auswahl.



Schritt 4 Überprüfen Sie, ob die Instanz tatsächlich durch Status = Shutoff und Power State = Shut

Down heruntergefahren wurde.

Mit diesem Schritt wird der CPAR-Abschaltvorgang beendet.

VM-Snapshot

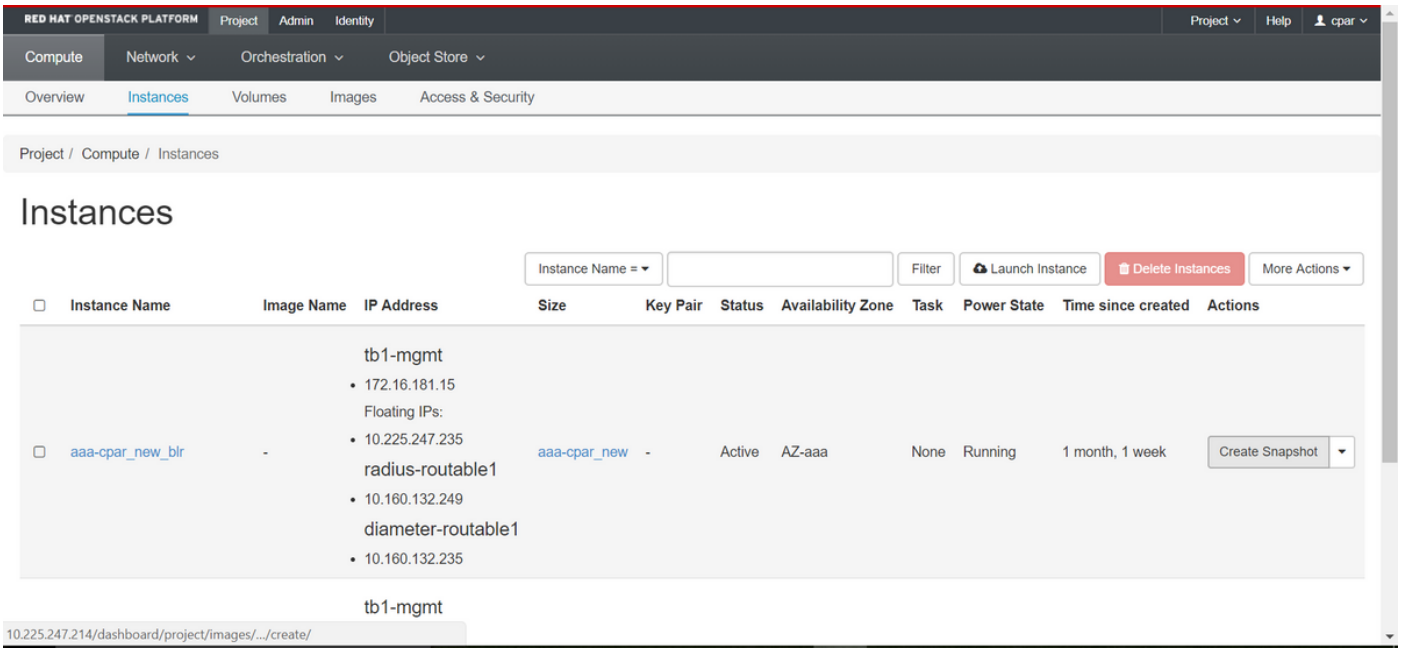
Sobald die CPAR-VMs ausfallen, können die Snapshots parallel erstellt werden, da sie zu unabhängigen Berechnungen gehören.

Die vier QCOW2-Dateien werden parallel erstellt.

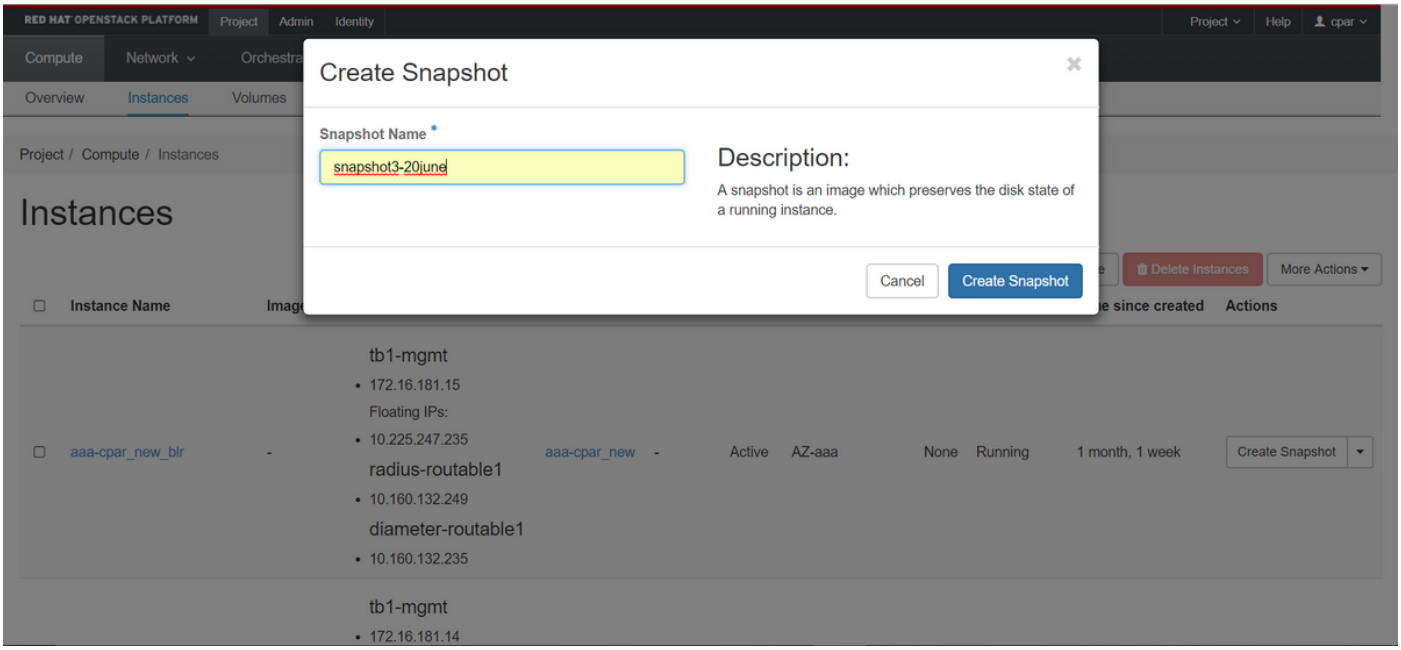
Erstellen Sie einen Snapshot jeder AAA-Instanz (25 Minuten bis 1 Stunde) (25 Minuten für Instanzen, die ein qcow-Image als Quelle und 1 Stunde für Instanzen verwenden, die ein Rohbild als Quelle verwenden).

Schritt 1: Melden Sie sich bei der Horizon **GUI** von POD OpenStack an.

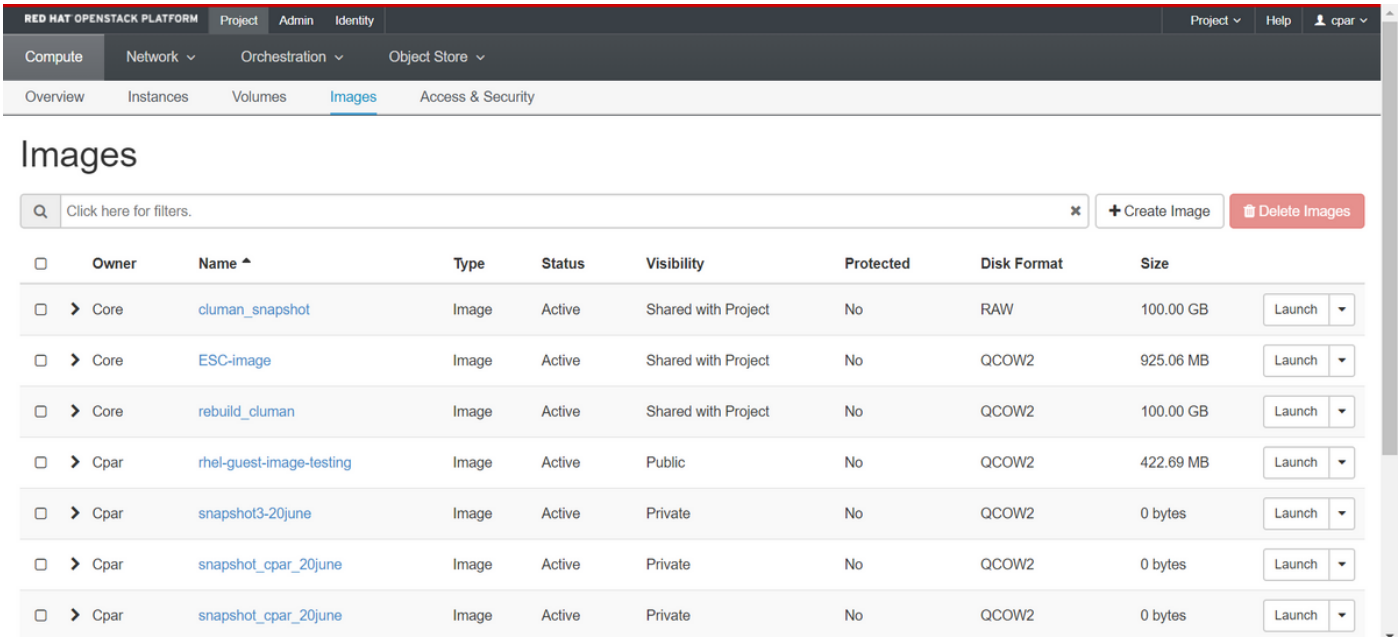
Schritt 2: Wenn Sie sich angemeldet haben, fahren Sie mit **Projekt > Computing > Instanzen**, im oberen Menü fort, und suchen Sie nach den AAA-Instanzen.



Schritt 3: Klicken Sie auf den **Snapshot erstellen**, um mit der Snapshot-Erstellung fortzufahren (diese muss für die entsprechende AAA-Instanz ausgeführt werden).



Schritt 4: Sobald der Snapshot ausgeführt wurde, navigieren Sie zum Menü **Images**, und überprüfen Sie, ob der Snapshot abgeschlossen ist, und melden Sie keine Probleme.



Schritt 5: Der nächste Schritt besteht darin, den Snapshot im QCOW2-Format herunterzuladen und an eine entfernte Einheit zu übertragen, falls das OSPD während dieses Prozesses verloren geht. Um dies zu erreichen, identifizieren Sie den Snapshot mithilfe dieser **Übersichtsbildliste** auf OSPD-Ebene.

```
[root@elospd01 stack]# glance image-list

+--------------------------------------+---------------------------+
| ID                                   | Name                      |
+--------------------------------------+---------------------------+
| 80f083cb-66f9-4fcf-8b8a-7d8965e47b1d | AAA-Temporary             |
| 22f8536b-3f3c-4bcc-ae1a-8f2ab0d8b950 | ELP1 cluman 10_09_2017    |
| 70ef5911-208e-4cac-93e2-6fe9033db560 | ELP2 cluman 10_09_2017    |
```

```
| e0b57fc9-e5c3-4b51-8b94-56cbccdf5401 | ESC-image                 |

| 92dfe18c-df35-4aa9-8c52-9c663d3f839b | lgnaaa01-sept102017       |

| 1461226b-4362-428b-bc90-0a98cbf33500 | tmobile-pcrf-13.1.1.iso   |

| 98275e15-37cf-4681-9bcc-d6ba18947d7b | tmobile-pcrf-13.1.1.qcow2 |

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

Schritt 6: Sobald der Snapshot identifiziert wurde, der heruntergeladen werden soll (in diesem Fall der Snapshot, der oben grün markiert ist), wird er über diesen Befehl **Blick Image-Download** auf ein QCOW2-Format heruntergeladen, wie hier gezeigt.

```
[root@elospd01 stack]# glance image-download 92dfe18c-df35-4aa9-8c52-9c663d3f839b --file
/tmp/AAA-CPAR-LGNoct192017.qcow2 &
```

- Das "&" sendet den Prozess an den Hintergrund. Es dauert einige Zeit, diese Aktion abzuschließen, sobald sie abgeschlossen ist, kann sich das Bild im Verzeichnis /tmp befinden.
- Wenn der Prozess an den Hintergrund gesendet wird und die Verbindung unterbrochen wird, wird der Vorgang ebenfalls beendet.
- Führen Sie den Befehl **dissown -h aus**, sodass der Prozess bei Verlust der Secure Shell (SSH)-Verbindung weiterhin auf dem OSPD ausgeführt wird und abgeschlossen wird.

Schritt 7: Nach Abschluss des Download-Vorgangs muss ein Komprimierungsprozess ausgeführt werden, da dieser Snapshot aufgrund von Prozessen, Aufgaben und temporären Dateien, die vom Betriebssystem behandelt werden, mit ZEROES gefüllt werden kann. Der für die Dateikomprimierung verwendete Befehl ist **virt-sparsify**.

```
[root@elospd01 stack]# virt-sparsify AAA-CPAR-LGNoct192017.qcow2 AAA-CPAR-
LGNoct192017_compressed.qcow2
```

Dieser Vorgang dauert etwa 10-15 Minuten. Nach Abschluss des Vorgangs muss die resultierende Datei wie im nächsten Schritt angegeben an eine externe Einheit übertragen werden.

Um dies zu erreichen, muss die Integrität der Datei überprüft werden. Führen Sie dazu den nächsten Befehl aus, und suchen Sie nach dem **beschädigten** Attribut am Ende der Ausgabe.

```
[root@wsospd01 tmp]# qemu-img info AAA-CPAR-LGNoct192017_compressed.qcow2
image: AAA-CPAR-LGNoct192017_compressed.qcow2
file format: qcow2
virtual size: 150G (161061273600 bytes)
disk size: 18G
cluster_size: 65536
Format specific information:

    compat: 1.1

    lazy refcounts: false

    refcount bits: 16

    corrupt: false
```

Um ein Problem beim Verlust des OSPD zu vermeiden, muss der vor kurzem erstellte Snapshot im QCOW2-Format an eine externe Einheit übertragen werden. Bevor wir die Dateiübertragung

starten, müssen wir überprüfen, ob das Ziel genügend freien Speicherplatz hat, verwenden Sie den Befehl **df -kh**, um den Speicherplatz zu überprüfen. Es wird empfohlen, das Dokument vorübergehend über SFTP **sftp root@x.x.x.x** in das OSPD-Dokument eines anderen Standorts zu übertragen, wobei x.x.x.x die IP-Adresse eines Remote-OSPD ist. Um die Übertragung zu beschleunigen, kann das Ziel an mehrere OSPDs gesendet werden. Ebenso kann dieser Befehl **scp *name_of_the_file*.qcow2 root@ x.x.x:/tmp** verwenden (wobei x.x.x.x die IP-Adresse eines Remote-OSPD ist), um die Datei in ein anderes OSPD-Projekt zu übertragen.

Graceful Power Aus

Ausschaltknoten

1. So schalten Sie die Instanz aus: nova stop <INSTANCE_NAME>

2. Nun sehen Sie den Instanznamen mit dem Status Shutoff.

```
[stack@director ~]$ nova stop  aaa2-21

Request to stop server aaa2-21 has been accepted.

[stack@director ~]$ nova list

+--------------------------------------+--------------------------+---------+------------+-----
--------+-------------------------------------------------------------------------------------
--------------------+

| ID                                   | Name                     | Status  | Task State |
Power State |
Networks
            |

+--------------------------------------+--------------------------+---------+------------+-----
--------+-------------------------------------------------------------------------------------
--------------------+

| 46b4b9eb-a1a6-425d-b886-a0ba760e6114 | AAA-CPAR-testing-instance | ACTIVE  | -          |
Running     | tb1-mgmt=172.16.181.14, 10.225.247.233; radius-routable1=10.160.132.245; diameter-
routable1=10.160.132.231 |

| 3bc14173-876b-4d56-88e7-b890d67a4122 | aaa2-21                  | SHUTOFF | -          |
Shutdown    | diameter-routable1=10.160.132.230; radius-routable1=10.160.132.248; tb1-
mgmt=172.16.181.7, 10.225.247.234  |

| f404f6ad-34c8-4a5f-a757-14c8ed7fa30e | aaa21june                | ACTIVE  | -          |
Running     | diameter-routable1=10.160.132.233; radius-routable1=10.160.132.244; tb1-
mgmt=172.16.181.10                 |

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

Löschen von Computing-Knoten

Die in diesem Abschnitt beschriebenen Schritte sind unabhängig von den im **Computing**-Knoten

gehosteten VMs häufig.

Computing-Knoten aus der Dienstliste löschen

Löschen Sie den **Computing-**Service aus der Liste:

```
[stack@director ~]$ openstack compute service list |grep compute-3

| 138 | nova-compute     | pod2-stack-compute-3.localdomain     | AZ-aaa   | enabled | up    |
2018-06-21T15:05:37.000000 |
```

Offenstack berechnen service delete <ID>

```
[stack@director ~]$ openstack compute service delete 138
```

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-3

| 3b37fa1d-01d4-404a-886f-ff68cec1ccb9 | Open vSwitch agent | pod2-stack-compute-
3.localdomain     | None              | True  | UP    | neutron-openvswitch-agent |
```

openstack network agent delete <ID>

```
[stack@director ~]$ openstack network agent delete 3b37fa1d-01d4-404a-886f-ff68cec1ccb9
```

Aus der Ironischen Datenbank löschen

Löschen Sie einen Knoten aus der ironischen Datenbank, und überprüfen Sie ihn:

nova show <berechnen-node> | grep Hypervisor

```
[root@director ~]# source stackrc
[root@director ~]# nova show pod2-stack-compute-4 | grep hypervisor
| OS-EXT-SRV-ATTR:hypervisor_hostname  | 7439ea6c-3a88-47c2-9ff5-0a4f24647444
```

ironischer Node-Delete <ID>

```
[stack@director ~]$ ironic node-delete 7439ea6c-3a88-47c2-9ff5-0a4f24647444
[stack@director ~]$ ironic node-list
```

Der gelöschte Knoten darf jetzt nicht in der ironischen Knotenliste aufgeführt werden.

Löschen aus der Overcloud

Schritt 1: Erstellen Sie eine Skriptdatei mit dem Namen **delete_node.sh** mit dem angezeigten Inhalt. 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-name> <UUID>

[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
pod2-stack 7439ea6c-3a88-47c2-9ff5-0a4f24647444
Deleting the following nodes from stack pod2-stack:
- 7439ea6c-3a88-47c2-9ff5-0a4f24647444
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-Stack-Vorgang in den VOLLSTÄNDIGEN Zustand wechselt:

```
[stack@director ~]$  openstack stack list
+--------------------------------------+------------+-----------------+----------------------+--
--------------------+
| ID                                   | Stack Name | Stack Status    | Creation Time        |
Updated Time         |
+--------------------------------------+------------+-----------------+----------------------+--
--------------------+
| 5df68458-095d-43bd-a8c4-033e68ba79a0 | pod2-stack | UPDATE_COMPLETE | 2018-05-08T21:30:06Z |
2018-05-08T20:42:48Z |
+--------------------------------------+------------+-----------------+----------------------+--
--------------------+
```

Installation des neuen Computing-Knotens

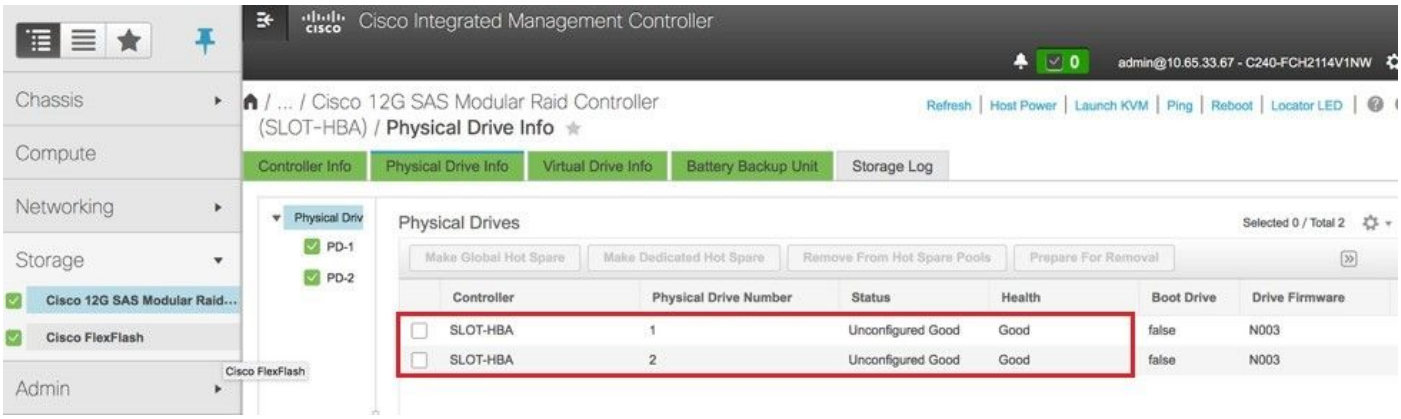
Die Schritte zur Installation eines neuen UCS C240 M4 Servers und die ersten Installationsschritte können im Cisco UCS C240 M4 Server Installations- und Serviceleitfaden beschrieben werden.

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

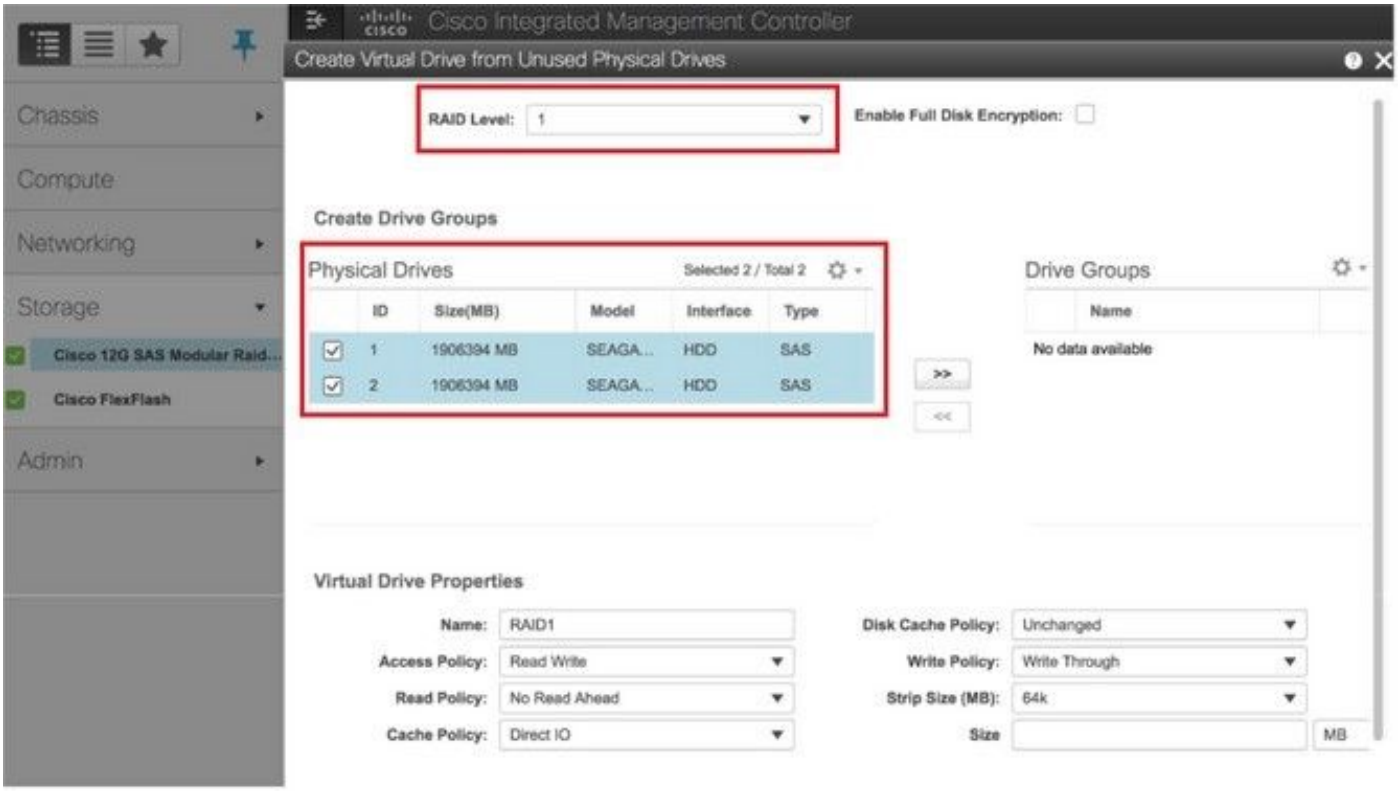
Schritt 2: Melden Sie sich mithilfe der CIMC IP beim Server an.

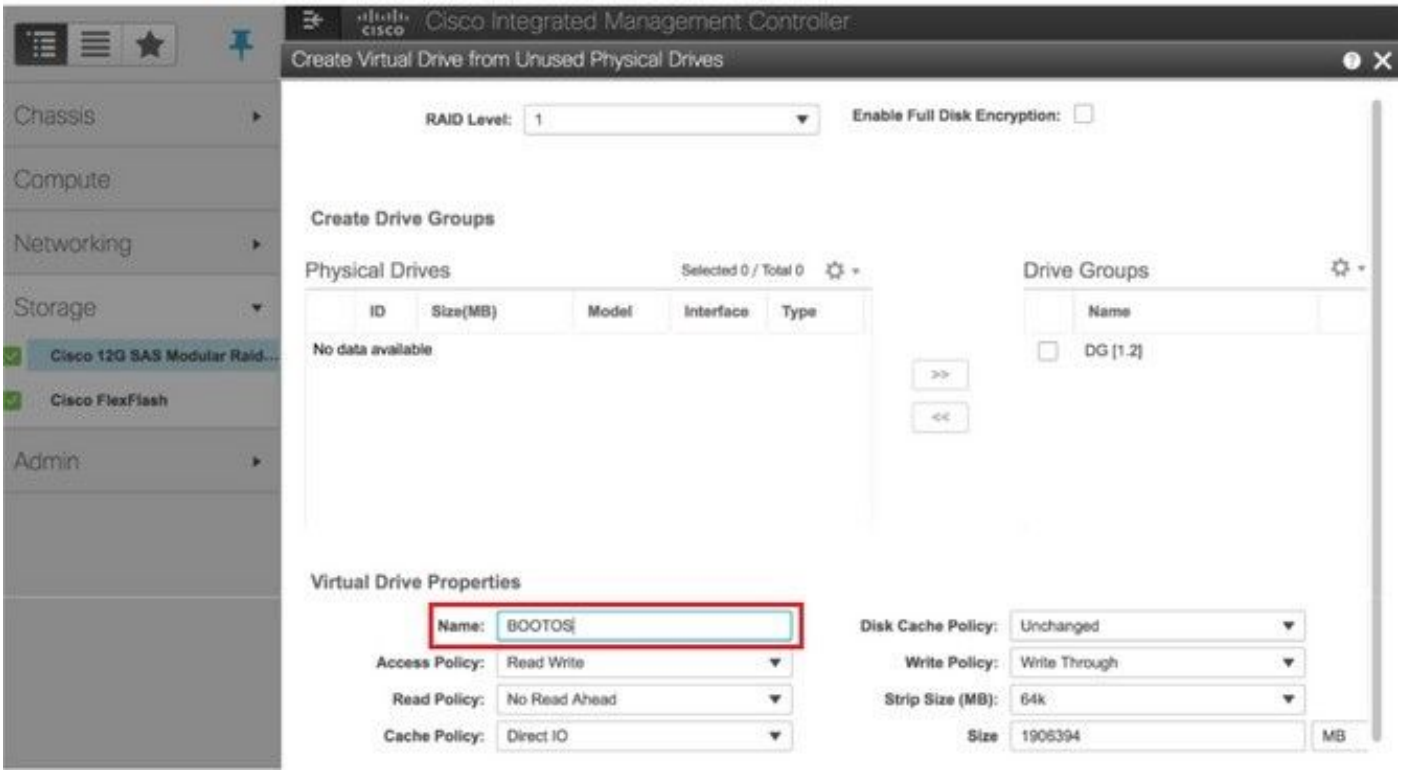
Schritt 3: Führen Sie ein BIOS-Upgrade durch, wenn die Firmware nicht der zuvor verwendeten empfohlenen Version entspricht. Schritte für ein BIOS-Upgrade finden Sie hier: [BIOS-Upgrade-Leitfaden für Rackmount-Server der Cisco UCS C-Serie]

Schritt 4: Um den Status von physischen Laufwerken zu überprüfen, die **nicht konfiguriert** sind, wechseln Sie zu **Storage > Cisco 12G SAS Modular Raid Controller (SLOT-HBA) > Informationen zu physischen Laufwerken**.



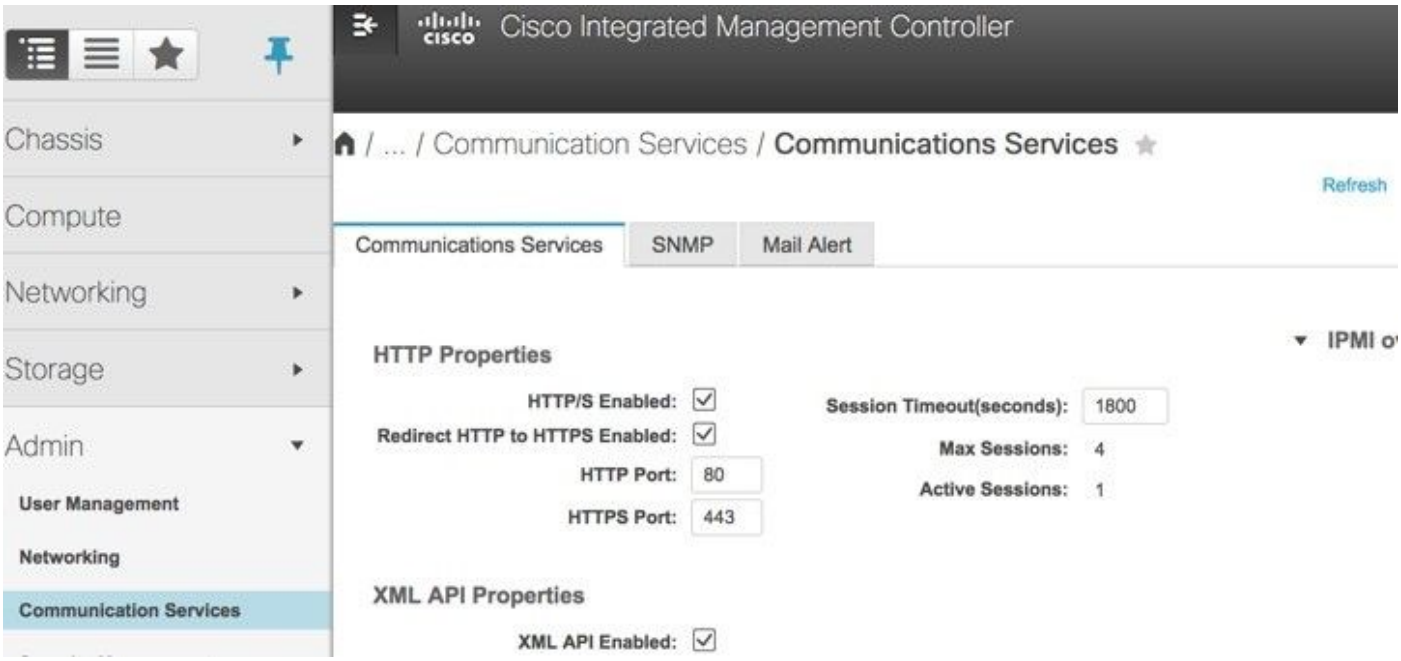
Schritt 5: Um eine virtuelle Festplatte von den physischen Laufwerken mit RAID-Level 1 zu erstellen, gehen Sie zu **Storage > Cisco 12G SAS Modular Raid Controller (SLOT-HBA) > Controller Info > Create Virtual Drive from Unused Physical Drives (Virtuelles Laufwerk aus nicht verwendeten physischen Laufwerken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





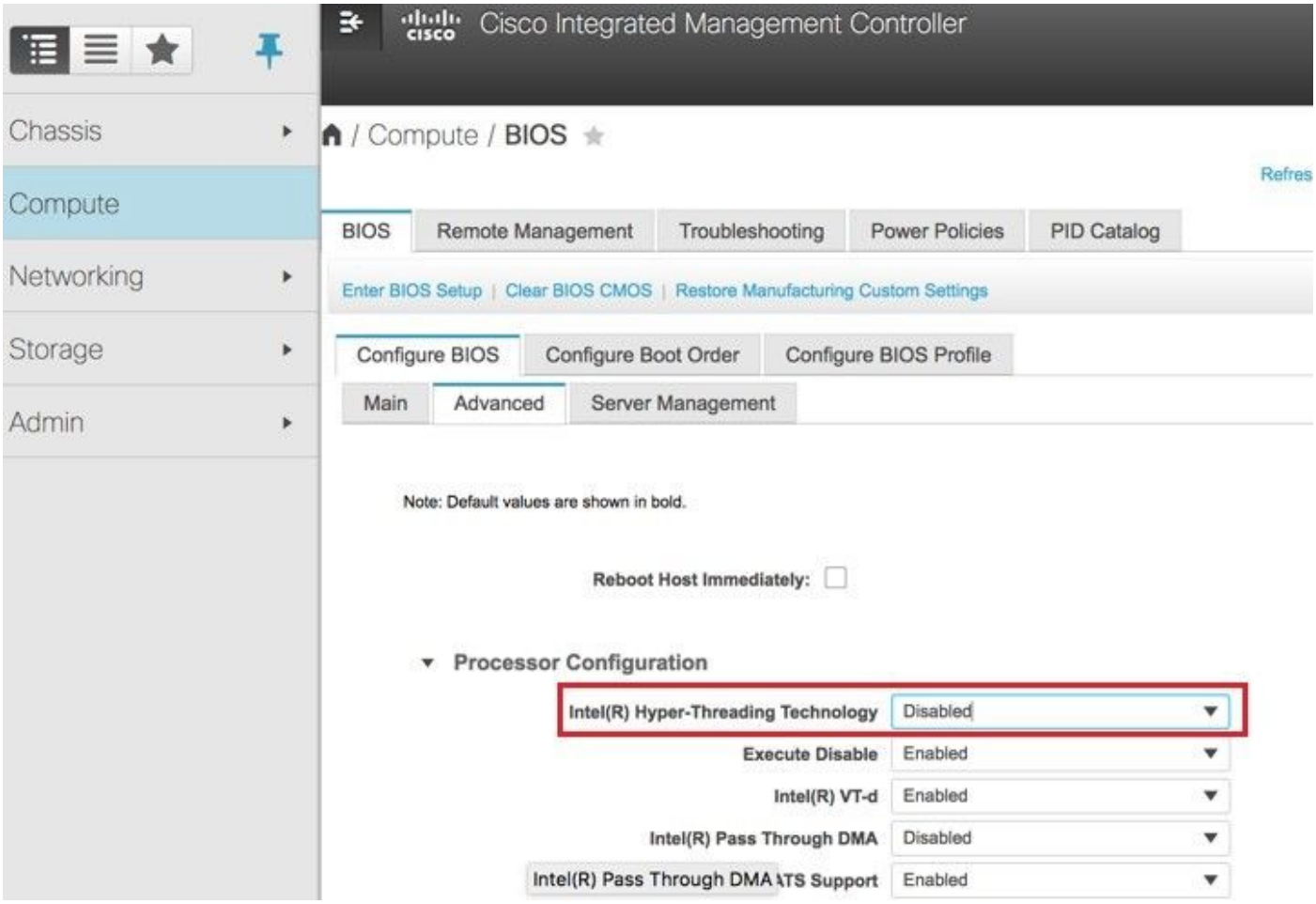
Schritt 6: Wählen Sie die VD aus, und konfigurieren Sie **Set as Boot Drive** (Als Startlaufwerk festlegen), wie im Bild gezeigt.

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, 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 VMs üblich.

Schritt 1: **Compute-**Server mit einem anderen Index hinzufügen

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 noch nicht verwendet wurde. Erhöhen Sie in der Regel den nächsthöchsten **Computing-**Wert.

Beispiel: Die höchste vorherige Version war **compute**-17, 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":[
                "<MAC_ADDRESS>"
            ],
            "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: Führen Sie das Skript deploy.sh aus, das zuvor für die Bereitstellung des Stacks verwendet wurde, um den neuen Computode 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 5: 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 6: Überprüfen Sie, ob sich der neue **Computing-**Knoten im aktiven Zustand befindet.

```
[root@director ~]# nova list | grep pod2-stack-compute-4

| 5dbac94d-19b9-493e-a366-1e2e2e5e34c5 | pod2-stack-compute-4     | ACTIVE | -          |
Running     | ctlplane=192.200.0.116 |
```

Stellen Sie die VMs wieder her

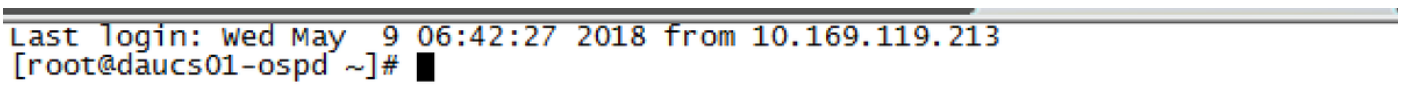
Wiederherstellen einer Instanz durch Snapshot

Wiederherstellungsprozess:

Es ist möglich, die vorherige Instanz mit dem in vorherigen Schritten ausgeführten Snapshot erneut bereitzustellen.

Schritt 1 [OPTIONAL]. Wenn kein früherer VMSnapshot verfügbar ist, stellen Sie eine Verbindung zum OSPD-Knoten her, an den die Sicherung gesendet wurde, und setzen Sie die Sicherung zurück zum ursprünglichen OSPD-Knoten. Über **sftp** root@x.x.x.x, wobei x.x.x.x die IP des ursprünglichen OSPD ist. Speichern Sie die Snapshot-Datei im Verzeichnis /tmp.

Schritt 2: Stellen Sie eine Verbindung zum OSPD-Knoten her, in dem die Instanz erneut bereitgestellt wird.



Geben Sie die Umgebungsvariablen mit dem folgenden Befehl zurück:

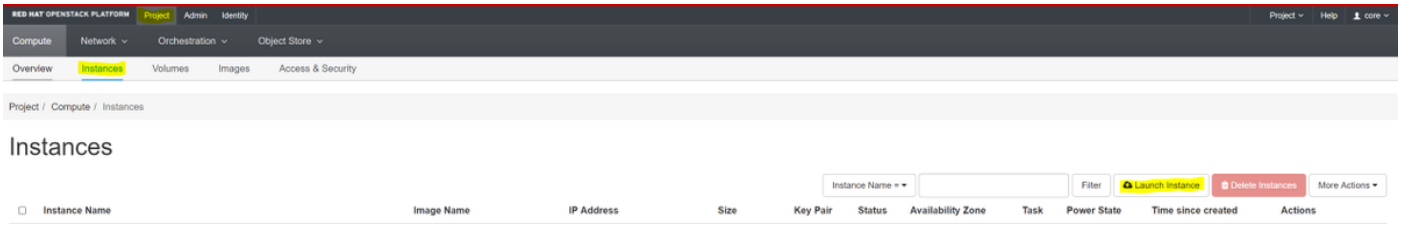
```
# source /home/stack/pod1-stackrc-Core-CPAR
```

Schritt 3: Um den Snapshot als Bild zu verwenden, ist notwendig, um ihn in Horizont als solches hochzuladen. Verwenden Sie dazu den nächsten Befehl.

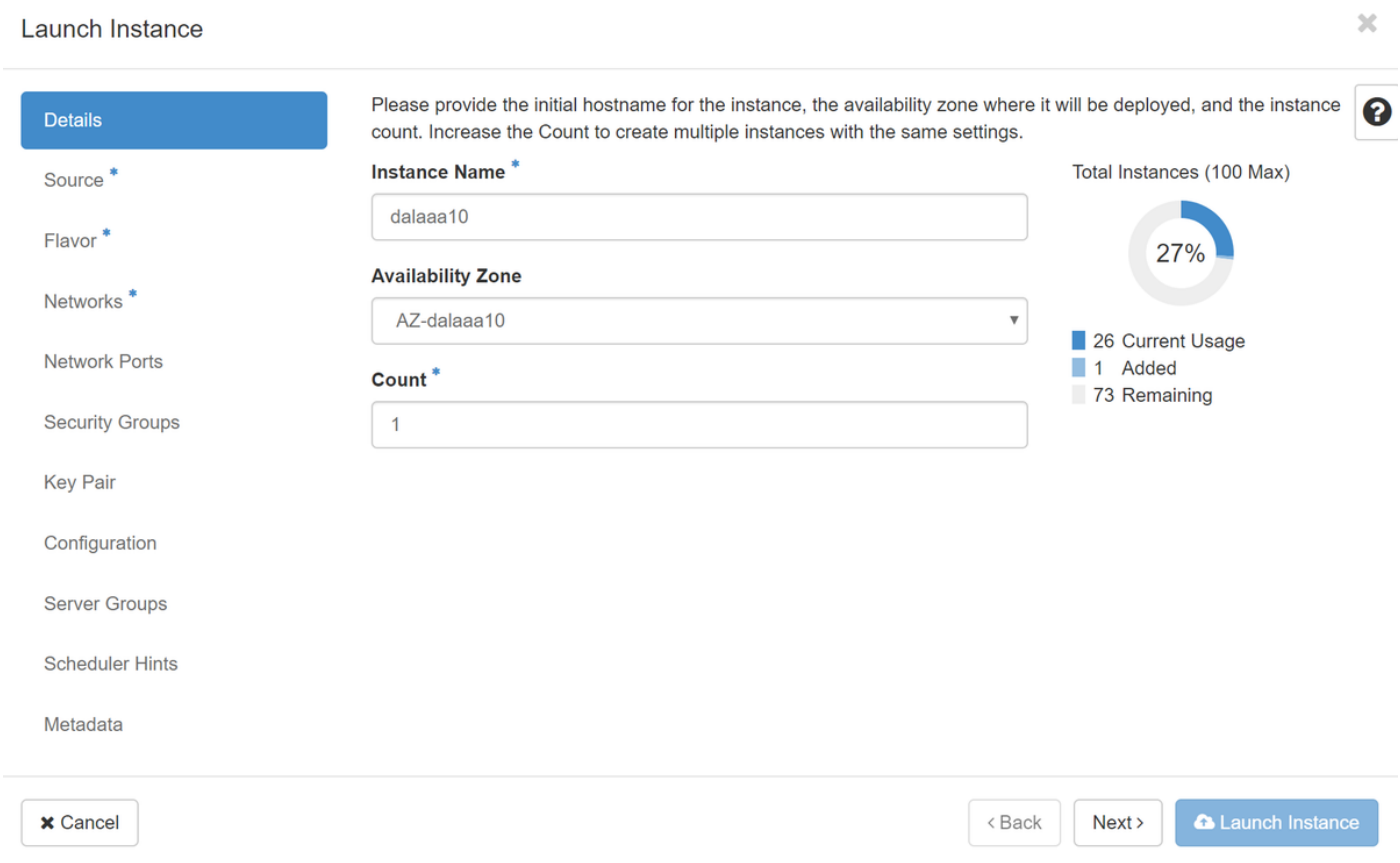
```
#glance image-create -- AAA-CPAR-Date-snapshot.qcow2 --container-format bare --disk-format qcow2
--name AAA-CPAR-Date-snapshot
```

Der Prozess ist am Horizont erkennbar.

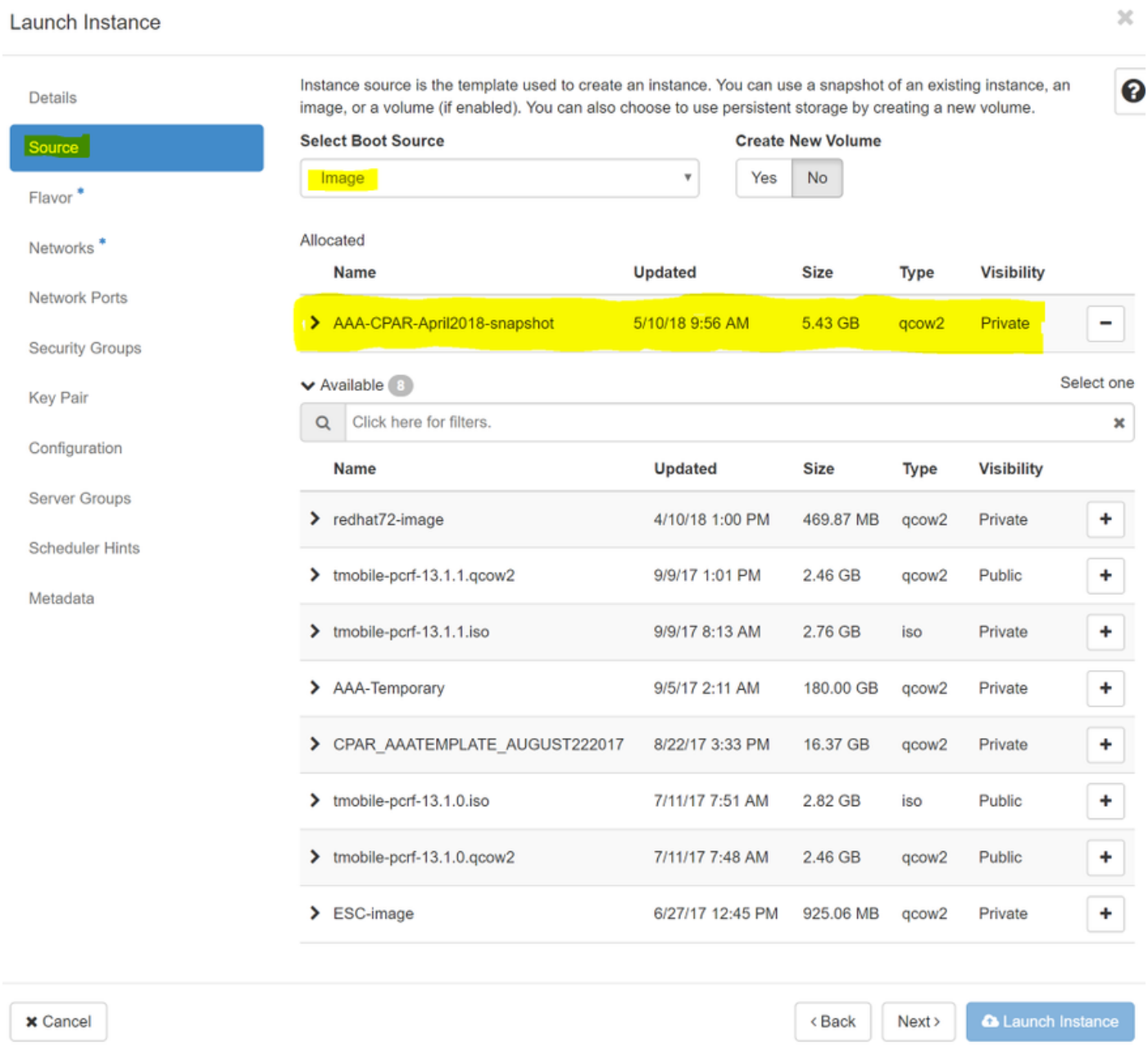
Schritt 4: Navigieren Sie im Horizont zu **Projekt > Instanzen**, und klicken Sie auf **Instanz starten**, wie im Bild gezeigt.



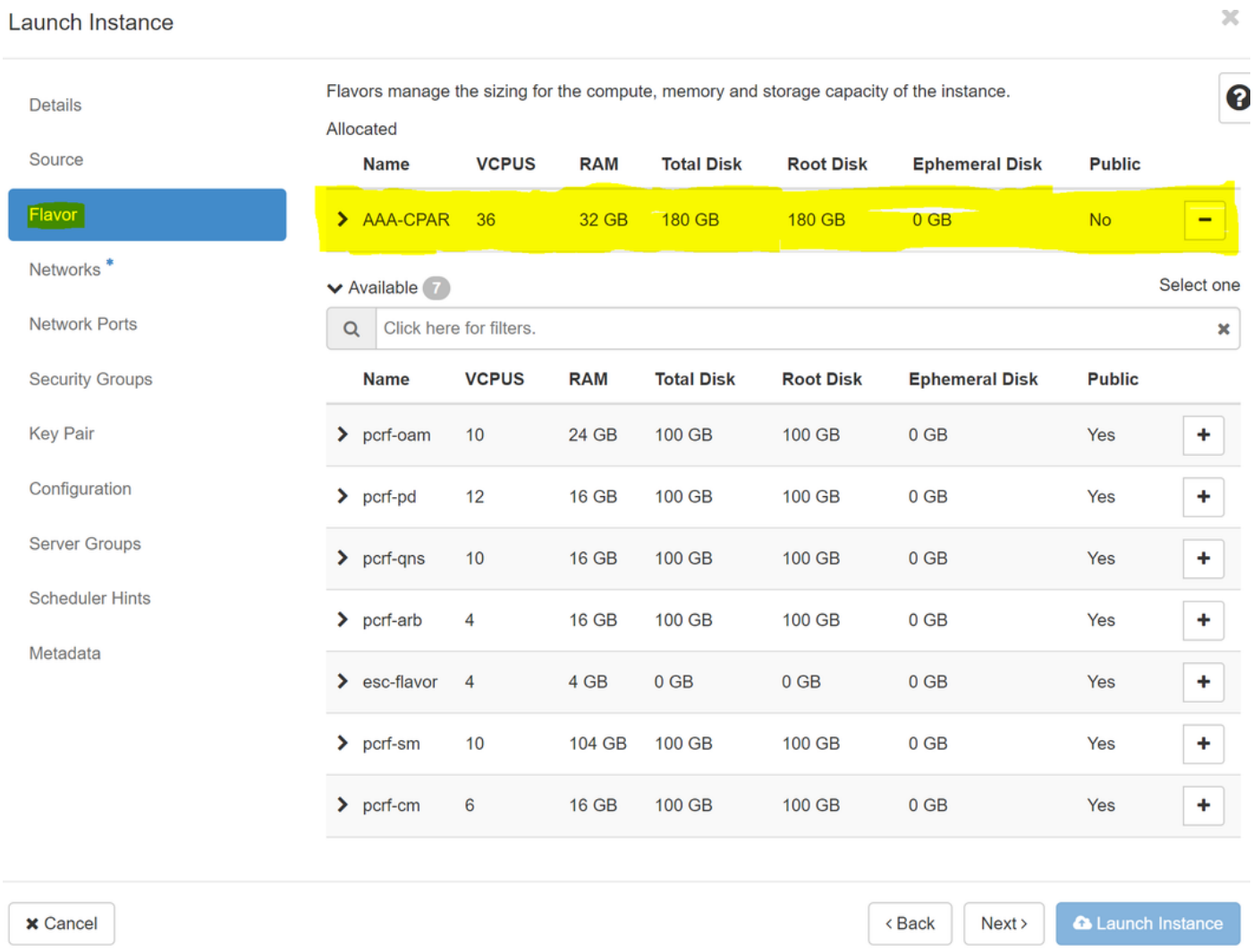
Schritt 5: Geben Sie den **Instanznamen ein** und wählen Sie die **Verfügbarkeitszone**, wie im Bild gezeigt.



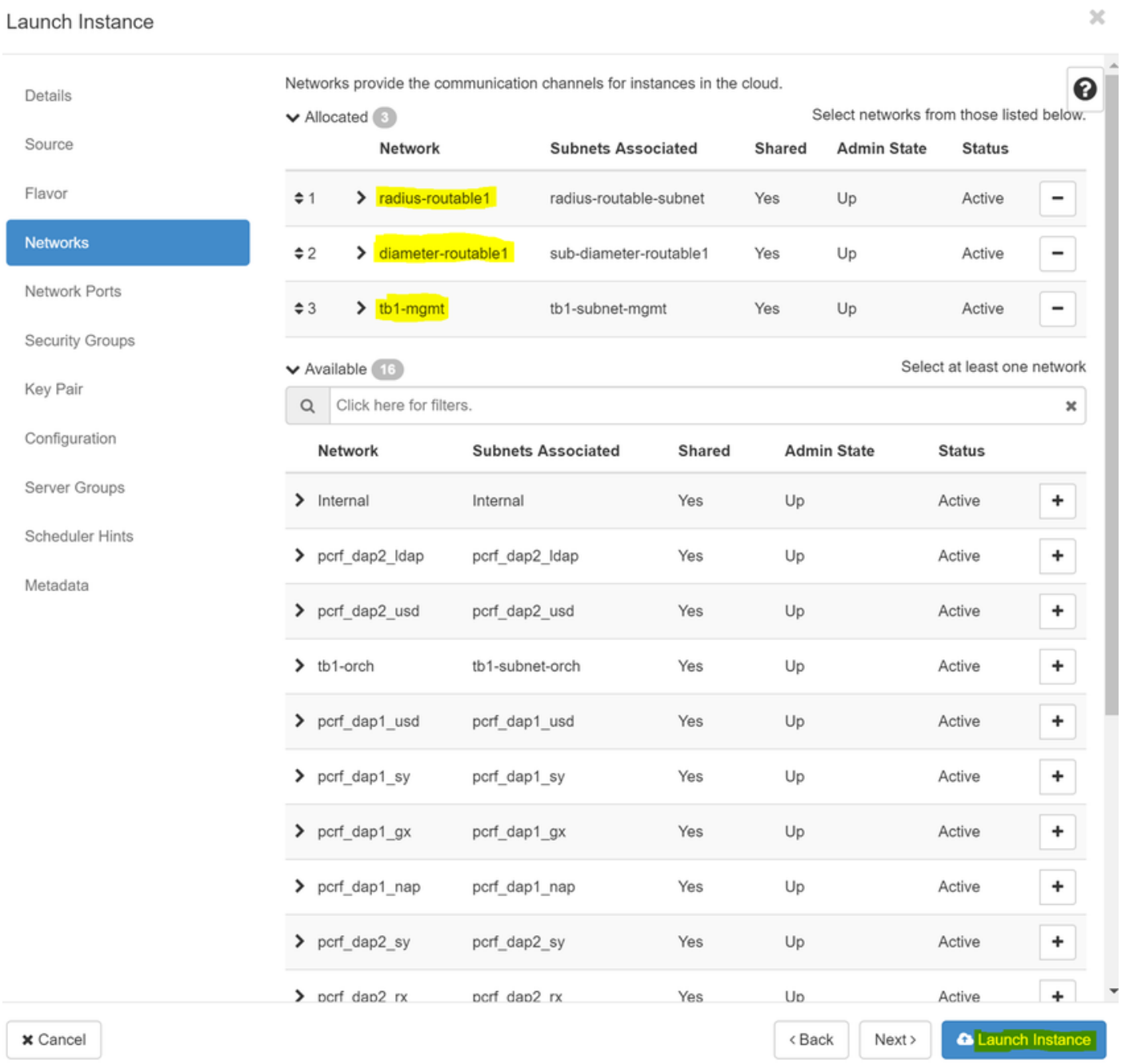
Schritt 6: Wählen Sie auf der Registerkarte **Quelle** das Bild aus, um die Instanz zu erstellen. Wählen Sie im Menü **Startquelle auswählen das Bild** aus, hier wird eine Liste der Bilder angezeigt. Wählen Sie das Bild aus, das zuvor hochgeladen wurde, während Sie auf das **+** Zeichen klicken.



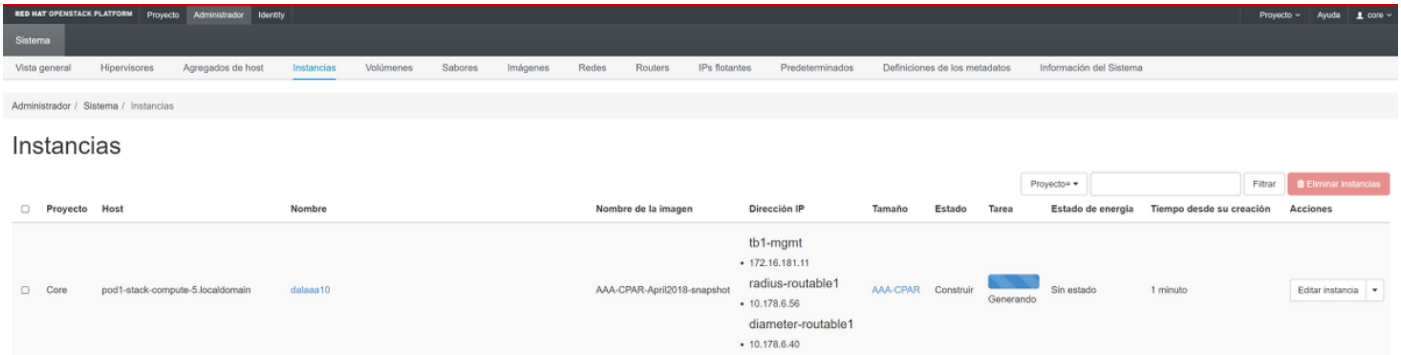
Schritt 7: Wählen Sie auf der Registerkarte **Flavor** den AAA-Geschmack aus, während Sie auf **+** klicken, wie im Bild gezeigt.



Schritt 8: Navigieren Sie jetzt zur Registerkarte **Netzwerke** und wählen Sie die Netzwerke aus, die die Instanz benötigt, während Sie auf das Pluszeichen + klicken. In diesem Fall wählen Sie **durchmesser-soutable1**, **radius-routing1** und **tb1-mgmt**, wie im Bild gezeigt.



Schritt 9: Klicken Sie auf Instanz starten, um die Instanz zu erstellen. Der Fortschritt kann in Horizont überwacht werden:



Nach einigen Minuten wird die Instanz vollständig bereitgestellt und einsatzbereit.

Erstellen und Zuweisen einer Floating-IP-Adresse

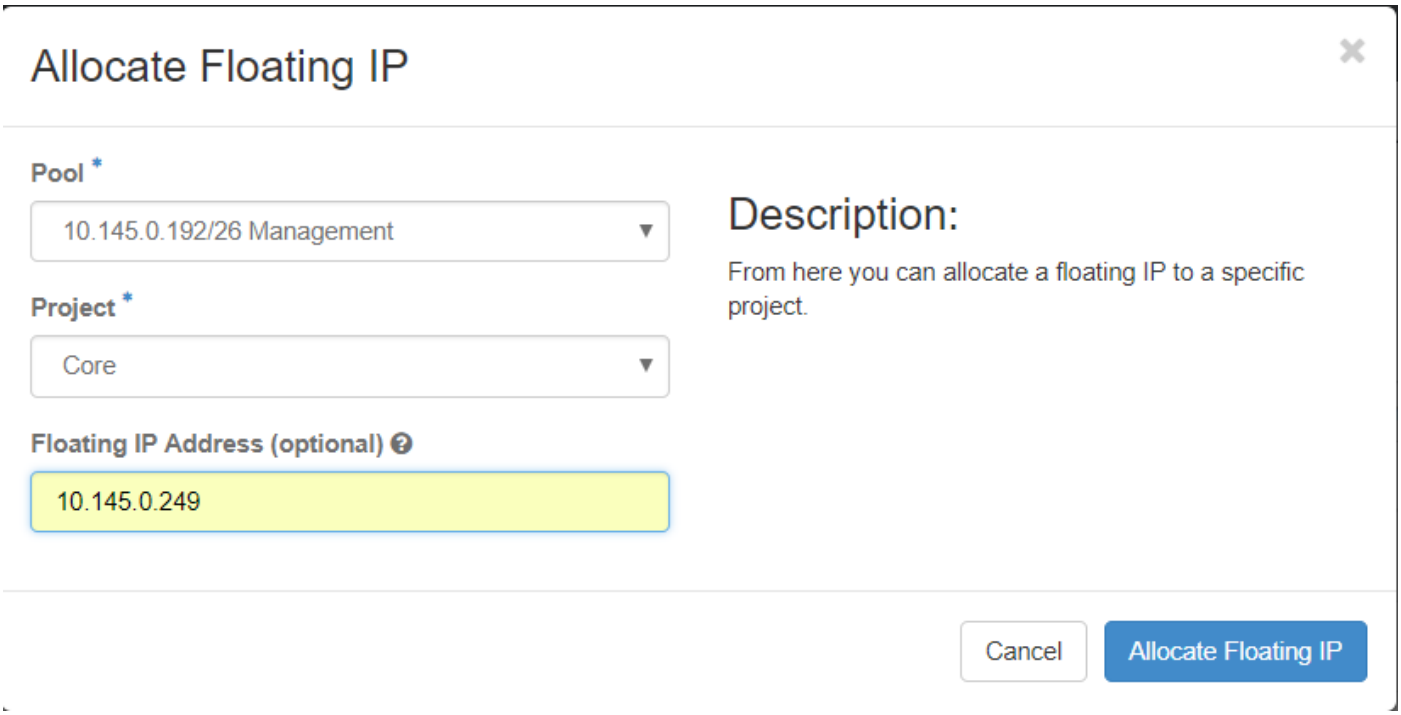
Eine Floating-IP-Adresse ist eine routbare Adresse, d. h. sie ist von der Außenseite der Ultra M/OpenStack-Architektur aus erreichbar und kann mit anderen Knoten aus dem Netzwerk kommunizieren.

Schritt 1: Navigieren Sie im oberen Horizon-Menü zu **Admin > Floating IPs (Admin > Floating-IPs).**

Schritt 2: Klicken Sie auf die Schaltfläche IP **Projekt zuweisen**.

Schritt 3: Wählen Sie im Fenster **Zuweisen von Floating-IP** den **Pool aus**, aus dem die neue unverankerte IP gehört, das **Projekt**, dem sie zugewiesen werden soll, und die neue **Floating-IP-Adresse** selbst.

Beispiel:

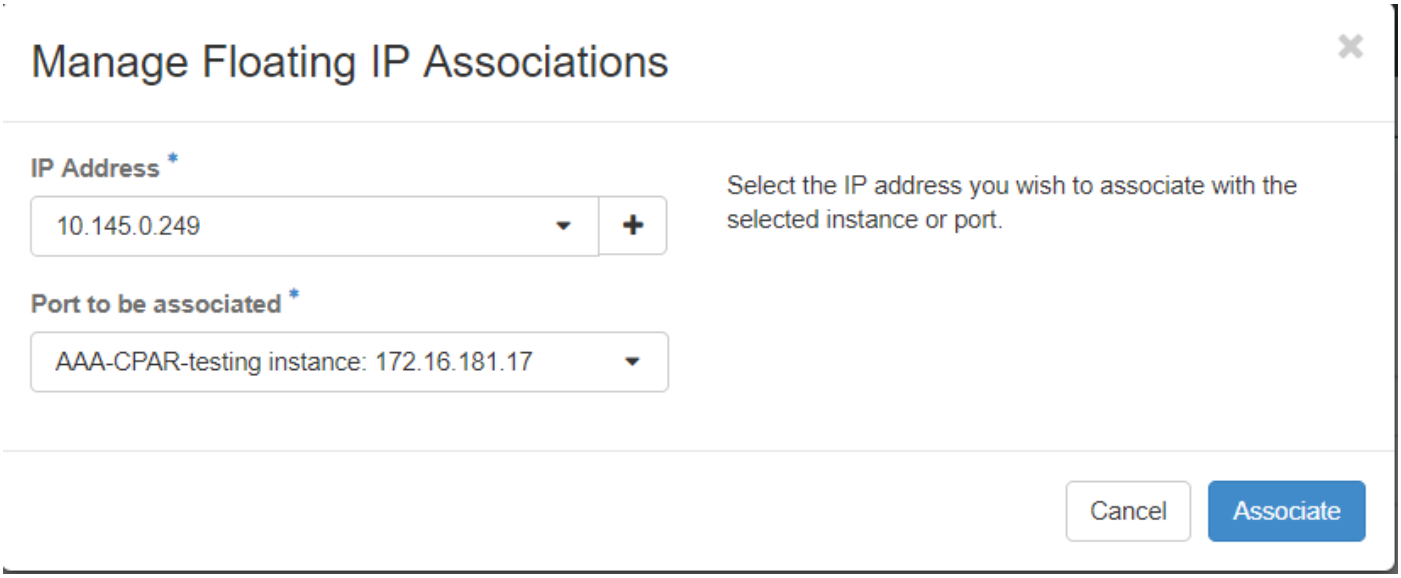


Schritt 4: Klicken Sie auf die Schaltfläche **Zuweisen von Floating-IP**.

Schritt 5: Navigieren Sie im oberen Menü Horizont zu **Projekt > Instanzen.**

Schritt 6: Klicken Sie in der Spalte **Aktion** auf den Pfeil, der in der Schaltfläche **Snapshot erstellen** nach unten zeigt, und ein Menü sollte angezeigt werden. Wählen Sie **die** Option **Zuordnen - Floating-IP aus**.

Schritt 7: Wählen Sie die entsprechende unverankerte IP-Adresse aus, die im Feld **IP-Adresse** verwendet werden soll, und wählen Sie die entsprechende Management-Schnittstelle (eth0) aus der neuen Instanz aus, der diese unverankerte IP im **zu verknüpfenden Port** zugewiesen wird. Das nächste Bild ist ein Beispiel für dieses Verfahren.



Schritt 8: Klicken Sie auf **Zuordnen**.

SSH aktivieren

Schritt 1: Navigieren Sie im oberen Menü Horizont zu **Projekt > Instanzen.**

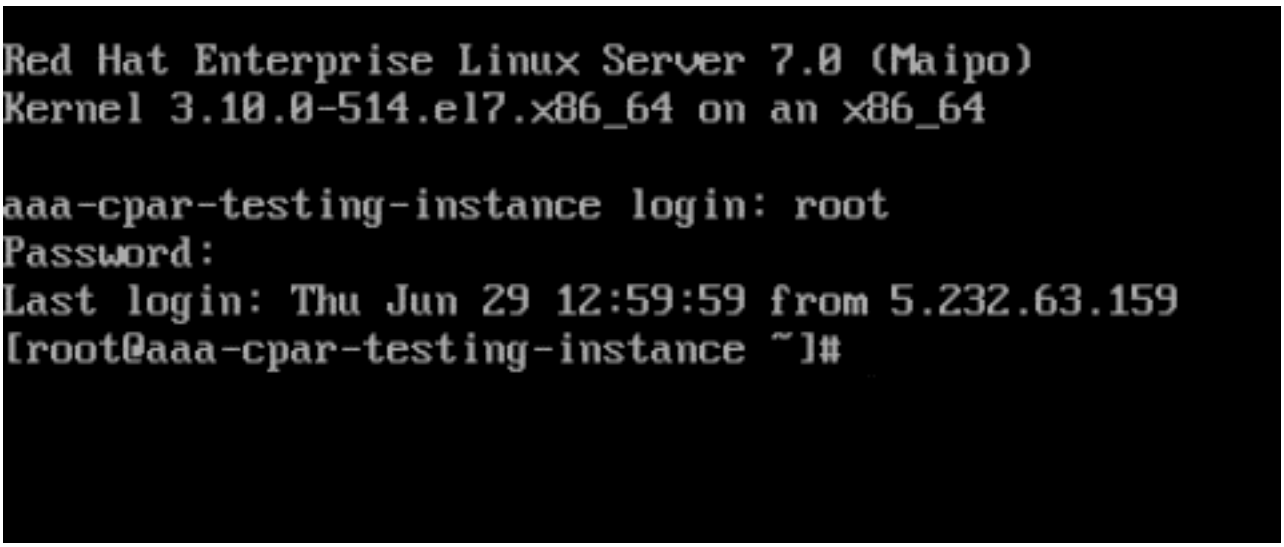
Schritt 2: Klicken Sie auf den Namen der im Abschnitt **Lunch a new instance** erstellten Instanz/VM.

Schritt 3: Klicken Sie auf die Registerkarte **Konsole**. Es wird die CLI des virtuellen Systems angezeigt.

Schritt 4: Geben Sie nach der Anzeige der CLI die entsprechenden Anmeldeinformationen ein:

Benutzername: **Wurzel**

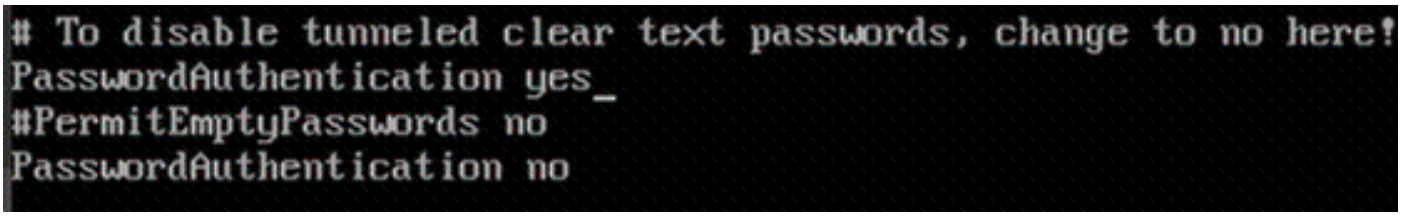
Kennwort: **Cisco 123**



Schritt 5: Geben Sie in der CLI den Befehl **vi /etc/ssh/sshd**_config zum Bearbeiten der SSH-Konfiguration ein.

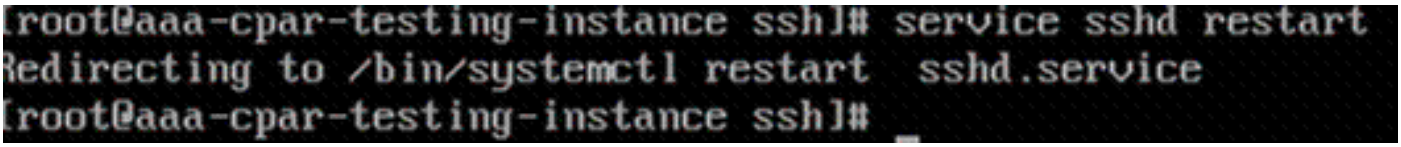
Schritt 6: Wenn die ssh-Konfigurationsdatei geöffnet ist, drücken Sie **I**, um die Datei zu bearbeiten. Suchen Sie dann nach dem unten angezeigten Abschnitt, und ändern Sie die erste Zeile von

PasswordAuthentication no in **PasswordAuthentication yes**.

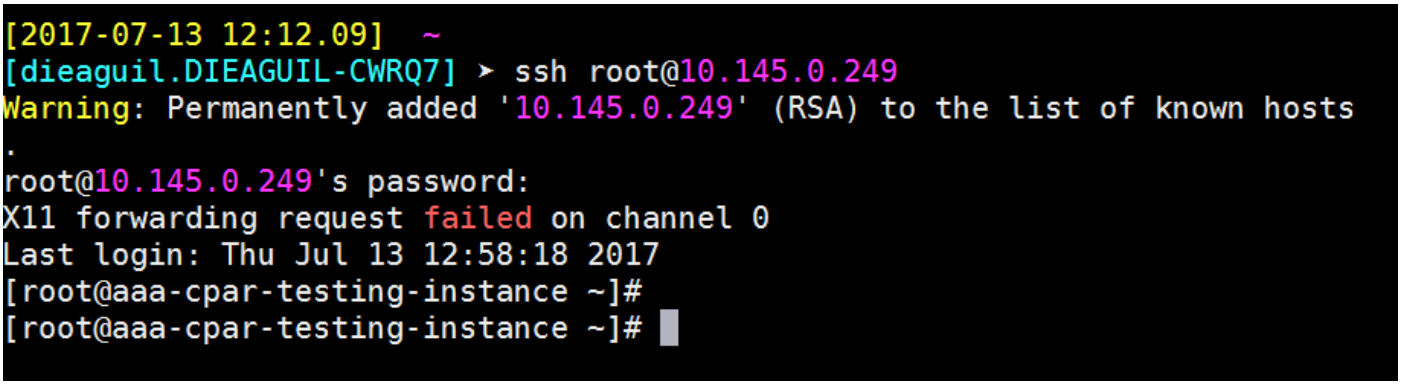


Schritt 7: Drücken Sie **ESC** und geben Sie **:wq!** um die Dateiänderungen sshd_config zu speichern.

Schritt 8: Führen Sie den Befehl service sshd restart aus.

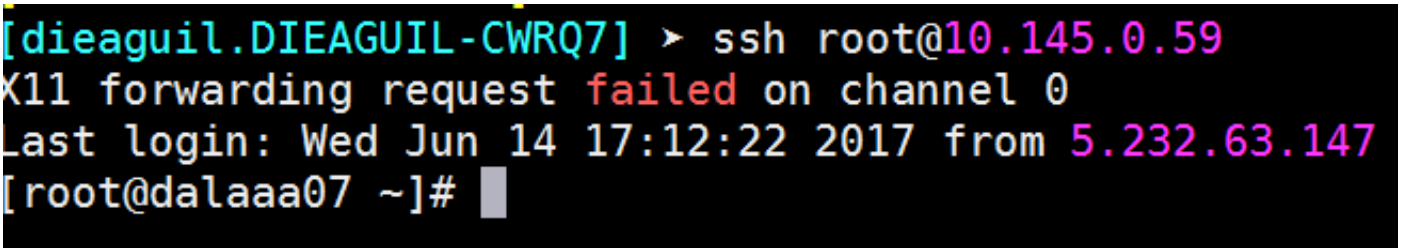


Schritt 9: Um die SSH-Konfigurationsänderungen ordnungsgemäß zu testen, öffnen Sie jeden SSH-Client, und versuchen Sie, eine sichere Remote-Verbindung **mithilfe der unverankerten IP** der Instanz (d. h. 10.145.0.249) und dem Benutzer-**Root** herzustellen.



Einrichten einer SSH-Sitzung

Öffnen Sie eine SSH-Sitzung mit der IP-Adresse des entsprechenden VM/Servers, auf dem die Anwendung installiert ist.



CPAR-Instanzstart

Bitte befolgen Sie die folgenden Schritte, sobald die Aktivität abgeschlossen ist und die CPAR-Services auf der heruntergefahrenen Website wiederhergestellt werden können.

1. Um sich wieder bei Horizon anzumelden, navigieren Sie zu **Project > Instance > Start Instance**.

2. Stellen Sie sicher, dass der Status der Instanz aktiv ist und der Stromversorgungszustand ausgeführt wird:

Statusprüfung nach Aktivität

Schritt 1: Führen Sie den Befehl **/opt/CSCOar/bin/arstatus** auf Betriebssystemebene aus.

```
[root@wscaaa04 ~]# /opt/CSCOar/bin/arstatus
Cisco Prime AR RADIUS server running       (pid: 24834)
Cisco Prime AR Server Agent running        (pid: 24821)
Cisco Prime AR MCD lock manager running    (pid: 24824)
Cisco Prime AR MCD server running          (pid: 24833)
Cisco Prime AR GUI running                 (pid: 24836)
SNMP Master Agent running                (pid: 24835)
[root@wscaaa04 ~]#
```

Schritt 2: Führen Sie den Befehl **/opt/CSCOar/bin/aregcmd** auf Betriebssystemebene aus, und geben Sie die Administratorberechtigungen ein. Stellen Sie sicher, dass CPAR Health 10 von 10 und die CPAR-CLI verlassen.

```
[root@aaa02 logs]# /opt/CSCOar/bin/aregcmd
Cisco Prime Access Registrar 7.3.0.1 Configuration Utility
Copyright (C) 1995-2017 by Cisco Systems, Inc.  All rights reserved.
Cluster:
User: admin
Passphrase:
Logging in to localhost
[ //localhost ]
      LicenseInfo = PAR-NG-TPS 7.2(100TPS:)

                    PAR-ADD-TPS 7.2(2000TPS:)

                    PAR-RDDR-TRX 7.2()

                    PAR-HSS 7.2()

    Radius/

    Administrators/
Server 'Radius' is Running, its health is 10 out of 10
--> exit
```

Schritt 3.Führen Sie den Befehl **netstat aus | grep-Durchmesser** und überprüfen, ob alle DRA-

Verbindungen hergestellt sind.

Die unten erwähnte Ausgabe ist für eine Umgebung vorgesehen, in der Durchmesser-Verbindungen erwartet werden. Wenn weniger Links angezeigt werden, stellt dies eine Trennung von DRA dar, die analysiert werden muss.

```
[root@aa02 logs]# netstat | grep diameter
tcp         0            0 aaa02.aaa.epc.:77 mp1.dra01.d:diameter ESTABLISHED
tcp         0            0 aaa02.aaa.epc.:36 tsa6.dra01:diameter ESTABLISHED
tcp         0            0 aaa02.aaa.epc.:47 mp2.dra01.d:diameter ESTABLISHED
tcp         0            0 aaa02.aaa.epc.:07 tsa5.dra01:diameter ESTABLISHED
tcp         0            0 aaa02.aaa.epc.:08 np2.dra01.d:diameter ESTABLISHED
```

Schritt 4: Überprüfen Sie, ob das TPS-Protokoll Anforderungen anzeigt, die von CPAR verarbeitet werden. Die hervorgehobenen Werte repräsentieren den TPS, und genau diese Werte müssen wir beachten.

Der TPS-Wert darf 1500 nicht überschreiten.

```
[root@wscaaa04 ~]# tail -f /opt/CSCOar/logs/tps-11-21-2017.csv
11-21-2017,23:57:35,263,0
11-21-2017,23:57:50,237,0
11-21-2017,23:58:05,237,0
11-21-2017,23:58:20,257,0
11-21-2017,23:58:35,254,0
11-21-2017,23:58:50,248,0
11-21-2017,23:59:05,272,0
11-21-2017,23:59:20,243,0
11-21-2017,23:59:35,244,0
11-21-2017,23:59:50,233,0
```

Schritt 5: Suchen Sie nach "error"- oder "alarm"-Meldungen in name_radius_1_log.

```
[root@aaa02 logs]# grep -E "error|alarm" name_radius_1_log
```

Schritt 6.Überprüfen Sie mithilfe des folgenden Befehls, wie viel Speicher der CPAR-Prozess beansprucht:

oberste | grep Radius

```
[root@sfraaa02 ~]# top | grep radius
27008 root      20   0 20.228g 2.413g  11408 S 128.3  7.7   1165:41 radius
```

Der hervorgehobene Wert sollte kleiner sein als: 7 Gb, d. h. der maximal zulässige Wert auf Anwendungsebene.