Hauptplatinenaustausch im Ultra-M UCS 240M4 Server - CPAR

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte, die erforderlich sind, um die fehlerhafte Hauptplatine eines Servers in einer Ultra-M-Konfiguration zu ersetzen.

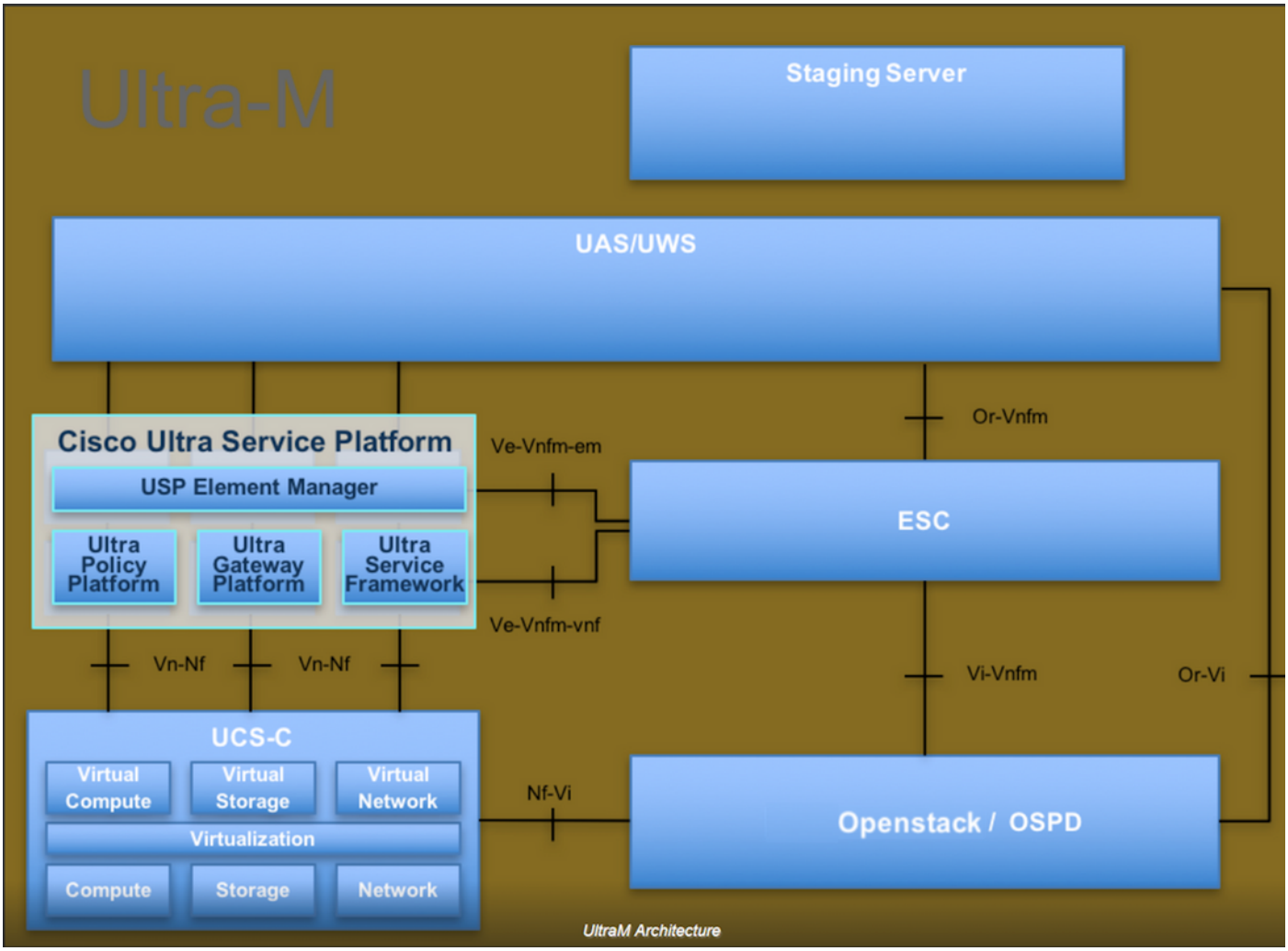
Dieses Verfahren gilt für eine OpenStack-Umgebung, in der die NEWTON-Version verwendet wird, in der CPAR von ESC nicht verwaltet wird und CPAR direkt auf dem auf OpenStack bereitgestellten virtuellen System installiert wird.

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:



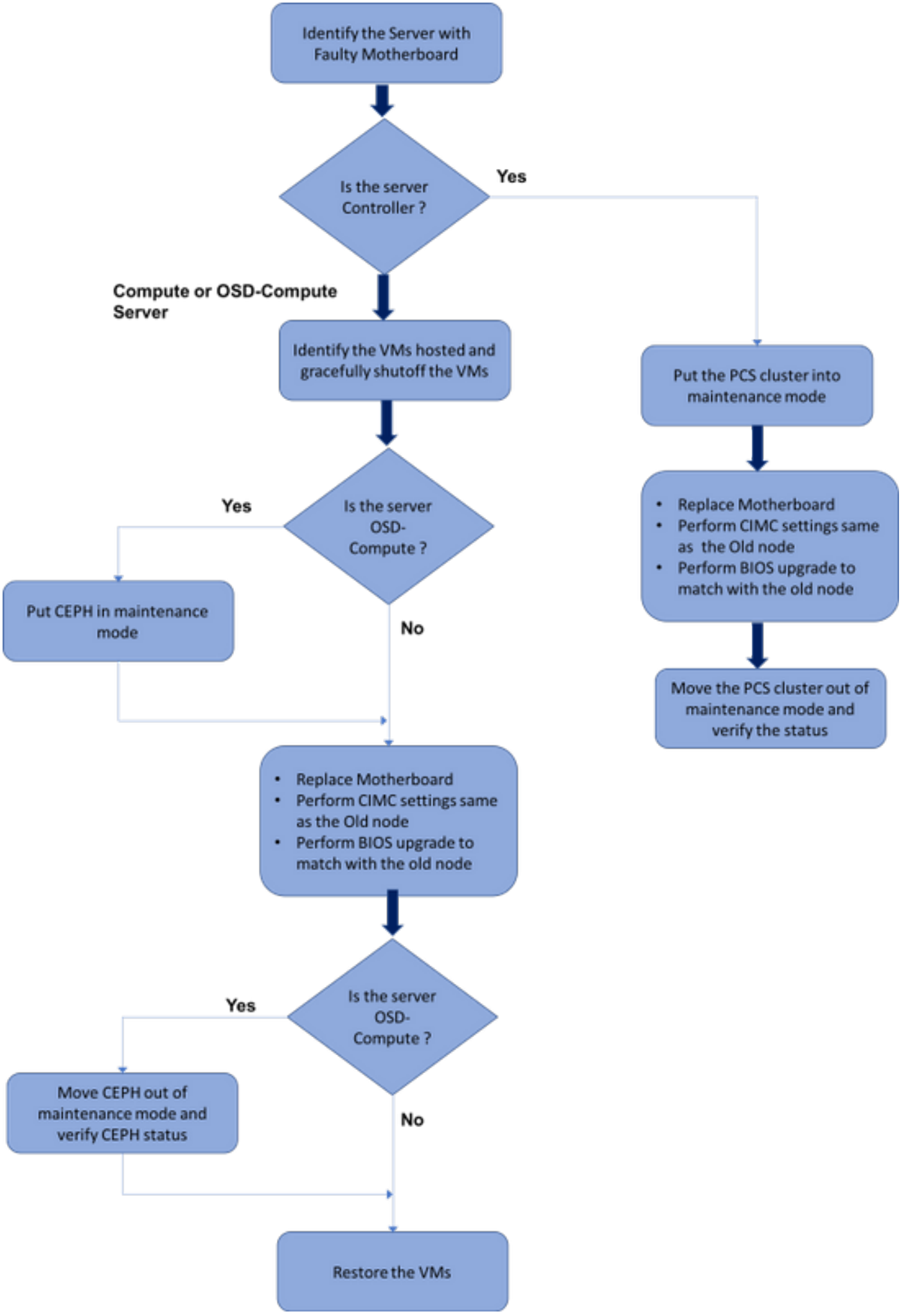
Dieses Dokument richtet sich an Mitarbeiter von Cisco, die mit der Cisco Ultra-M-Plattform vertraut sind. Es beschreibt die Schritte, die bei OpenStack und Redhat OS ausgeführt werden müssen.

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


Identify the Server with Faulty Motherboard
Is the server Controller ?
Yes
Compute or OSD-Compute Server
Identify the VMs hosted and gracefully shutoff the VMs
Is the server OSD-Compute ?
Yes
Put CEPH in maintenance mode
No
Replace Motherboard
Perform CIMC settings same as the Old node
Perform BIOS upgrade to match with the old node
Is the server OSD-Compute ?
Yes
Move CEPH out of maintenance mode and verify CEPH status
No
Restore the VMs
Put the PCS cluster into maintenance mode
Replace Motherboard
Perform CIMC settings same as the Old node
Perform BIOS upgrade to match with the old node
Move the PCS cluster out of maintenance mode and verify the status

Austausch der Hauptplatine im Ultra-M-Setup

In einer Ultra-M-Konfiguration kann es Szenarien geben, in denen ein Austausch der Hauptplatine für die folgenden Servertypen erforderlich ist: Computing, OSD-Computing und Controller.

> **Hinweis**: Die Boot-Laufwerke mit der OpenStack-Installation werden nach dem Austausch der Hauptplatine ersetzt. Daher ist es nicht erforderlich, den Knoten wieder zur Cloud hinzuzufügen. Sobald der Server nach der Ersetzung eingeschaltet wurde, meldet er sich wieder beim Overcloud-Stack an.

Voraussetzungen

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@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.

> **Hinweis**: Vergewissern Sie sich, dass Sie den Snapshot der Instanz zur Hand haben, damit Sie das virtuelle System bei Bedarf wiederherstellen können. Befolgen Sie dieses Verfahren, um einen Snapshot des VM zu erstellen.

Austausch des Motherboards im Computing-Knoten

Vor der Aktivität werden die im Knoten Compute gehosteten VMs ordnungsgemäß heruntergefahren. Nachdem die Hauptplatine ausgetauscht wurde, werden die VMs wiederhergestellt.

Identifizieren der im Compute-Knoten gehosteten VMs

```
[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 nachfolgenden Abschnitten verwendet.

Sicherung: Snapshot-Prozess

Schritt 1: Herunterfahren der CPAR-Anwendung.

Schritt 1: Öffnen Sie alle SSH-Clients, die mit dem Netzwerk verbunden sind, 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

A Message stating “Cisco Prime Access Registrar Server Agent shutdown complete.” Should show up
```

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. Falls dies der Fall ist, beenden Sie diesen Vorgang mit dem folgenden Befehl:

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

Wiederholen Sie anschließend Schritt 1.

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

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

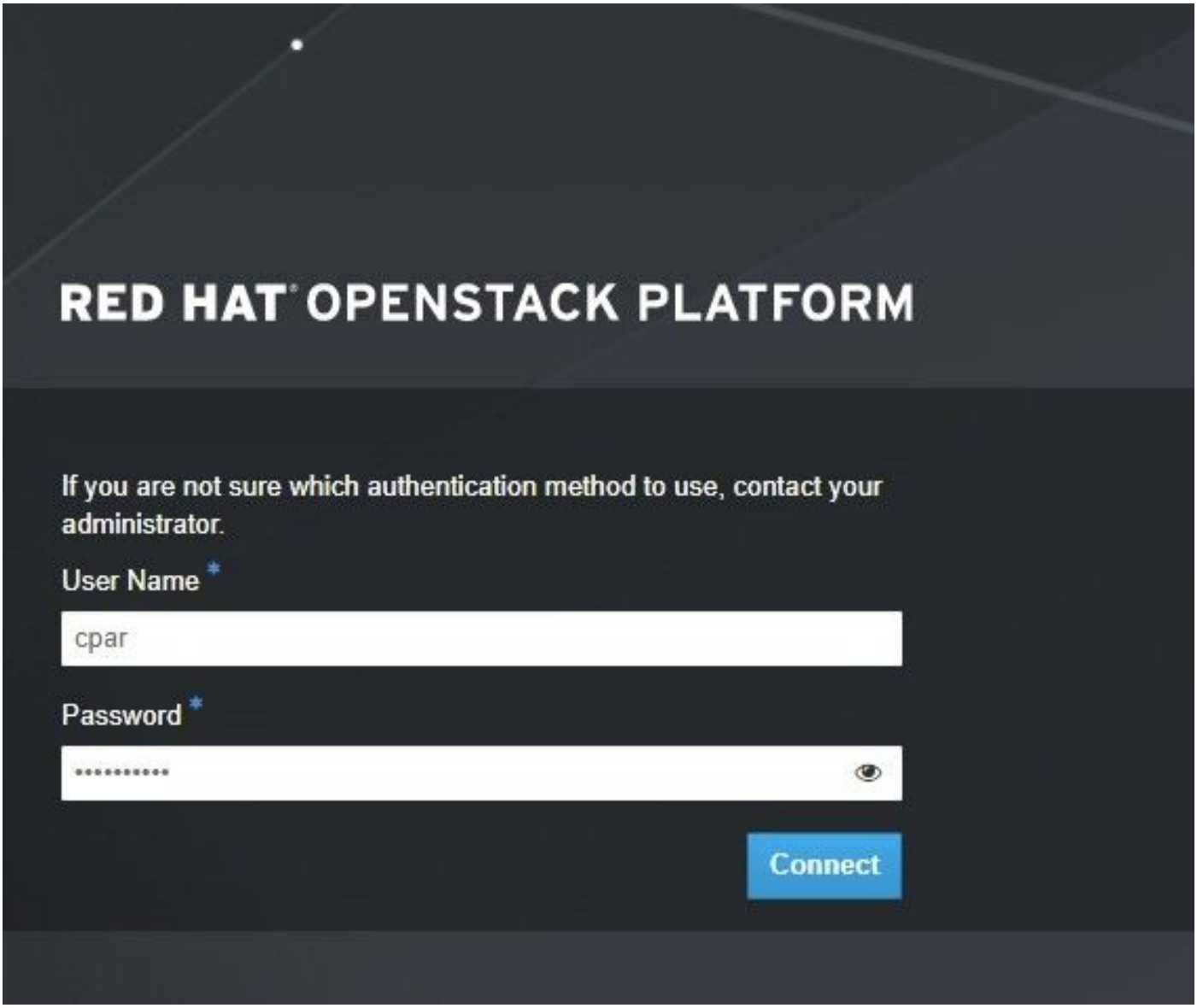
Diese Meldungen sollten angezeigt werden:

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

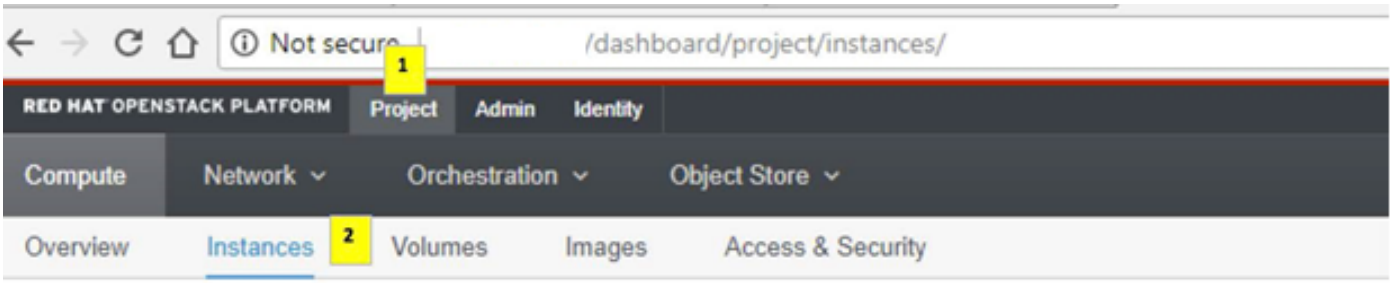
VM-Snapshot-Aufgabe

Schritt 1:Geben Sie die Horizon GUI-Website ein, die der aktuell bearbeiteten Website (Stadt) entspricht.

Beim Zugriff auf Horizon wird dieser Bildschirm angezeigt:



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



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. 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 heruntergefahren wurde, indem Sie Status = Shutoff und Power State = Shut Down (Status abschalten) überprüfen.

Mit diesem Schritt wird der CPAR-Abschaltvorgang beendet.

VM-Snapshot

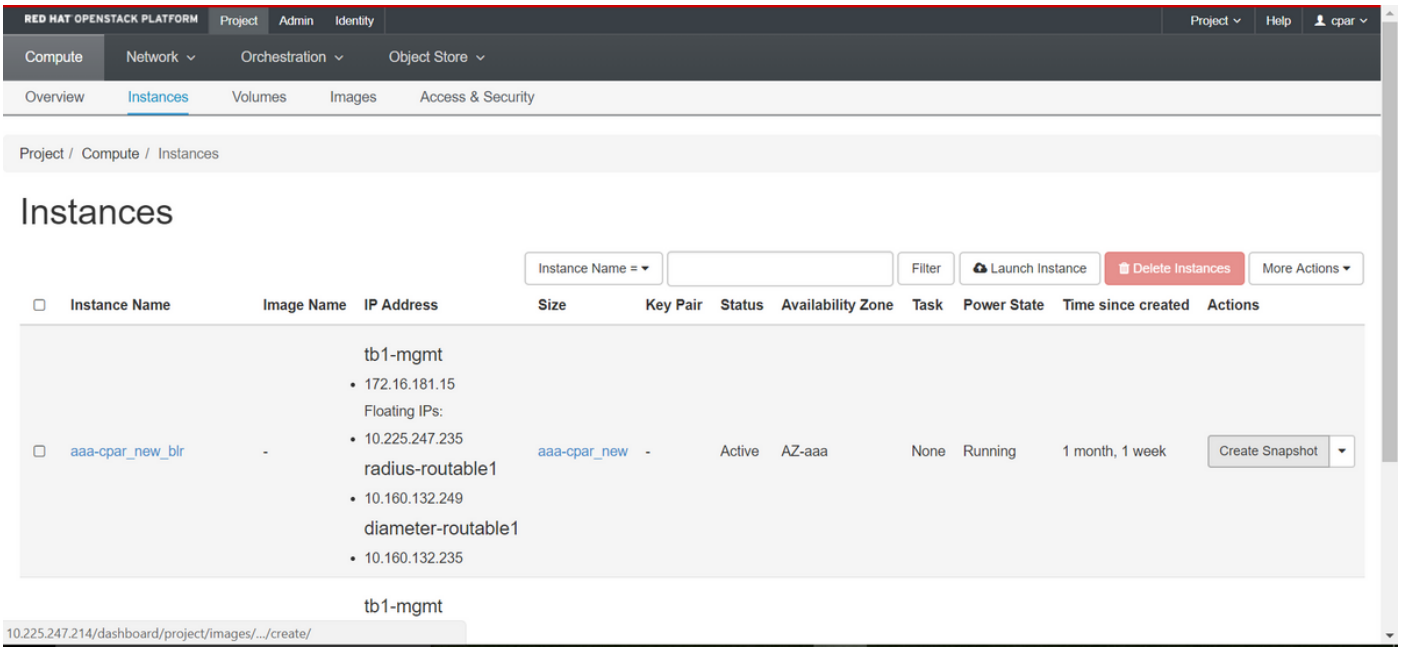
Sobald die CPAR-VMs ausfallen, können die Snapshots parallel erstellt werden, da sie zu unabhängigen Berechnungen gehören.

Die vier QCOW2-Dateien werden parallel erstellt.

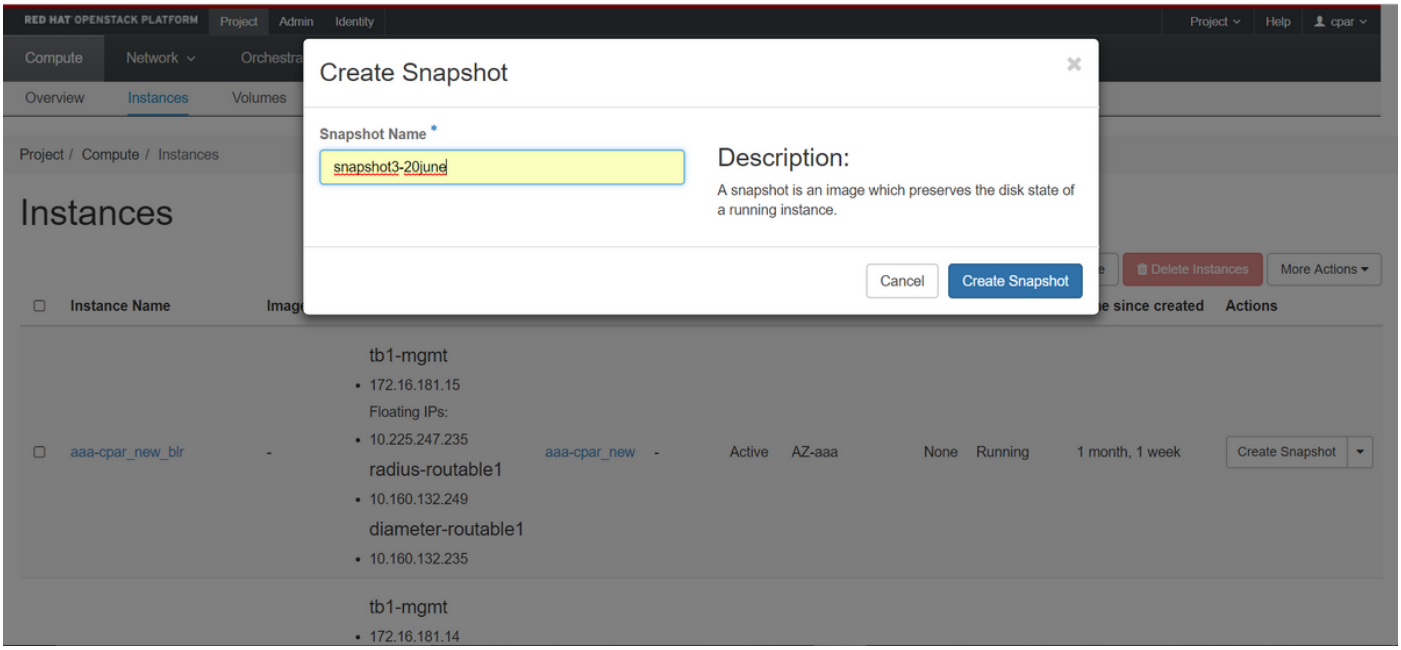
Erstellen eines Snapshots jeder AAA-Instanz (25 Minuten bis 1 Stunde) (25 Minuten für Instanzen, die ein qcow-Image als Quelle und 1 Stunde für Instanzen verwenden, die ein Rohbild als Quelle verwenden)

Schritt 1: Anmeldung bei OpenStack Horizon des POD**Benutzeroberfläche.**

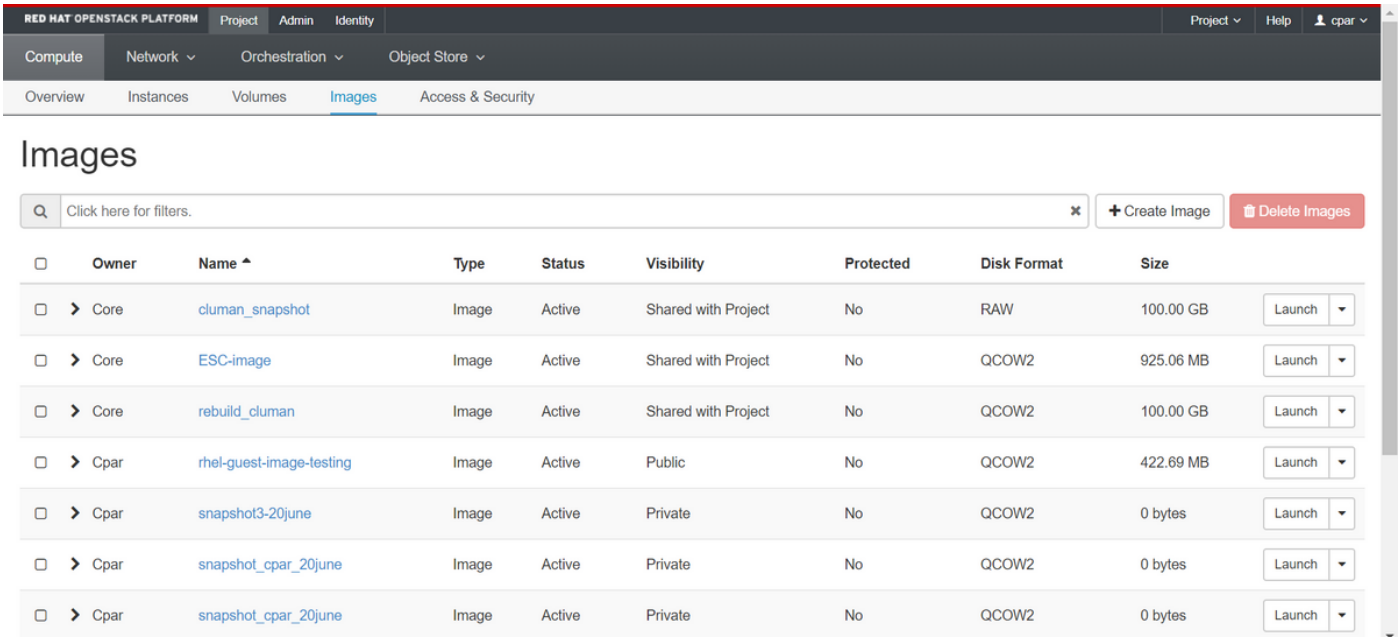
Schritt 2: Wenn Sie sich angemeldet haben, gehen Sie im oberen Menü zum Abschnitt **Projekt > Computing > Instanzen** und suchen Sie nach den AAA-Instanzen.



Schritt 3: Klicken Sie auf die Schaltfläche **Create Snapshot** (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 IMAGES-Menü, und überprüfen Sie, ob alle fertig gestellt sind, 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 mit diesem Befehl **Glance image-list** 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 herunterzuladende Snapshot identifiziert wurde (in diesem Fall ist der Snapshot in grün markiert), laden Sie ihn in einem QCOW2-Format mit dem Befehl **glance image-download** 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 wird einige Zeit dauern, 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, damit der Prozess im Falle einer SSH-Verbindung trotzdem ausgeführt wird und im OSPD abgeschlossen ist.

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, ist eine Überprüfung der Dateiintegrität erforderlich. Führen Sie den nächsten Befehl aus, und suchen Sie am Ende der Ausgabe nach dem Attribut "beschädigt".

```
[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, den Befehl "*df -kh"* verwenden, um den Speicherplatz zu überprüfen. Wir empfehlen, die Datei temporär mithilfe von SFTP "sftproot@x.x.x.x" in das OSPD einer anderen Website zu übertragen, wobei x.x.x.x die IP-Adresse einer Remote-OSPD ist. Um die Übertragung zu beschleunigen, kann das Ziel an mehrere OSPDs gesendet werden. Auf dieselbe Weise können wir den folgenden Befehl verwenden: scp *name_of_the_file*.qcow2 root@ x.x.x.x:/tmp (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 wird der Instanzname mit dem Status Shutoff angezeigt.

```
[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                 |

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

Hauptplatine ersetzen

Die Schritte zum Ersetzen des Motherboards in einem UCS C240 M4 Server können im Cisco UCS C240 M4 Server Installations- und Serviceleitfaden beschrieben werden.

1. Melden Sie sich mit der CIMC IP-Adresse beim Server an.

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

Stellen Sie die VMs wieder her

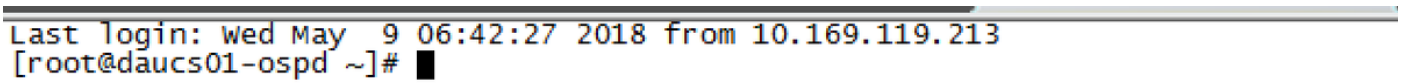
Wiederherstellen einer Instanz durch Snapshot

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. Verwenden von "sftproot@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.



Rufen Sie die Umgebungsvariablen mit dem folgenden Befehl auf:

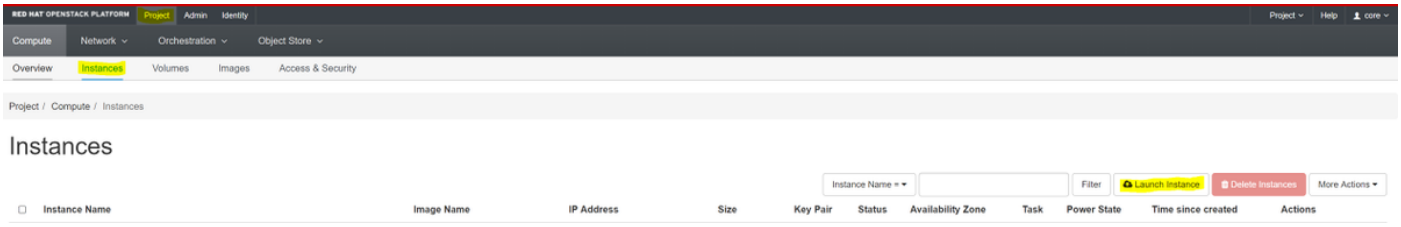
```
# source /home/stack/pod1-stackrc-Core-CPAR
```

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

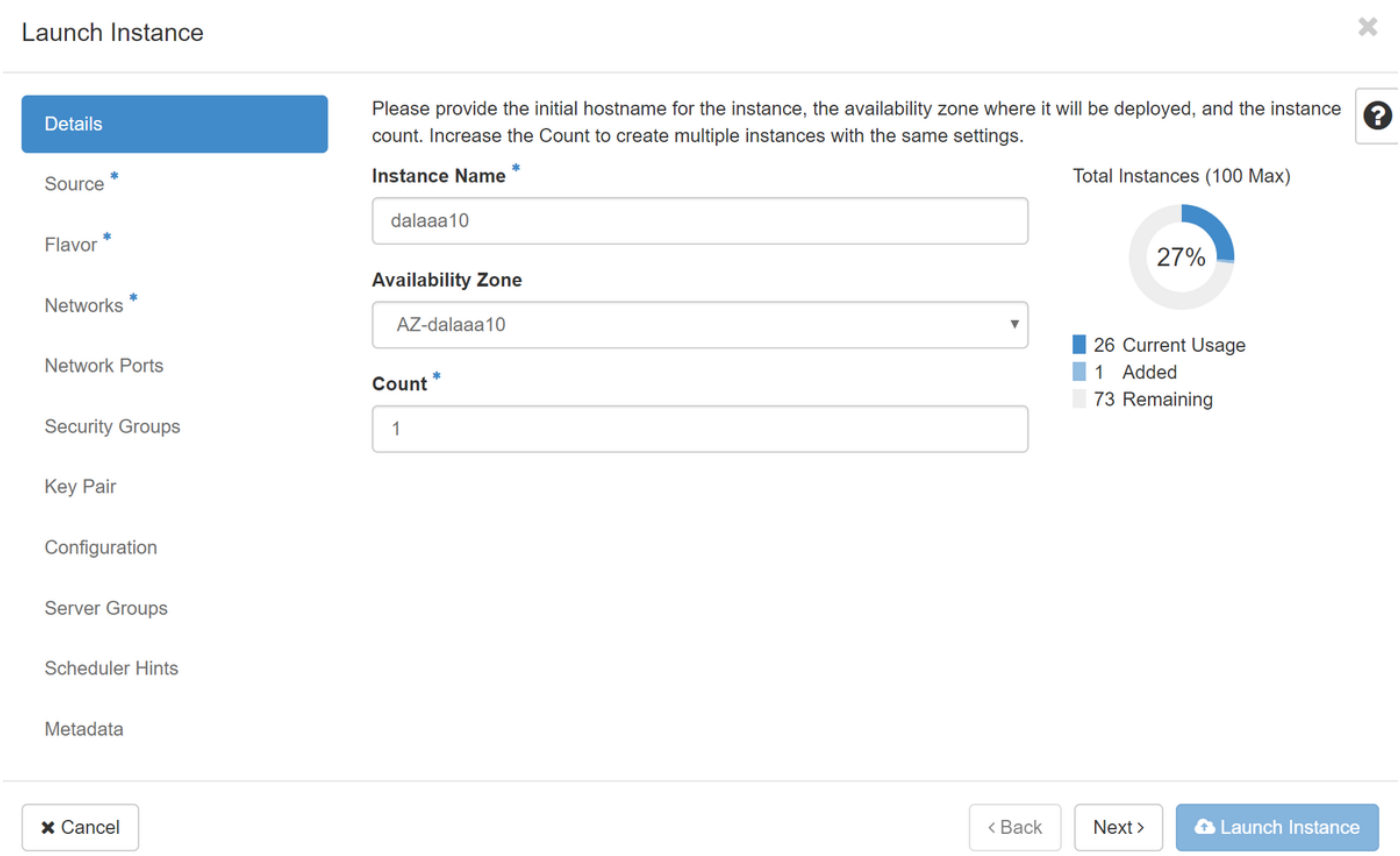
```
#glance image-create -- AAA-CPAR-Date-snapshot.qcow2 --container-format bare --disk-format qcow2
--name AAA-CPAR-Date-snapshot
```

Der Prozess ist am Horizont erkennbar.

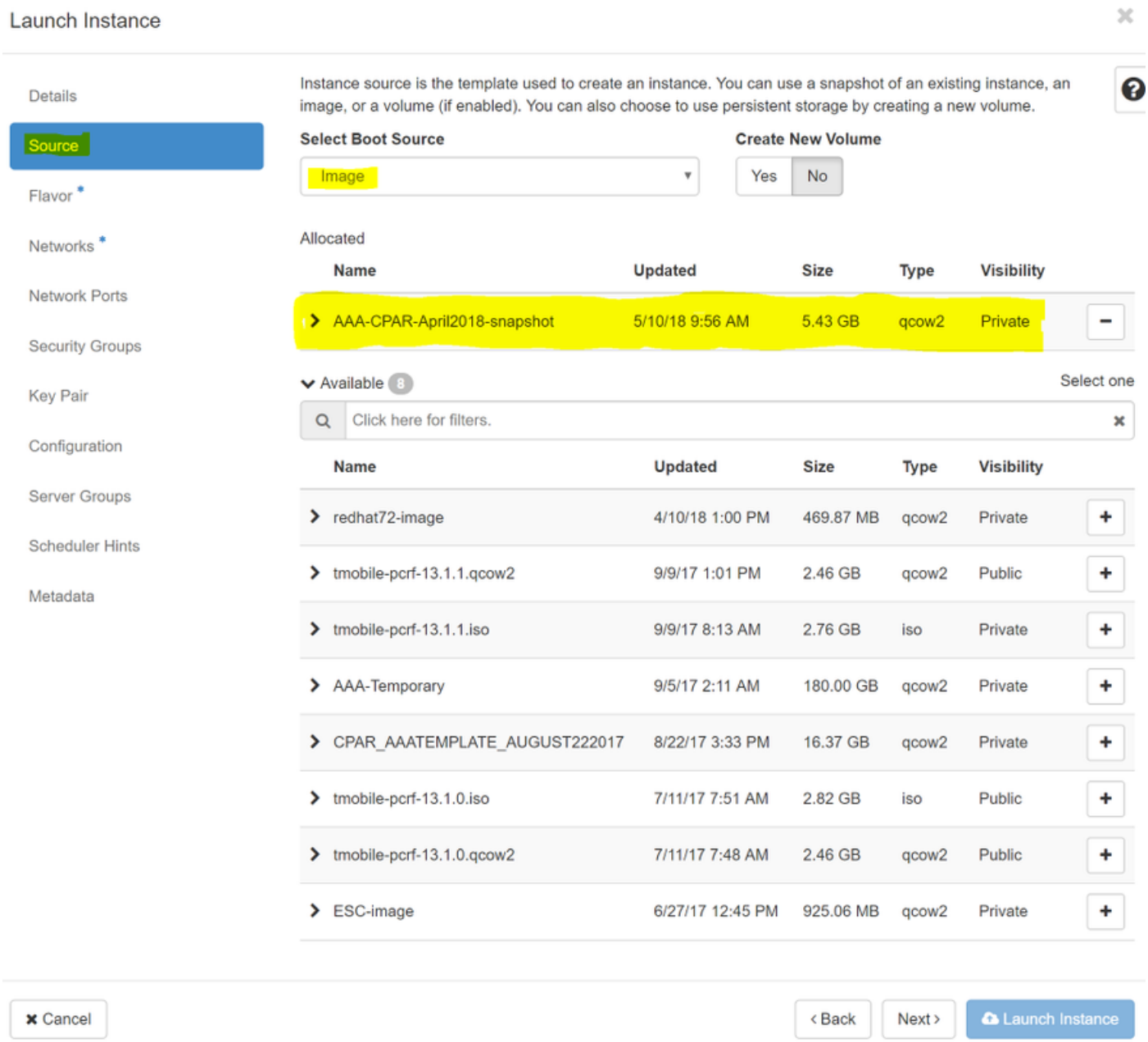
Schritt 4:Navigieren Sie in Horizon zu **Projekt > Instanzen**, und klicken Sie auf **Instanz starten**.



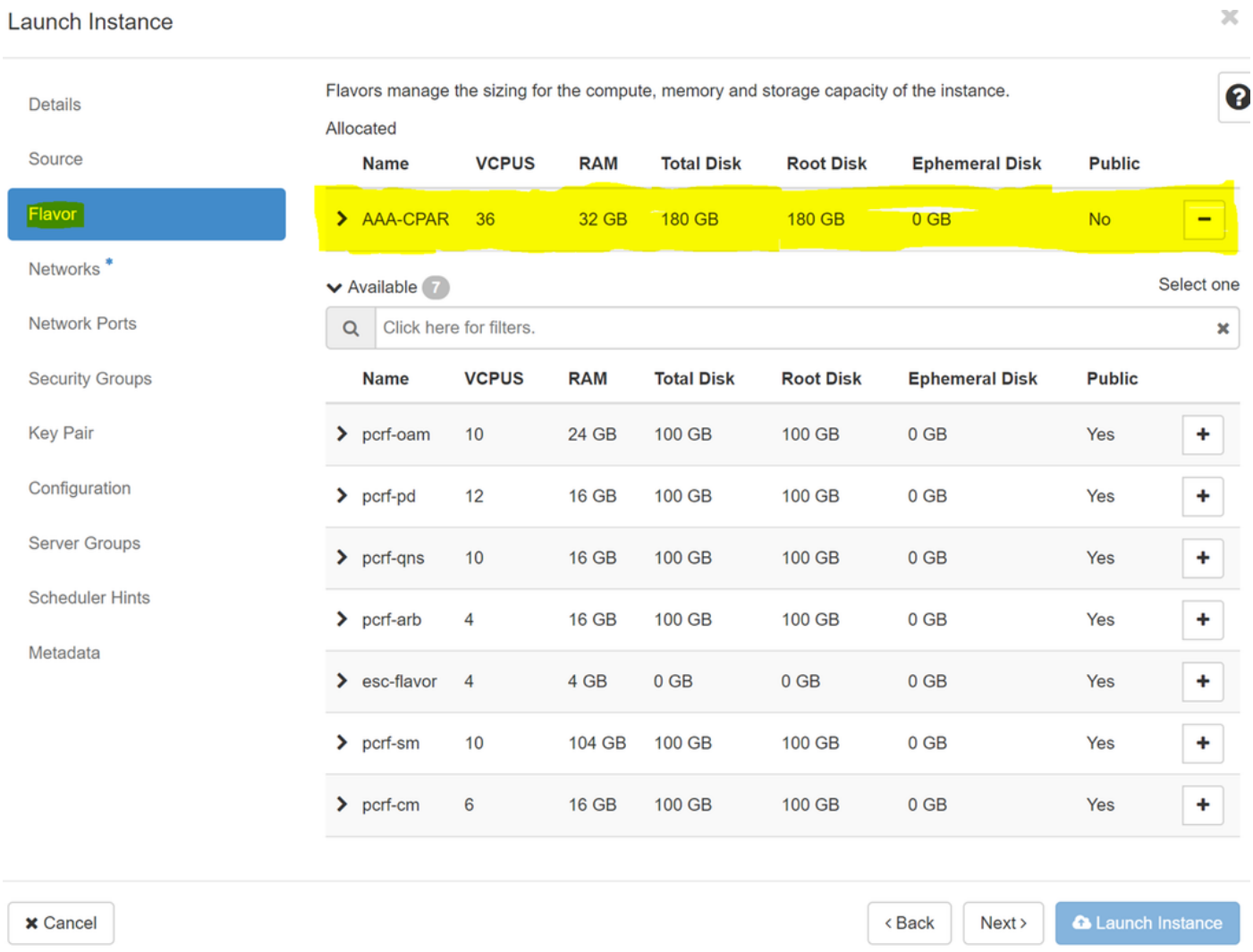
Schritt 5:Geben Sie den Instanznamen ein, und wählen Sie die Verfügbarkeitszone aus.



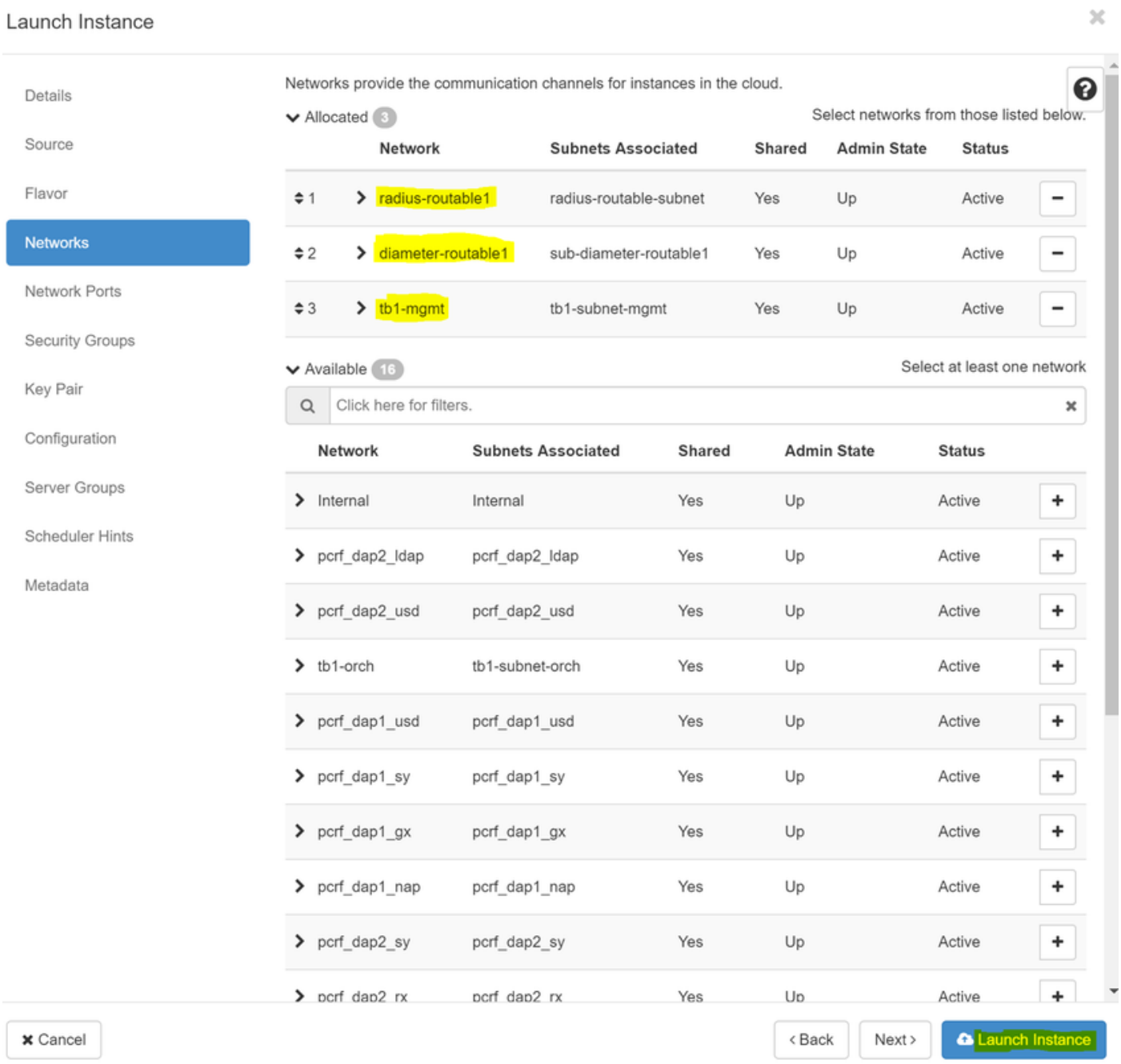
Schritt 6:Wählen Sie auf der Registerkarte **Quelle** das Bild aus, um die Instanz zu erstellen. Wählen Sie im Menü Select Boot Source (Startquelle auswählen) **Image (Bild** auswählen) aus. Hier wird eine Liste mit Bildern angezeigt. Wählen Sie das zuvor hochgeladene Image aus, während Sie auf **+**Zeichen klicken.



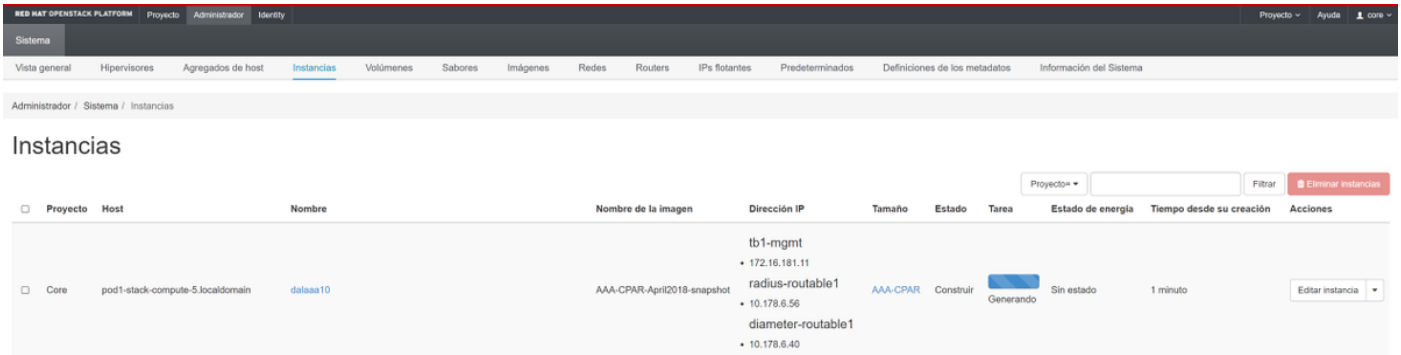
Schritt 7:Wählen Sie auf der Registerkarte Flavor die AAA-Variante aus, während Sie auf **+** klicken.



Schritt 8: Navigieren Sie schließlich zur Registerkarte Netzwerk, und wählen Sie die Netzwerke aus, die die Instanz benötigt, wenn Sie auf **+** klicken. Wählen Sie in diesem Fall **durchmesser-soutable1**, **radius-routing1** und **tb1-mgmt aus**.



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



Nach einigen Minuten ist die Instanz vollständig bereitgestellt und einsatzbereit.

Erstellen und Zuweisen einer Floating-IP-Adresse

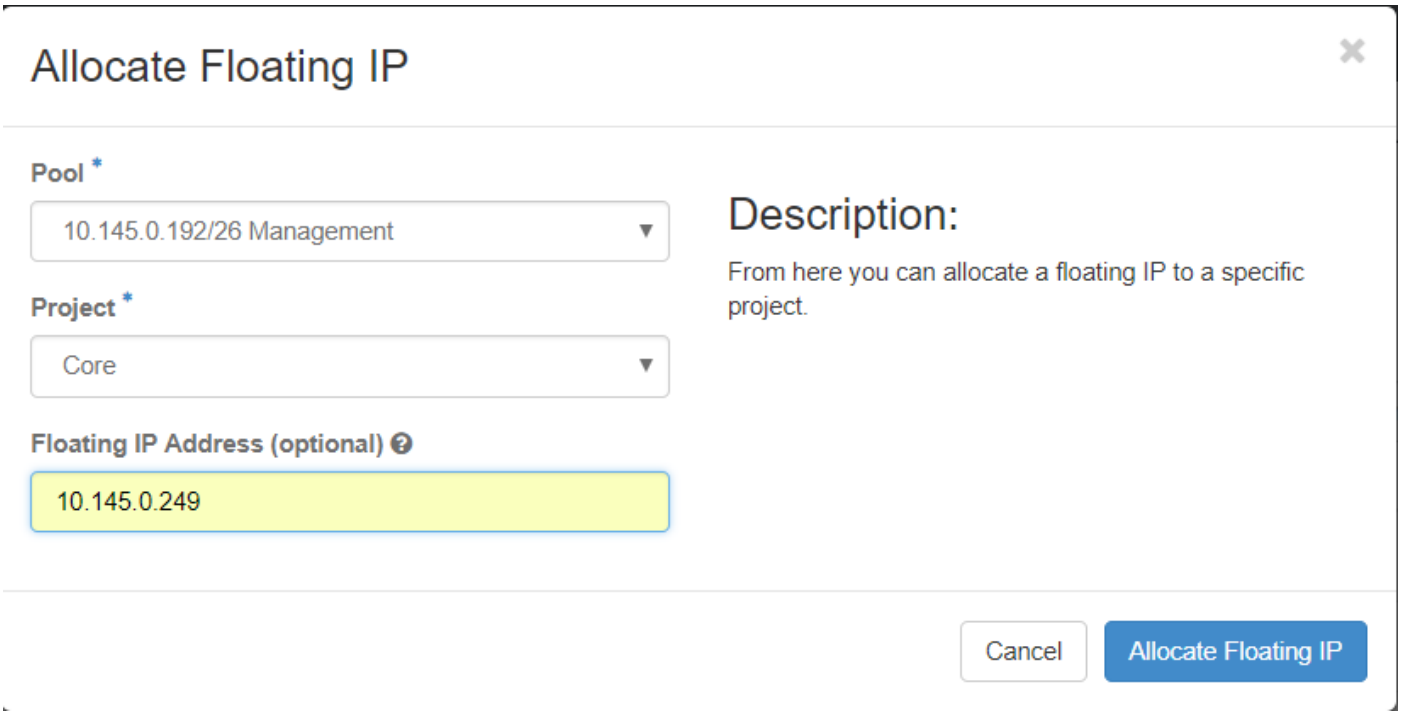
Eine Floating-IP-Adresse ist eine routbare Adresse, d. h. sie ist von der Außenseite der Ultra M/OpenStack-Architektur aus erreichbar und kann mit anderen Knoten aus dem Netzwerk kommunizieren.

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

Schritt 2: Klicken Sie auf die **SchaltflächeAllocationsIP to Project**.

Schritt 3: Wählen Sie **im** Fenster **Zuweisen von Floating** IP (Floating-IP-Adresse zuweisen) den Poolbereich aus, aus dem die neue Floating-IP-Adresse gehört, das Projekt, dem sie zugewiesen wird, und die **neue Floating-IP-**Adresse selbst.

Beispiel:

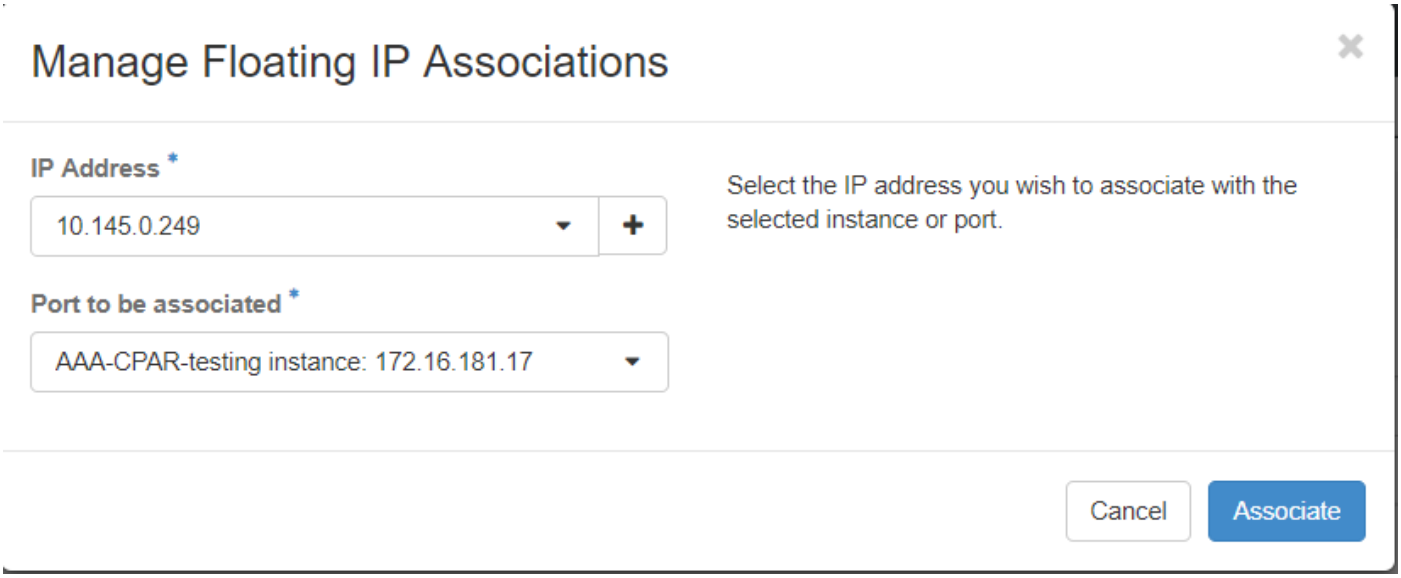


Schritt 4.Klicken Sie auf **AllocationsFloating** IPbutton.

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

Schritt 6:Klicken Sie in derSpalte Aktion auf den Pfeil, der in **der** Schaltfläche Snapshot erstellen nach unten zeigt, um ein Menü anzuzeigen. **Wählen SieFloating-**IP-Option **Zuordnen** aus.

Schritt 7: Wählen Sie die entsprechende unverankerte IP-Adresse aus, **die** im IP-Adressenfeld verwendet werden soll, und wählen Sie die entsprechende Verwaltungsschnittstelle (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 abschließend auf Associatebutton.

Aktivieren von SSH

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

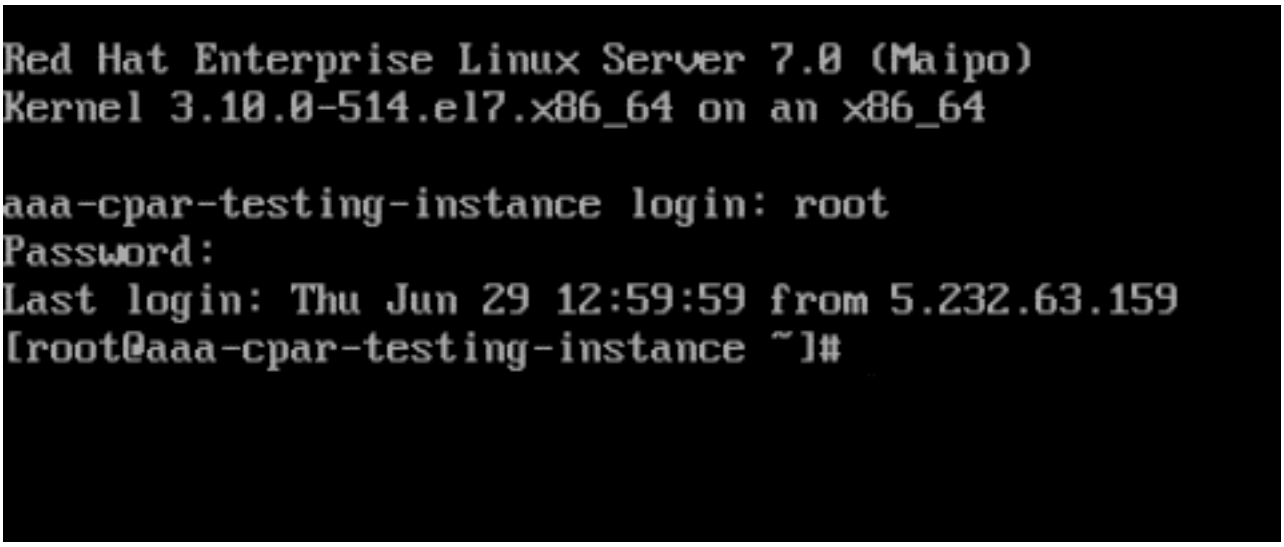
Schritt 2:Klicken Sie auf den Namen der im **AbschnittLunch einer neuen Instanz** erstellten Instanz/VM.

Schritt 3: Klicken Sie auf Consoletab. Dadurch wird die Befehlszeilenschnittstelle des virtuellen Systems angezeigt.

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

Benutzername: **root**

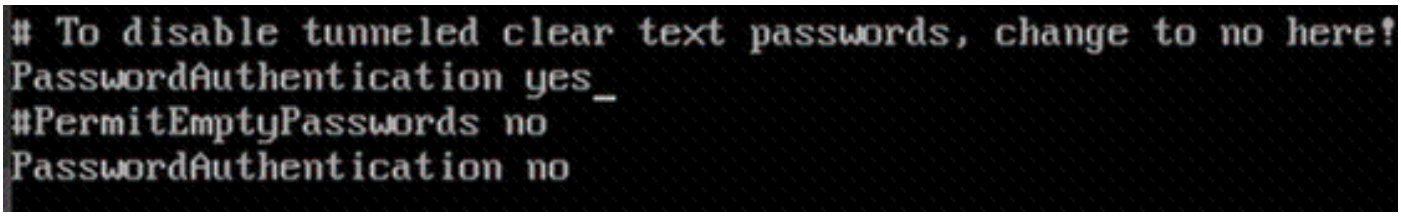
Kennwort: **cisco123**



Schritt 5:Geben Sie in der CLI den Befehl /etc/ssh/sshd_configein, um die SSH-Konfiguration zu bearbeiten.

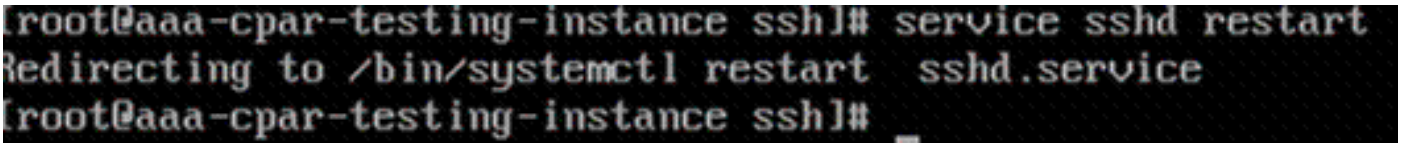
Schritt 6: Wenn die ssh-Konfigurationsdatei geöffnet ist, drücken Sie die Eingabetaste, um die

Datei zu bearbeiten. Suchen Sie dann nach dem unten angezeigten Abschnitt, und ändern Sie die erste Zeile **vonPasswordAuthentication notoPasswordAuthentication yes**.

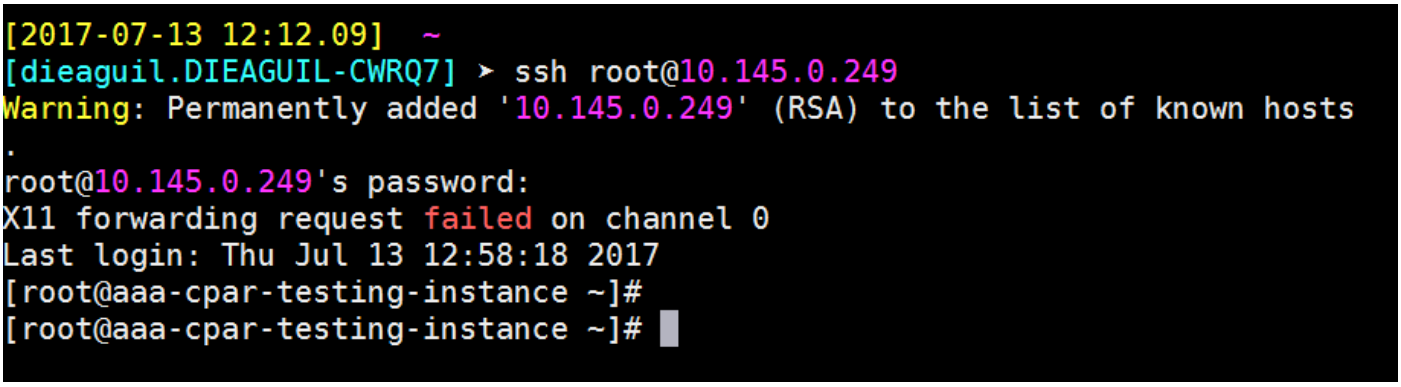


Schritt 7:Drücken Sie ESC, und geben Sie**:wq!**ein, um die Dateiänderungen sshd_config zu speichern.

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

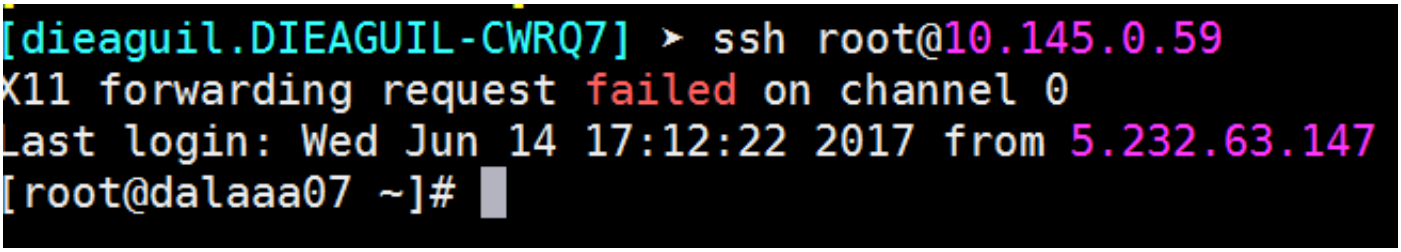


Schritt 9.Um die SSH-Konfigurationsänderungen zu testen, öffnen Sie jeden SSH-Client, und versuchen Sie, eine sichere Remote-**Verbindung** herzustellen, **indem Sie die** der Instanz (d. h. 10.145.0.249) und dem **Benutzer** zugewiesene unverankerte IP **verwenden**.



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 **Projekt > Instanz > 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@aaa04 ~]# /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 die Speicherkapazität, die der CPAR-Prozess verwendet, indem Sie den folgenden Befehl eingeben:

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.

Hauptplatinenaustausch im OSD-Computing-Knoten

Vor der Aktivität werden die im Knoten Compute gehosteten VMs ordnungsgemäß heruntergefahren und in den Wartungsmodus versetzt. Nachdem die Hauptplatine ausgetauscht wurde, werden die VMs wiederhergestellt und CEPH aus dem Wartungsmodus entfernt.

Identifizieren der im Osd-Compute-Knoten gehosteten VMs

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

```
[stack@director ~]$ nova list --field name,host | grep osd-compute-0
| 46b4b9eb-a1a6-425d-b886-a0ba760e6114 | AAA-CPAR-testing-instance | pod2-stack-compute-
4.localdomain |
```

Sicherung: Snapshot-Prozess

Herunterfahren der CPAR-Anwendung

Schritt 1: Öffnen Sie alle SSH-Clients, die mit dem Netzwerk verbunden sind, 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

A Message stating “Cisco Prime Access Registrar Server Agent shutdown complete.” Should show up
```

> **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. Falls dies der Fall ist, beenden Sie diesen Vorgang mit dem folgenden Befehl:

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

Wiederholen Sie anschließend Schritt 1.

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

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

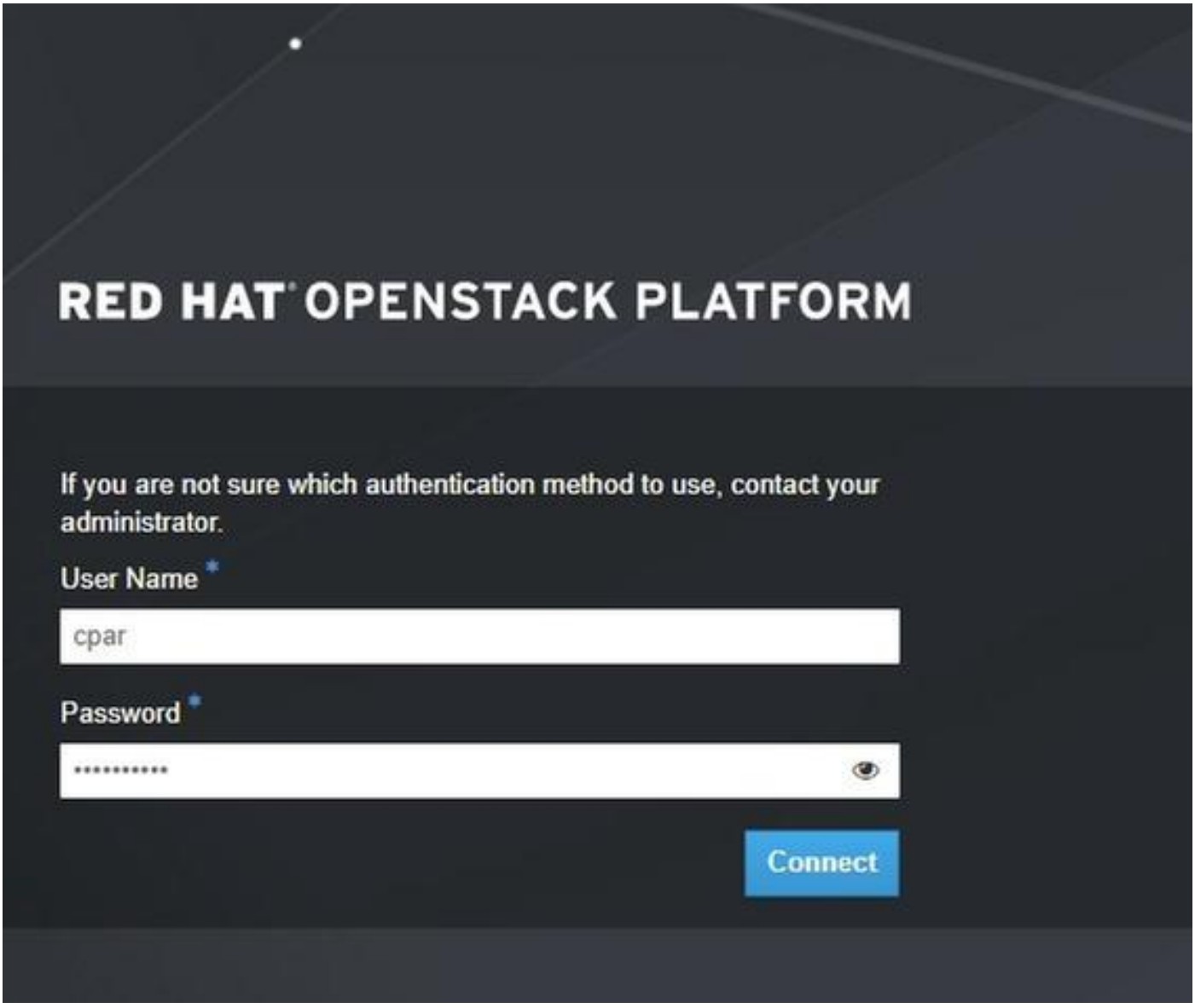
Diese Meldungen werden angezeigt:

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

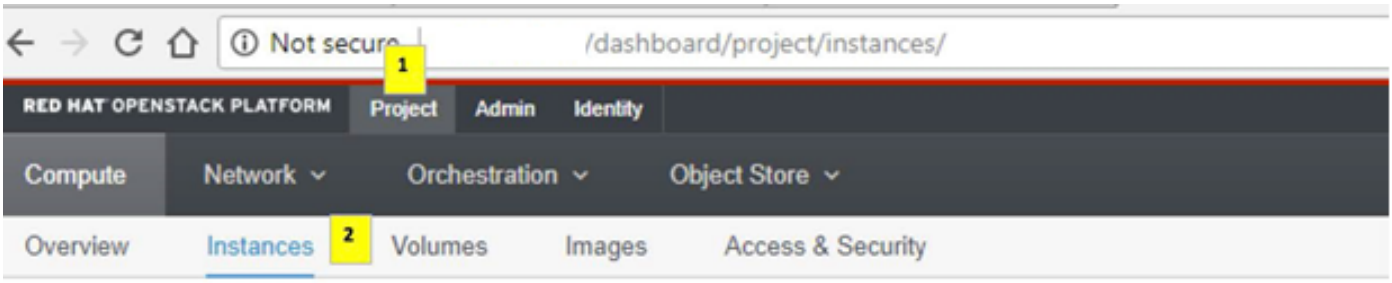
VM-Snapshot-Aufgabe

Schritt 1:Geben Sie die Horizon GUI-Website ein, die der aktuell bearbeiteten Website (Stadt) entspricht.

Beim Zugriff auf Horizon wird das abgebildete Bild beobachtet:



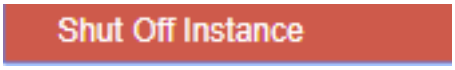
Schritt 2: Navigieren Sie zu **Projekt > Instanzen**, wie im Bild gezeigt.



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. Wiederholen Sie den gesamten Vorgang in diesem Dokument.

Um das virtuelle System herunterzufahren, navigieren Sie zu **Aktionen > Instanz abschalten** und bestätigen Sie Ihre Auswahl.



Schritt 4:Überprüfen Sie, ob die Instanz tatsächlich heruntergefahren wurde, indem Sie Status = Shutoff und Power State = Shut Down (Status abschalten) überprüfen.

Mit diesem Schritt wird der CPAR-Abschaltvorgang beendet.

VM-Snapshot

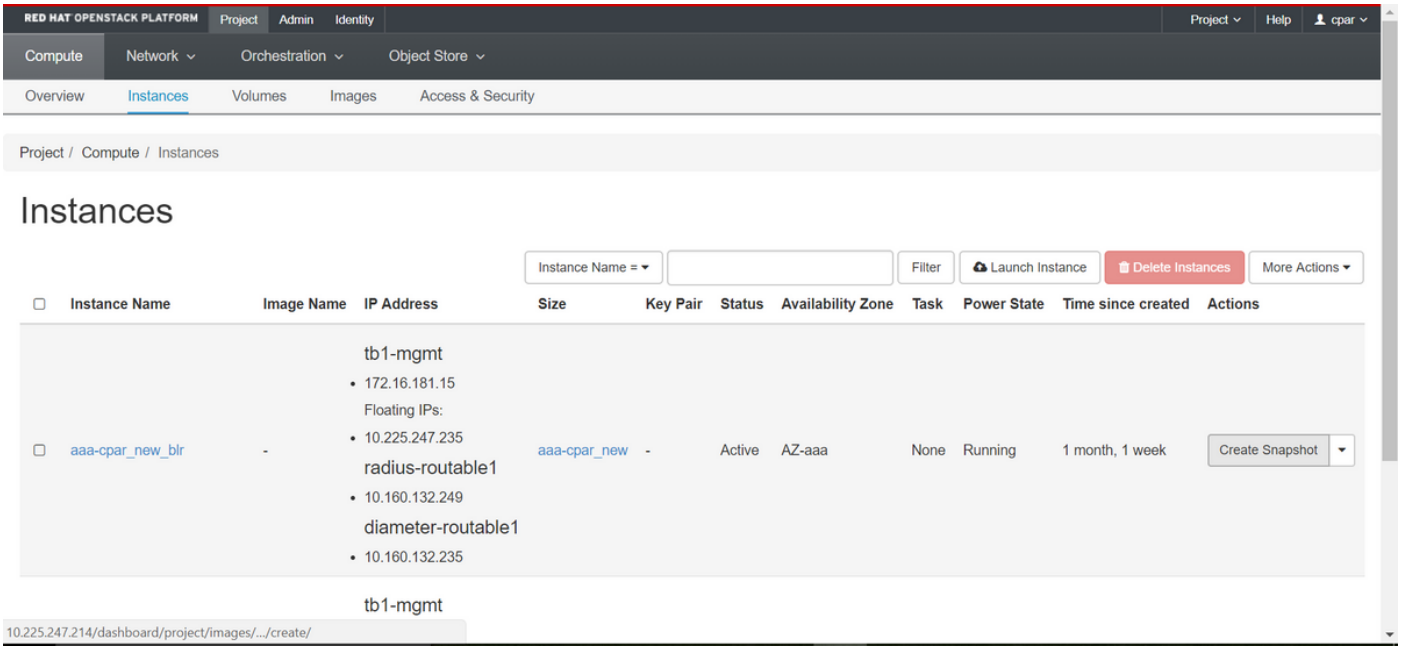
Sobald die CPAR-VMs ausfallen, können die Snapshots parallel erstellt werden, da sie zu unabhängigen Berechnungen gehören.

Die vier QCOW2-Dateien werden parallel erstellt.

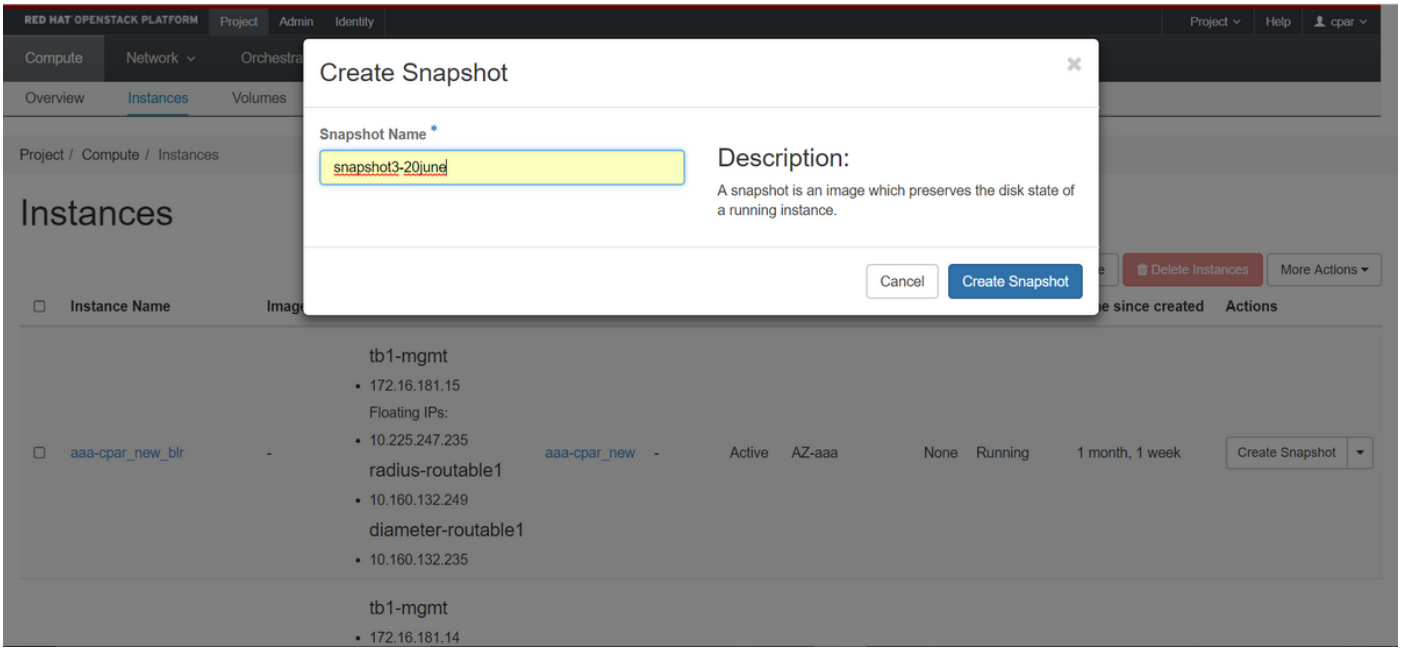
Erstellen Sie einen Snapshot jeder AAA-Instanz (25 Minuten bis 1 Stunde) (25 Minuten für Instanzen, die ein qcow-Image als Quelle und 1 Stunde für Instanzen verwenden, die ein Rohbild als Quelle verwenden)

Schritt 1: Melden Sie sich bei der **HorizonGUI** der POD OpenStack an.

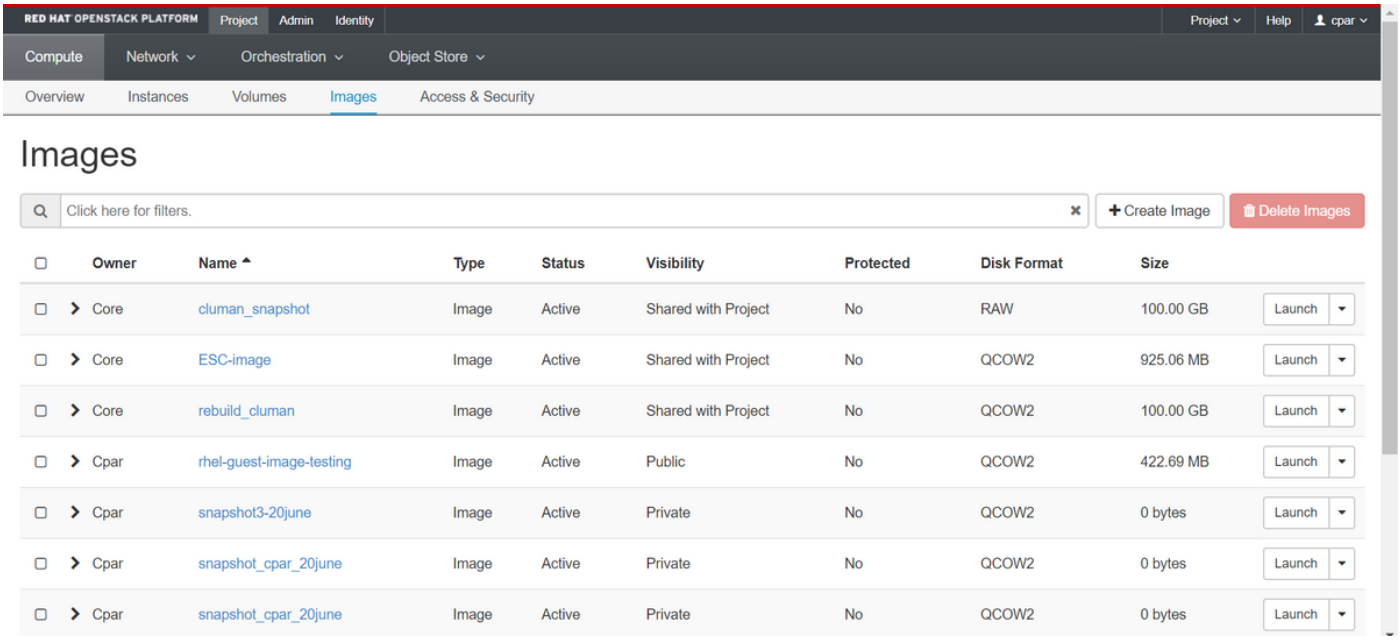
Schritt 2: Wenn Sie sich angemeldet haben, gehen Sie im oberen Menü zum Abschnitt **Projekt > Computing > Instanzen** und suchen Sie nach den AAA-Instanzen.



Schritt 3: Klicken Sie auf die Schaltfläche **Create Snapshot** (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 IMAGES-Menü, und überprüfen Sie, ob alle fertig gestellt sind, 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 mit diesem Befehl **Glance image-list** 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 ist zu downloaden (in diesem Fall wird der oben in grün markiert), jetzt laden Sie ihn in einem QCOW2-Format mit diesem Befehl **Glance Image-Download-**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 wird einige Zeit dauern, 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, damit der Prozess im Falle einer SSH-Verbindung trotzdem ausgeführt wird und im OSPD abgeschlossen ist.

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 Dateiintegrität überprüft werden. Führen Sie dazu den nächsten Befehl aus, und suchen Sie am Ende der Ausgabe nach dem Attribut "beschädigt".

```
[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, den Befehl "*df -kh"* verwenden, um den Speicherplatz zu überprüfen. Wir empfehlen, die Datei temporär mithilfe von SFTP "sftproot@x.x.x.x" in das OSPD einer anderen Website zu übertragen, wobei x.x.x.x die IP-Adresse einer Remote-OSPD ist. Um die Übertragung zu beschleunigen, kann das Ziel an mehrere OSPDs gesendet werden. Auf dieselbe Weise können wir den folgenden Befehl verwenden: scp *name_of_the_file*.qcow2 root@ x.x.x.x:/tmp (wobei x.x.x.x die IP-Adresse eines Remote-OSPD ist), um die Datei in ein anderes OSPD-Projekt zu übertragen.

CEPH im Servicemodus aktivieren

Schritt 1: Stellen Sie sicher, dass der Status "sceph osd tree" auf dem Server aktiv ist.

```
[heat-admin@pod2-stack-osd-compute-0 ~]$ sudo ceph osd tree
ID WEIGHT TYPE NAME UP/DOWN REWEIGHT PRIMARY-AFFINITY
-1 13.07996 root default
-2 4.35999 host pod2-stack-osd-compute-0
0 1.09000 osd.0 up 1.00000 1.00000
3 1.09000 osd.3 up 1.00000 1.00000
6 1.09000 osd.6 up 1.00000 1.00000
```

```
9 1.09000 osd.9 up 1.00000 1.00000
-3 4.35999 host pod2-stack-osd-compute-1
1 1.09000 osd.1 up 1.00000 1.00000
4 1.09000 osd.4 up 1.00000 1.00000
7 1.09000 osd.7 up 1.00000 1.00000
10 1.09000 osd.10 up 1.00000 1.00000
-4 4.35999 host pod2-stack-osd-compute-2
2 1.09000 osd.2 up 1.00000 1.00000
5 1.09000 osd.5 up 1.00000 1.00000
8 1.09000 osd.8 up 1.00000 1.00000
11 1.09000 osd.11 up 1.00000 1.00000
```

Schritt 2: Melden Sie sich beim Knoten OSD Compute an, und setzen Sie CEPH in den Wartungsmodus.

```
[root@pod2-stack-osd-compute-0 ~]# sudo ceph osd set norebalance
[root@pod2-stack-osd-compute-0 ~]# sudo ceph osd set noout

[root@pod2-stack-osd-compute-0 ~]# sudo ceph status

cluster eb2bb192-b1c9-11e6-9205-525400330666
health HEALTH_WARN
noout,norebalance,sortbitwise,require_jewel_osds flag(s) set
monmap e1: 3 mons at {pod2-stack-controller-0=11.118.0.10:6789/0,pod2-stack-controller-
1=11.118.0.11:6789/0,pod2-stack-controller-2=11.118.0.12:6789/0}
election epoch 10, quorum 0,1,2 pod2-stack-controller-0,pod2-stack-controller-1,pod2-stack-
controller-2
osdmap e79: 12 osds: 12 up, 12 in
flags noout,norebalance,sortbitwise,require_jewel_osds
pgmap v22844323: 704 pgs, 6 pools, 804 GB data, 423 kobjects
2404 GB used, 10989 GB / 13393 GB avail
704 active+clean
client io 3858 kB/s wr, 0 op/s rd, 546 op/s wr
```

Hinweis: Wenn CEPH entfernt wird, wechselt VNF HD RAID in den Status "Degraded" (Heruntergestuft), aber der Zugriff auf die Festplatte muss noch möglich sein.

Graceful Power Aus

Ausschaltknoten

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

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

Hauptplatine ersetzen

Die Schritte zum Ersetzen des Motherboards in einem UCS C240 M4 Server können im Cisco UCS C240 M4 Server Installations- und Serviceleitfaden beschrieben werden.

1. Melden Sie sich mit der CIMC IP-Adresse beim Server an.

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

CEPH aus dem Servicemodus verschieben

Melden Sie sich beim Knoten OSD Compute an, und verschieben Sie CEPH aus dem Wartungsmodus.

```
[root@pod2-stack-osd-compute-0 ~]# sudo ceph osd unset norebalance
[root@pod2-stack-osd-compute-0 ~]# sudo ceph osd unset noout

[root@pod2-stack-osd-compute-0 ~]# sudo ceph status

cluster eb2bb192-b1c9-11e6-9205-525400330666
health HEALTH_OK
monmap e1: 3 mons at {pod2-stack-controller-0=11.118.0.10:6789/0,pod2-stack-controller-
1=11.118.0.11:6789/0,pod2-stack-controller-2=11.118.0.12:6789/0}
election epoch 10, quorum 0,1,2 pod2-stack-controller-0,pod2-stack-controller-1,pod2-stack-
controller-2
osdmap e81: 12 osds: 12 up, 12 in
flags sortbitwise,require_jewel_osds
pgmap v22844355: 704 pgs, 6 pools, 804 GB data, 423 kobjects
2404 GB used, 10989 GB / 13393 GB avail
704 active+clean
client io 3658 kB/s wr, 0 op/s rd, 502 op/s wr
```

Stellen Sie die VMs wieder her

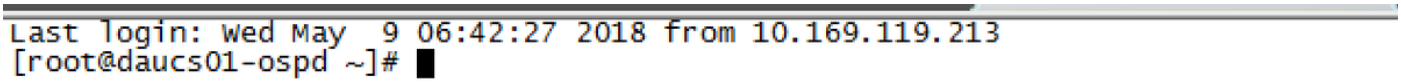
Wiederherstellen einer Instanz durch Snapshot

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. Verwenden von "sftproot@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 neu bereitgestellt wird.



Rufen Sie die Umgebungsvariablen mit dem folgenden Befehl auf:

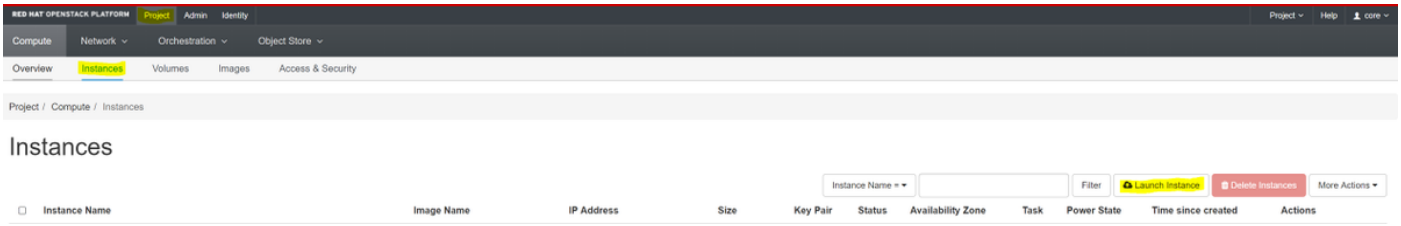
```
# source /home/stack/pod1-stackrc-Core-CPAR
```

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

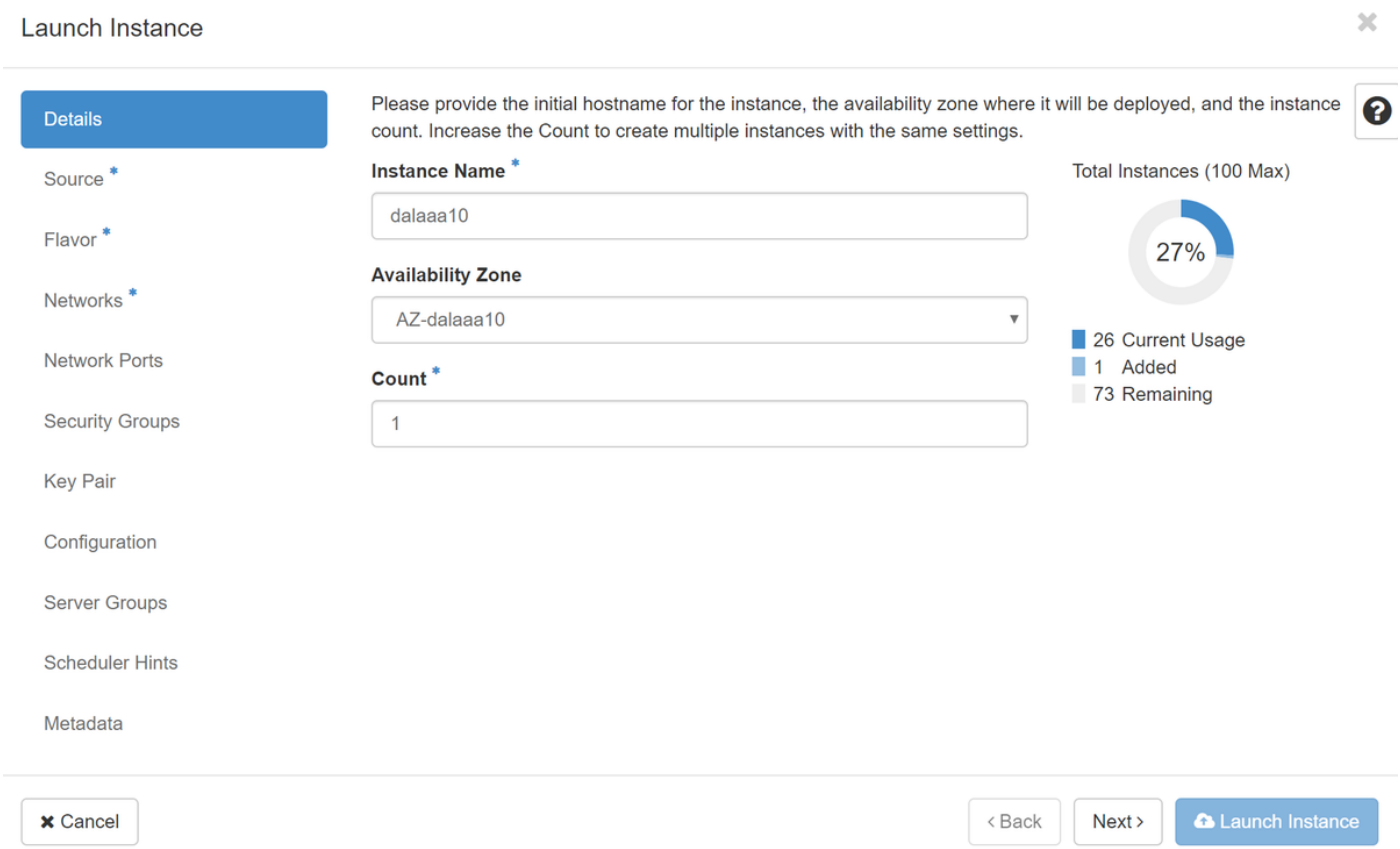
```
#glance image-create -- AAA-CPAR-Date-snapshot.qcow2 --container-format bare --disk-format qcow2
--name AAA-CPAR-Date-snapshot
```

Der Prozess ist am Horizont erkennbar.

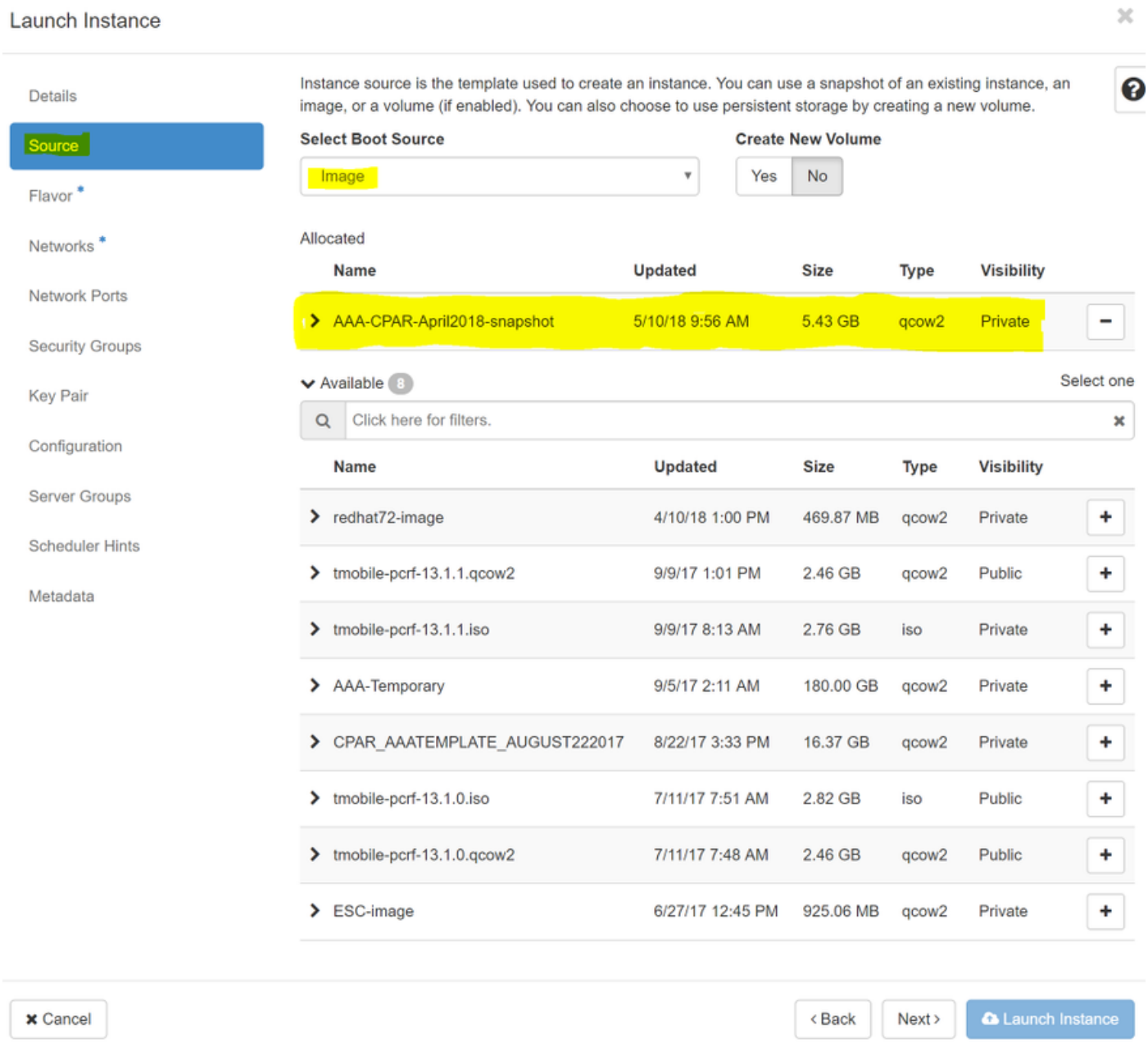
Schritt 4:Navigieren Sie in Horizon zu **Projekt > Instanzen**, und klicken Sie auf **Instanz starten**.



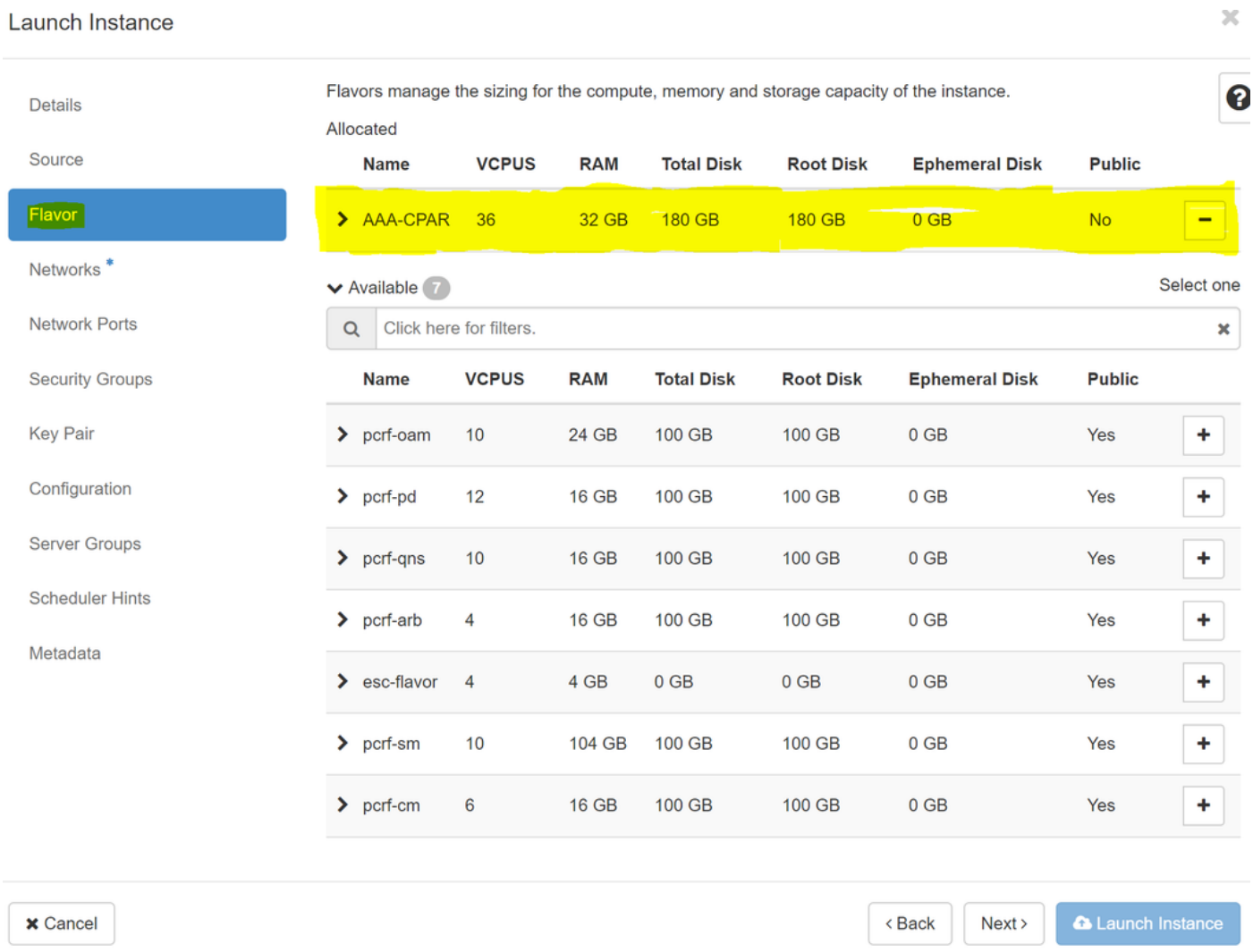
Schritt 5:Geben Sie den Instanznamen ein, und wählen Sie die Verfügbarkeitszone aus.



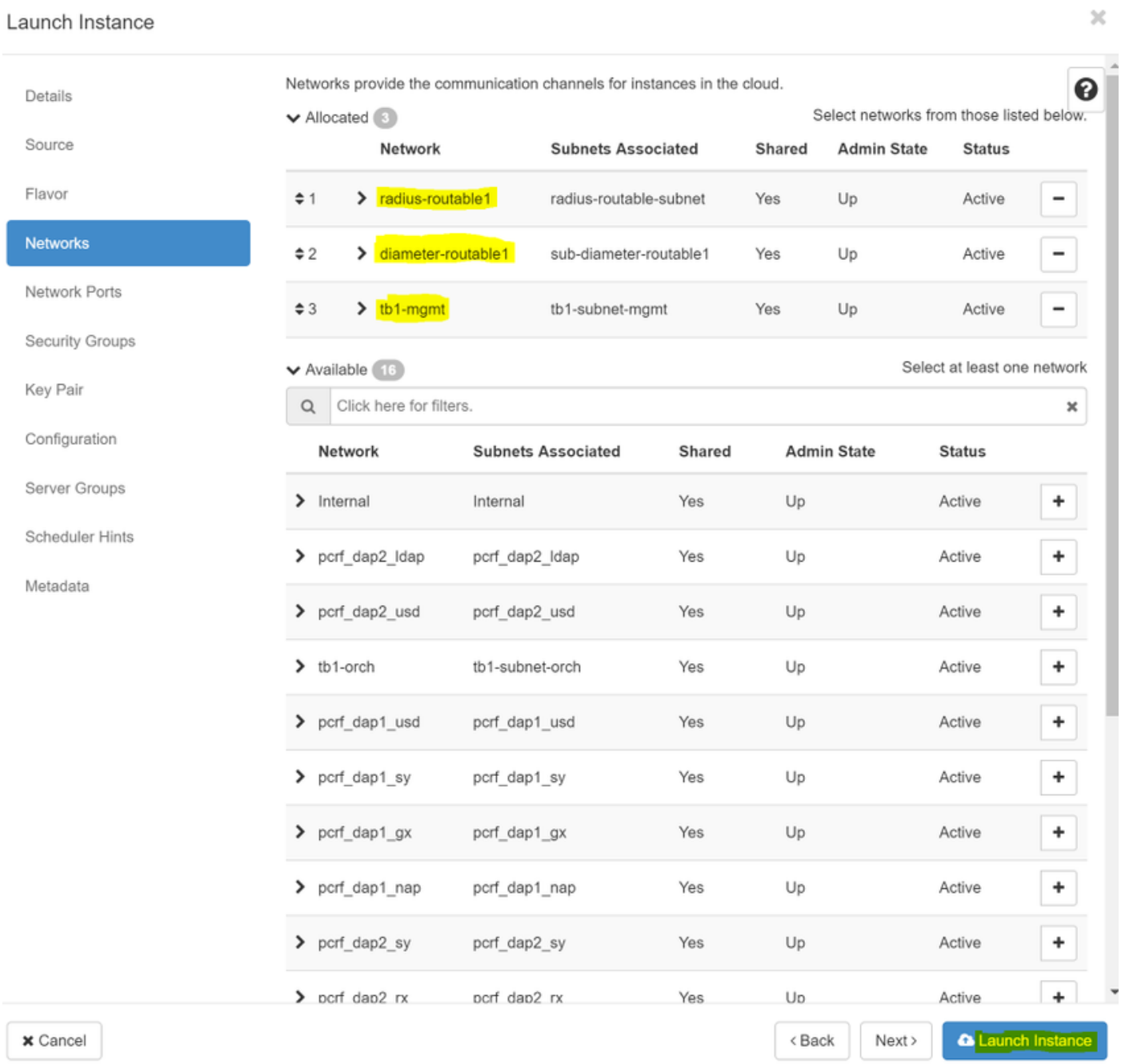
Schritt 6:Wählen Sie auf der Registerkarte Quelle das Bild aus, um die Instanz zu erstellen. Wählen Sie im Menü Select Boot Source (Startquelle auswählen) **Image (Bild** auswählen) aus. Hier wird eine Liste der Bilder angezeigt. Wählen Sie das zuvor hochgeladene Bild aus, wenn Sie auf **+**Zeichen klicken.



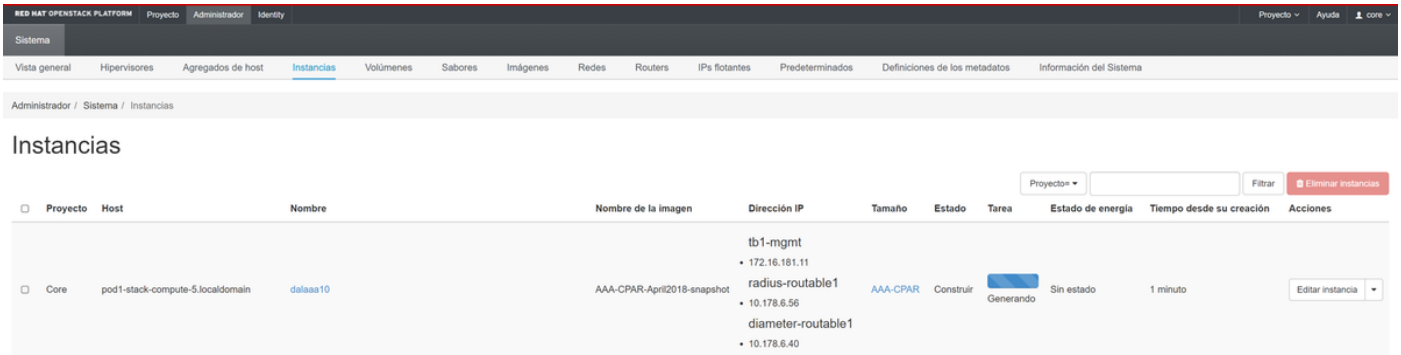
Schritt 7:Wählen Sie auf der Registerkarte Flavor die AAA-Variante aus, während Sie auf das **+** Zeichen klicken.



Schritt 8: Navigieren Sie schließlich zur Registerkarte Netzwerk, und wählen Sie die Netzwerke aus, die die Instanz benötigt, während Sie auf das **+** Zeichen klicken. Wählen Sie in diesem Fall **durchmesser-soutable1**, **radius-routing1** und **tb1-mgmt aus**.



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



Nach einigen Minuten ist die Instanz vollständig bereitgestellt und einsatzbereit.

Erstellen und Zuweisen einer Floating-IP-Adresse

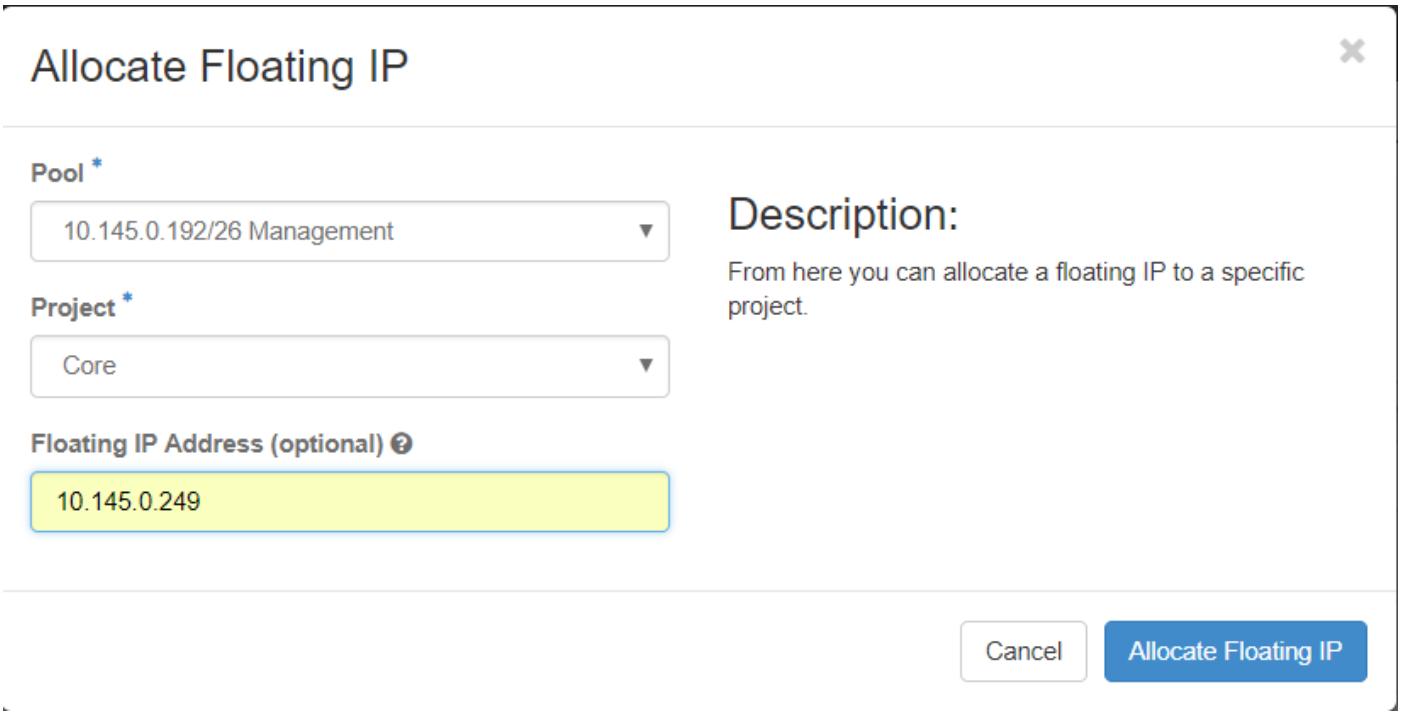
Eine Floating-IP-Adresse ist eine routbare Adresse, d. h. sie ist von der Außenseite der Ultra M/OpenStack-Architektur aus erreichbar und kann mit anderen Knoten aus dem Netzwerk kommunizieren.

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

Schritt 2:Klicken Sie auf die **SchaltflächeAllocationsIP to Project**.

Schritt 3: Wählen Sie **im** Fenster **Zuweisen von Floating** IP (Floating-IP-Adresse zuweisen) den Poolbereich aus, aus dem die neue Floating-IP-Adresse gehört, das Projekt, dem sie zugewiesen wird, und die **neue Floating-IP-**Adresse selbst.

Beispiel:

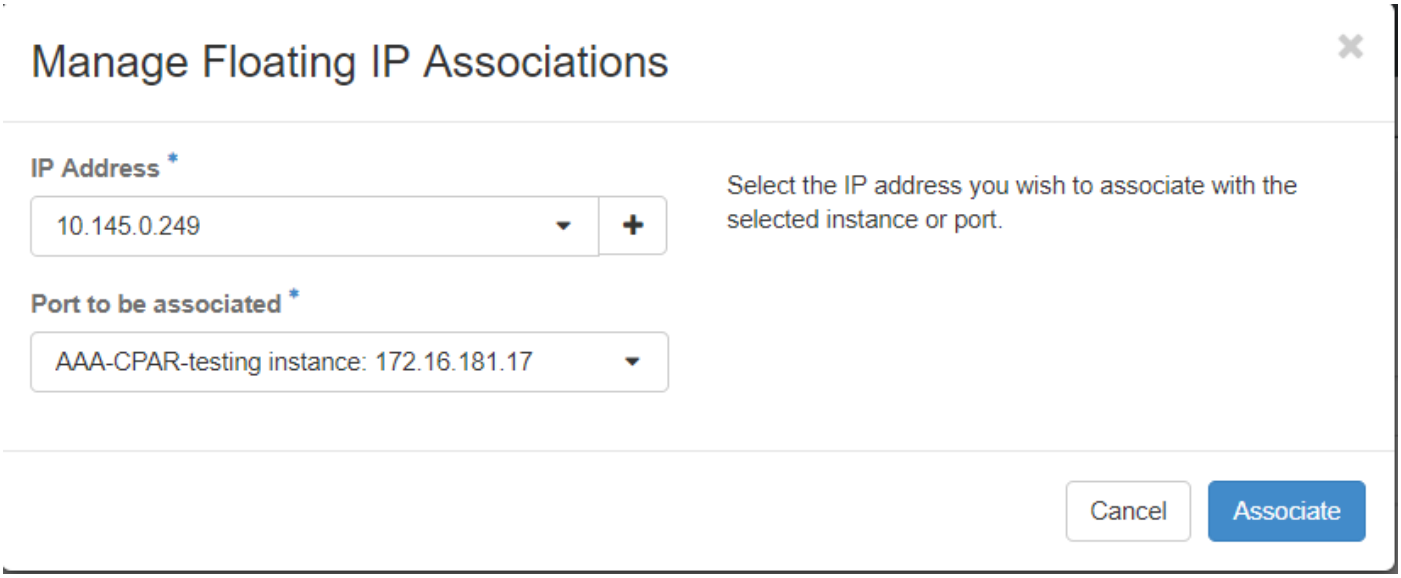


Schritt 4.Klicken Sie auf **AllocationsFloating** IPbutton.

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

Schritt 6: Klicken Sie in derSpalte Aktion auf den Pfeil, der in **der** Schaltfläche Snapshot erstellen nach unten zeigt, um ein Menü anzuzeigen. **Wählen SieFloating-**IP-Option **Zuordnen** aus.

Schritt 7: Wählen Sie die entsprechende unverankerte IP-Adresse aus, **die** im IP-Adressenfeld verwendet werden soll, und wählen Sie die entsprechende Verwaltungsschnittstelle (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 abschließend auf die Schaltfläche **Zuordnen**.

Aktivieren von SSH

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

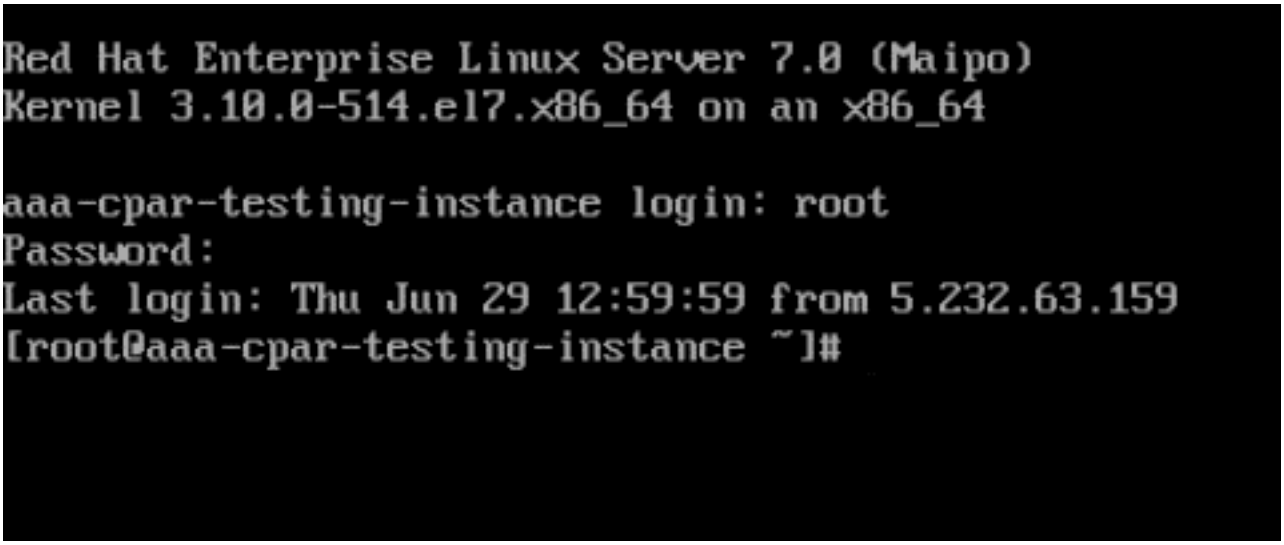
Schritt 2:Klicken Sie auf den Namen der im **AbschnittLunch einer neuen Instanz** erstellten Instanz/VM.

Schritt 3:Klicken Sie auf Consoletab. Es wird die CLI des virtuellen Systems angezeigt.

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

Benutzername: **root**

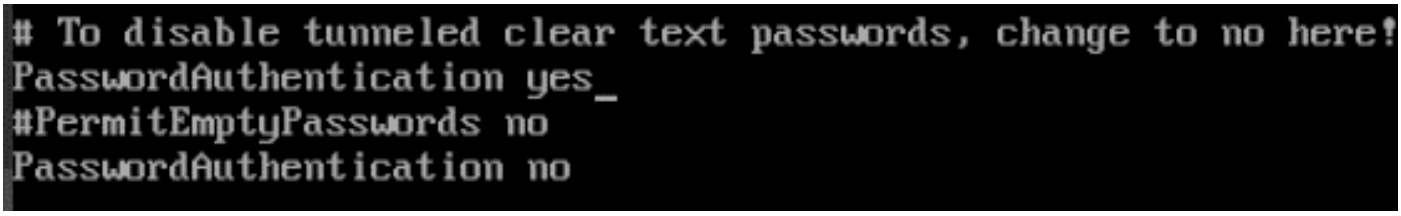
Kennwort: **cisco123**



Schritt 5:Geben Sie in der CLI den Befehl /etc/ssh/sshd_configein, um die SSH-Konfiguration zu

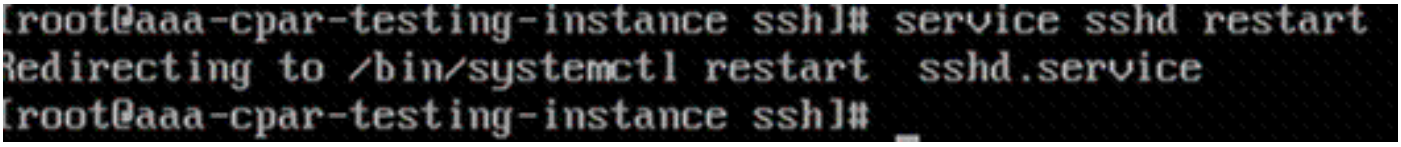
bearbeiten.

Schritt 6: Wenn die ssh-Konfigurationsdatei geöffnet ist, drücken Sie die Eingabetaste, um die Datei zu bearbeiten. Suchen Sie dann nach dem Abschnitt, der hier angezeigt wird, und ändern Sie die erste Zeile **vonPasswordAuthentication notoPasswordAuthentication yes**.

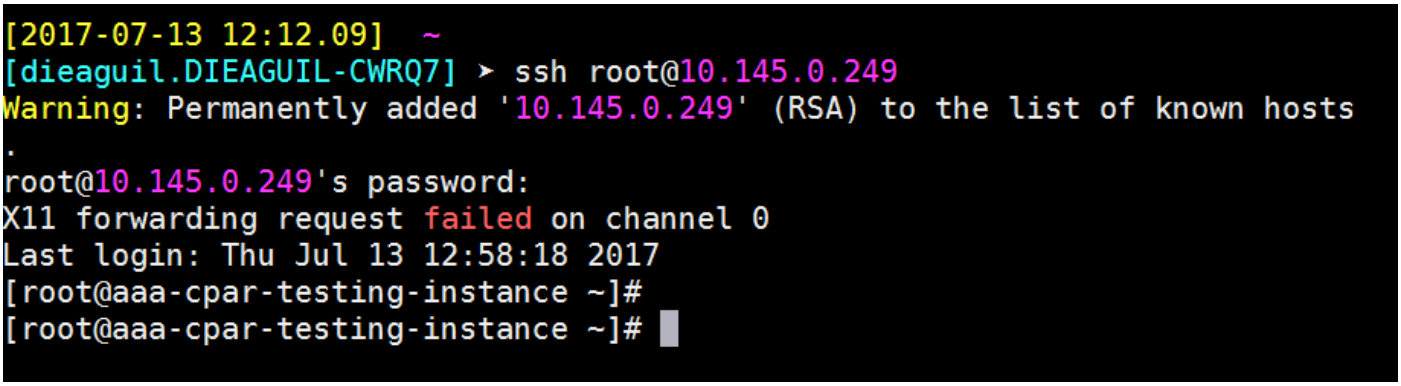


Schritt 7:Drücken Sie ESC, und geben Sie**:wq!**ein, um die Dateiänderungen sshd_config zu speichern.

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

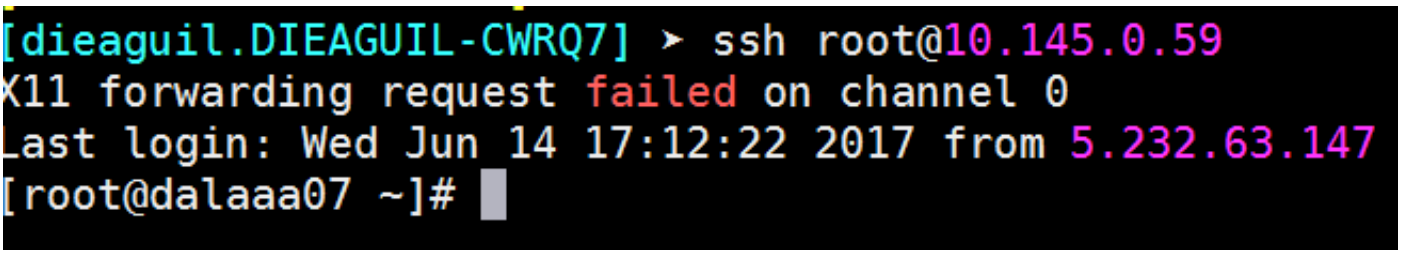


Schritt 9.Um die SSH-Konfigurationsänderungen zu testen, öffnen Sie jeden SSH-Client, und versuchen Sie, eine sichere Remote-**Verbindung** herzustellen, **indem Sie die** der Instanz (d. h. 10.145.0.249) und dem **Benutzer** zugewiesene unverankerte IP **verwenden**.



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 diese Schritte, sobald die Aktivität abgeschlossen wurde und die CPAR-Services auf der heruntergefahrenen Website wiederhergestellt werden können.

1. Melden Sie sich wieder bei Horizon an, navigieren Sie zu **Projekt > Instanz > Instanz starten**.

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@aaa04 ~]# /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 hier erwähnte Ausgabe ist für eine Umgebung vorgesehen, in der Durchmesser-Links 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 die Speichergröße, die der CPAR-Prozess mit diesem Befehl verwendet:

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.

Austausch der Hauptplatine im Controller-Knoten

Controller-Status überprüfen und Cluster in Servicemodus setzen

Vom OSPD, melden Sie sich an den Controller und überprüfen Sie, ob die PCs in gutem Zustand

sind - alle drei Controller Online und galera zeigen alle drei Controller als Master.

```
[heat-admin@pod2-stack-controller-0 ~]$ sudo pcs status
Cluster name: tripleo_cluster
Stack: corosync
Current DC: pod2-stack-controller-2 (version 1.1.15-11.el7_3.4-e174ec8) - partition with quorum
Last updated: Fri Jul 6 09:02:52 2018Last change: Mon Jul 2 12:49:52 2018 by root via
crm_attribute on pod2-stack-controller-0

3 nodes and 19 resources configured

Online: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]

Full list of resources:

ip-11.120.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
Clone Set: haproxy-clone [haproxy]
Started: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]
Master/Slave Set: galera-master [galera]
Masters: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]
ip-192.200.0.110(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
ip-11.120.0.44(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
ip-11.118.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
Clone Set: rabbitmq-clone [rabbitmq]
Started: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]
ip-10.225.247.214(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
Master/Slave Set: redis-master [redis]
Masters: [ pod2-stack-controller-2 ]
Slaves: [ pod2-stack-controller-0 pod2-stack-controller-1 ]
ip-11.119.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
openstack-cinder-volume(systemd:openstack-cinder-volume):Started pod2-stack-controller-1

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

Aktivieren Sie den Wartungsmodus für den Cluster.

```
[heat-admin@pod2-stack-controller-0 ~]$ sudo pcs cluster standby

[heat-admin@pod2-stack-controller-0 ~]$ sudo pcs status
Cluster name: tripleo_cluster
Stack: corosync
Current DC: pod2-stack-controller-2 (version 1.1.15-11.el7_3.4-e174ec8) - partition with quorum
Last updated: Fri Jul 6 09:03:10 2018Last change: Fri Jul 6 09:03:06 2018 by root via
crm_attribute on pod2-stack-controller-0

3 nodes and 19 resources configured

Node pod2-stack-controller-0: standby
Online: [ pod2-stack-controller-1 pod2-stack-controller-2 ]

Full list of resources:

ip-11.120.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
Clone Set: haproxy-clone [haproxy]
Started: [ pod2-stack-controller-1 pod2-stack-controller-2 ]
Stopped: [ pod2-stack-controller-0 ]
```

```
Master/Slave Set: galera-master [galera]
Masters: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]
ip-192.200.0.110(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
ip-11.120.0.44(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
ip-11.118.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
Clone Set: rabbitmq-clone [rabbitmq]
Started: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]
ip-10.225.247.214(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
Master/Slave Set: redis-master [redis]
Masters: [ pod2-stack-controller-2 ]
Slaves: [ pod2-stack-controller-1 ]
Stopped: [ pod2-stack-controller-0 ]
ip-11.119.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
openstack-cinder-volume(systemd:openstack-cinder-volume):Started pod2-stack-controller-1

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

Hauptplatine ersetzen

Verfahren zum Ersetzen des Motherboards in einem UCS C240 M4 Server können aus dem Cisco UCS C240 M4 Server Installations- und Serviceleitfaden abgeleitet werden.

1. Melden Sie sich mit der CIMC IP-Adresse beim Server an.

2. 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

Cluster-Status wiederherstellen

Melden Sie sich beim betroffenen Controller an, entfernen Sie den Standby-Modus, indem Sie **den Standby-Modus** festlegen. Überprüfen Sie, ob der Controller online mit Cluster geliefert wird, und galera zeigt alle drei Controller als Master an. Dies kann einige Minuten dauern.

```
[heat-admin@pod2-stack-controller-0 ~]$ sudo pcs cluster unstandby

[heat-admin@pod2-stack-controller-0 ~]$ sudo pcs status
Cluster name: tripleo_cluster
Stack: corosync
Current DC: pod2-stack-controller-2 (version 1.1.15-11.el7_3.4-e174ec8) - partition with quorum
Last updated: Fri Jul 6 09:03:37 2018Last change: Fri Jul 6 09:03:35 2018 by root via
crm_attribute on pod2-stack-controller-0

3 nodes and 19 resources configured

Online: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]

Full list of resources:

ip-11.120.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
Clone Set: haproxy-clone [haproxy]
Started: [ pod2-stack-controller-0 pod2-stack-controller-1 pod2-stack-controller-2 ]
Master/Slave Set: galera-master [galera]
Masters: [ pod2-stack-controller-1 pod2-stack-controller-2 ]
```

```
Slaves: [ pod2-stack-controller-0 ]
ip-192.200.0.110(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
ip-11.120.0.44(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
ip-11.118.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
Clone Set: rabbitmq-clone [rabbitmq]
Started: [ pod2-stack-controller-1 pod2-stack-controller-2 ]
Stopped: [ pod2-stack-controller-0 ]
ip-10.225.247.214(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-1
Master/Slave Set: redis-master [redis]
Masters: [ pod2-stack-controller-2 ]
Slaves: [ pod2-stack-controller-0 pod2-stack-controller-1 ]
ip-11.119.0.49(ocf::heartbeat:IPaddr2):Started pod2-stack-controller-2
openstack-cinder-volume(systemd:openstack-cinder-volume):Started pod2-stack-controller-1

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```