CPAR VM Snapshot und Recovery

Inhalt

Einführung

Dieses Dokument beschreibt eine schrittweise Anleitung zum Sichern (Snapshot) der AAA-Instanzen (Authentication, Authorization, Accounting).

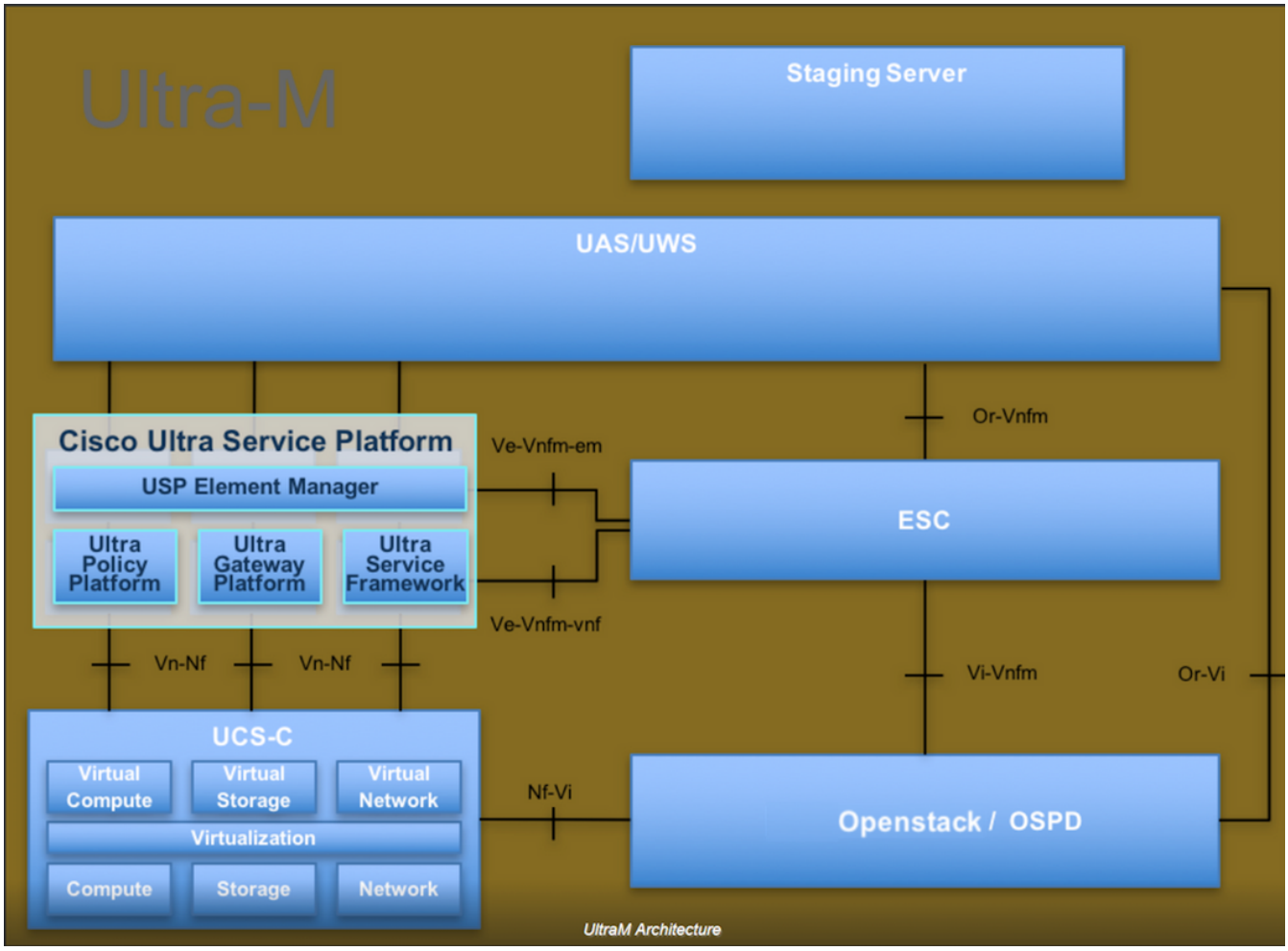
Hintergrundinformationen

Die Ausführung pro Standort und Standort ist zwingend erforderlich, um die Auswirkungen auf den Datenverkehr des Teilnehmers möglichst gering zu halten.

Dieses Verfahren gilt für eine OpenStack-Umgebung mit der NEWTON-Version, in der der Elastic Services Controller (ESC) Cisco Prime Access Registrar (CPAR) nicht verwaltet und CPAR direkt auf dem Virtual Machine (VM) installiert wird, das auf OpenStack bereitgestellt wird.

Ultra-M ist eine vorkonfigurierte und validierte Kernlösung für virtualisierte mobile Pakete, die die Bereitstellung von Virtual Network Functions (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 enthält eine Beschreibung der Schritte, die für die Ausführung unter OpenStack und Redhat OS erforderlich sind.

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

Auswirkungen auf das Netzwerk

Im Allgemeinen wird bei einem Ausfall des CPAR-Prozesses eine Verschlechterung der Kennzahlen erwartet, wie beim Herunterfahren der Anwendung. Es dauert bis zu 5 Minuten, bis der Durchmesser-Peer-Down-Trap gesendet wird. Zu diesem Zeitpunkt werden alle an den CPAR weitergeleiteten Anfragen fehlschlagen. Nach dieser Zeit werden die Verbindungen als inaktiv festgelegt, und der Diameter Routing Agent (DRA) beendet das Routing des Datenverkehrs zu diesem Knoten.

Wenn für alle vorhandenen Sitzungen im AAA ein Attach/Detach-Verfahren mit einer anderen aktiven AAA-Instanz durchgeführt wird, schlägt dieses Verfahren fehl, da der Hosted Security-as-a-Service (HSS) antwortet, dass der Benutzer beim abgeschlossenen AAA registriert ist und das Verfahren nicht erfolgreich abgeschlossen werden kann.

Die STR-Leistung wird etwa 10 Stunden nach Abschluss der Aktivität voraussichtlich unter 90 % der Erfolgsrate liegen. Danach muss der Normalwert von 90 % erreicht werden.

Alarme

SNMP-Alarme (Simple Network Management Protocol) werden bei jedem Beenden und Starten des CPAR-Dienstes generiert. Daher müssen während des gesamten Prozesses SNMP-Traps generiert werden. Folgende Traps werden erwartet:

- STOPP FÜR CPAR-SERVER
- VM AUSGESCHALTET
- NODE DOWN - (Erwarteter Alarm, der nicht direkt von der CPAR-Instanz generiert wird)
- DRA

VM-Snapshot-Backup

Herunterfahren der CPAR-Anwendung

> **Hinweis**: Stellen Sie sicher, dass Sie über einen Internetzugang zu HORIZON für die Website und Zugriff auf OSPD verfügen.

Schritt 1: Öffnen Sie einen Secure Shell (SSH)-Client, der mit dem Transformation Management Office (TMO)-Produktionsnetzwerk verbunden ist, und stellen Sie eine Verbindung zur CPAR-Instanz her.

> **Hinweis**: Es ist wichtig, nicht alle vier AAA-Instanzen gleichzeitig an einem Standort abzuschalten, sondern nacheinander durchzuführen.

Schritt 2: Führen Sie zum Herunterfahren der CPAR-Anwendung den folgenden Befehl aus:

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

Es muss die Meldung "Abgeschlossen des Cisco Prime Access Registrar Server Agent" angezeigt werden.

> **Hinweis**: Wenn Sie die CLI-Sitzung geöffnet lassen, funktioniert der **Befehl arserver stop** nicht, und diese Fehlermeldung 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. Wenn dies der Fall ist, führen Sie den Befehl aus und beenden Sie den Vorgang:

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

Wiederholen Sie anschließend Schritt 1.

Schritt 3: Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die CPAR-Anwendung tatsächlich heruntergefahren wurde:

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

Diese Meldungen müssen angezeigt werden:

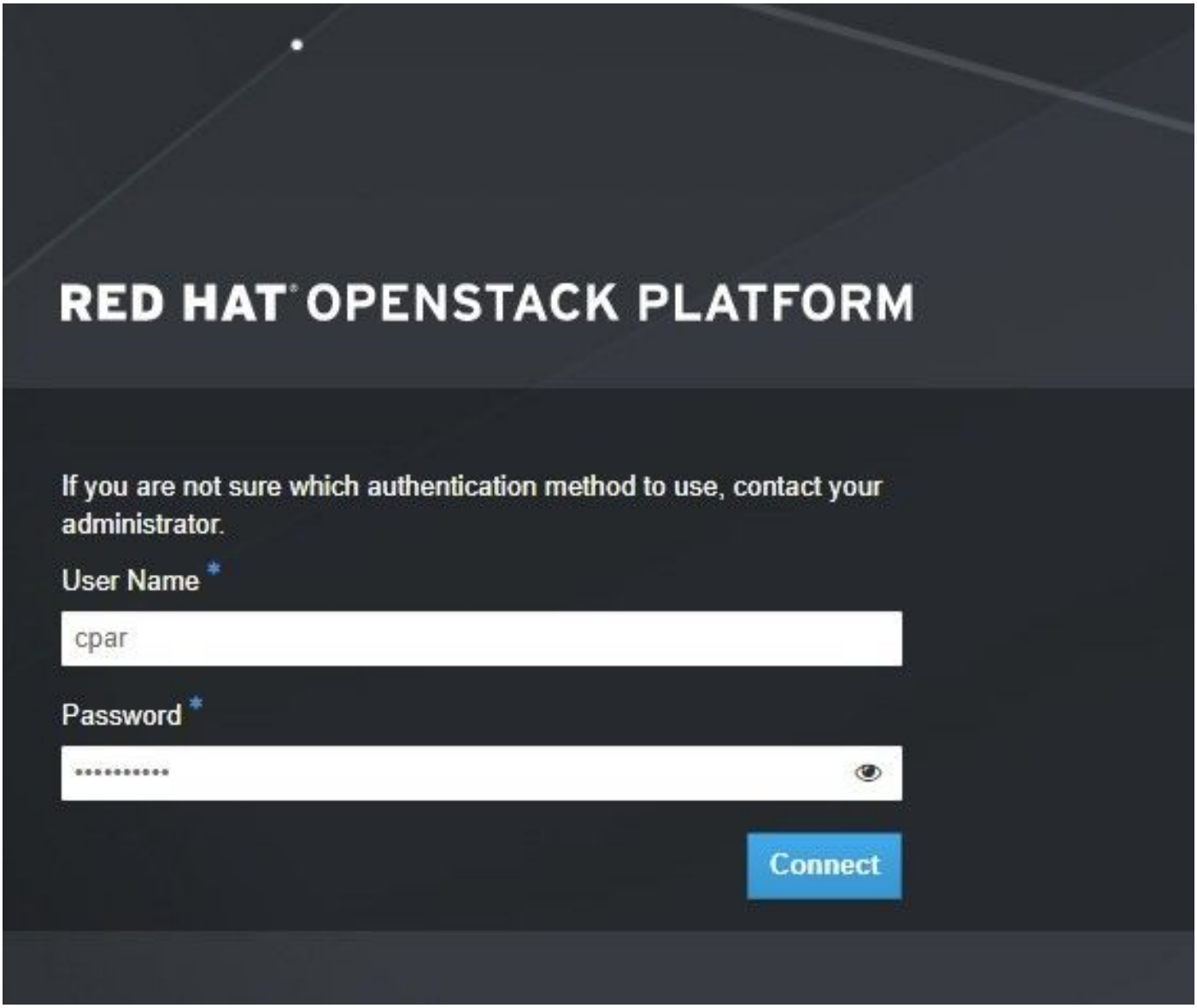
```
Cisco Prime Access Registrar Server Agent not running

Cisco Prime Access Registrar GUI not running
```

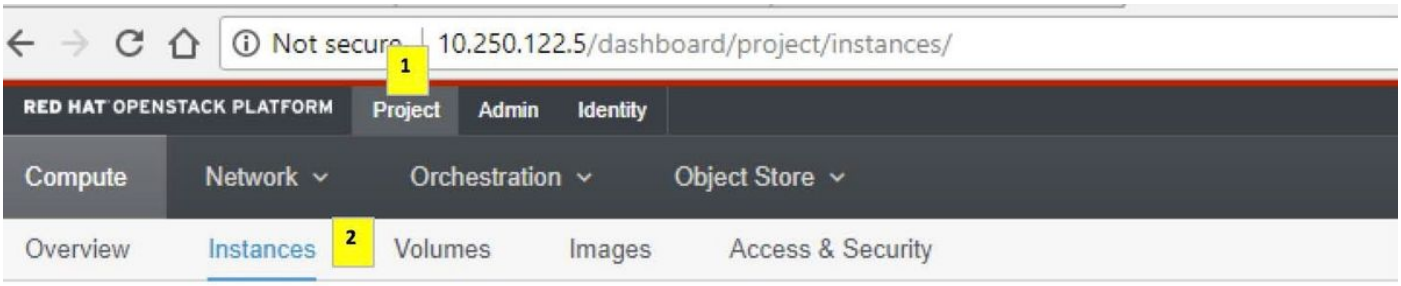
VM-Backup-Snapshot-Aufgabe

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

Wenn Sie auf Horizon zugreifen, wird der beobachtete Bildschirm wie im Bild gezeigt 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, und wiederholen Sie den gesamten Vorgang in diesem Dokument. Um das virtuelle System herunterzufahren, navigieren Sie zu **Actions > Shut Off Instance (Aktion > Deaktivierung beenden)** wie im Bild gezeigt, und bestätigen Sie Ihre Auswahl.

Schritt 4: Um zu überprüfen, ob die Instanz tatsächlich heruntergefahren ist, überprüfen Sie Status = **Shutoff** und Power State = **Shut Down**, wie im Bild gezeigt.

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.

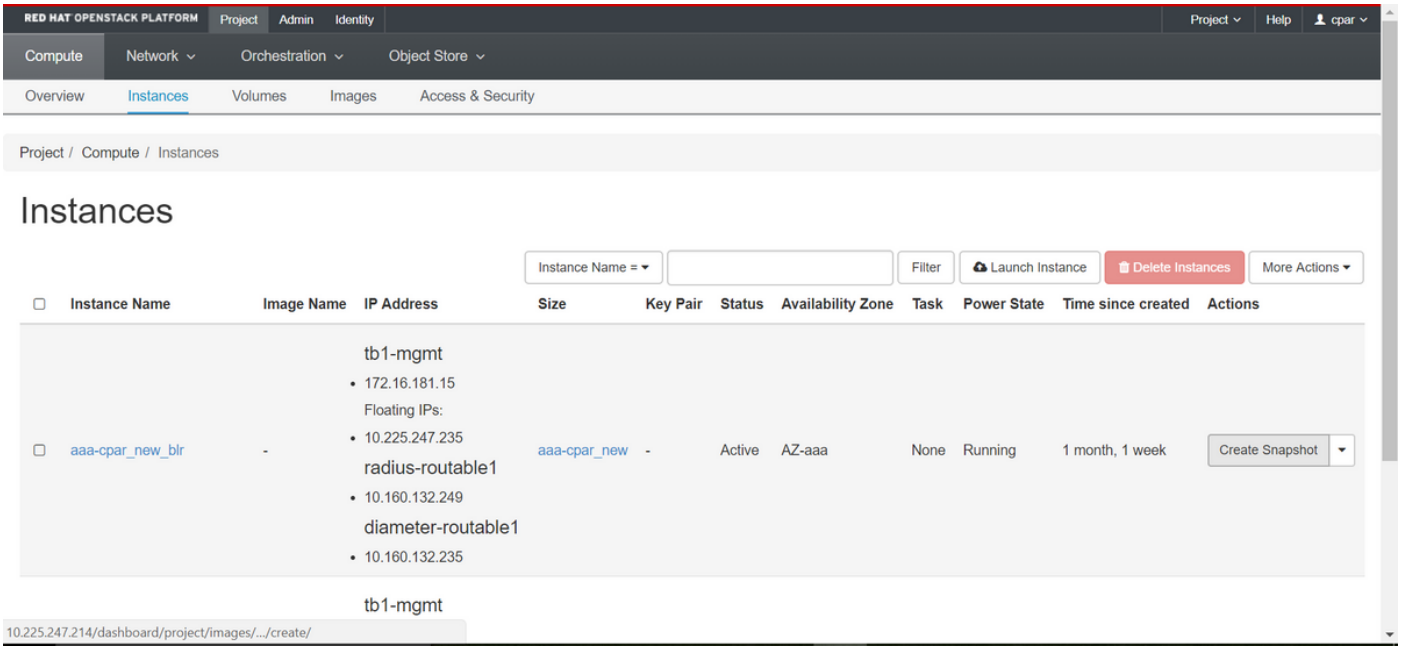
Die vier QCOW2-Dateien werden parallel erstellt.

Schritt 1: Erstellen Sie einen Snapshot jeder AAA-Instanz.

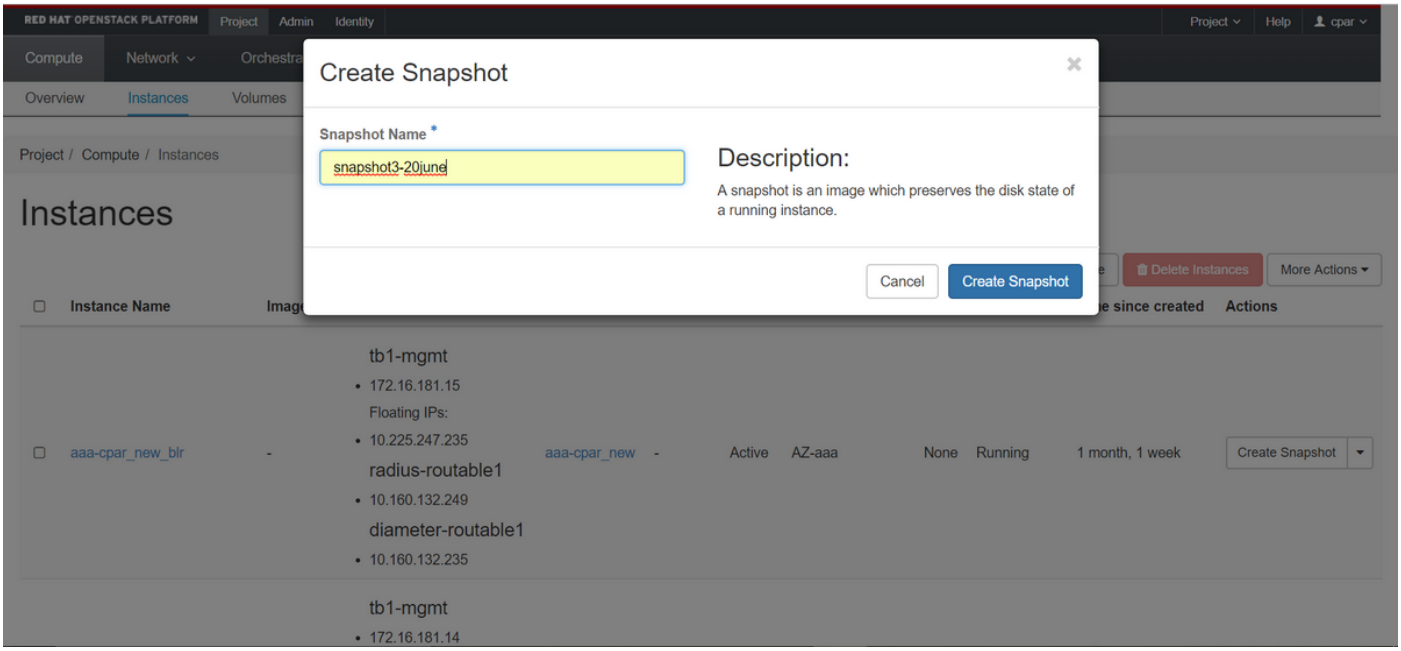
> **Hinweis**: 25 Minuten für Instanzen, die ein QCOW-Image als Quelle verwenden, und 1 Stunde für Instanzen, die ein Rohbild als Quelle verwenden.

Schritt 2: Melden Sie sich bei der Horizon **GUI** von POD OpenStack an.

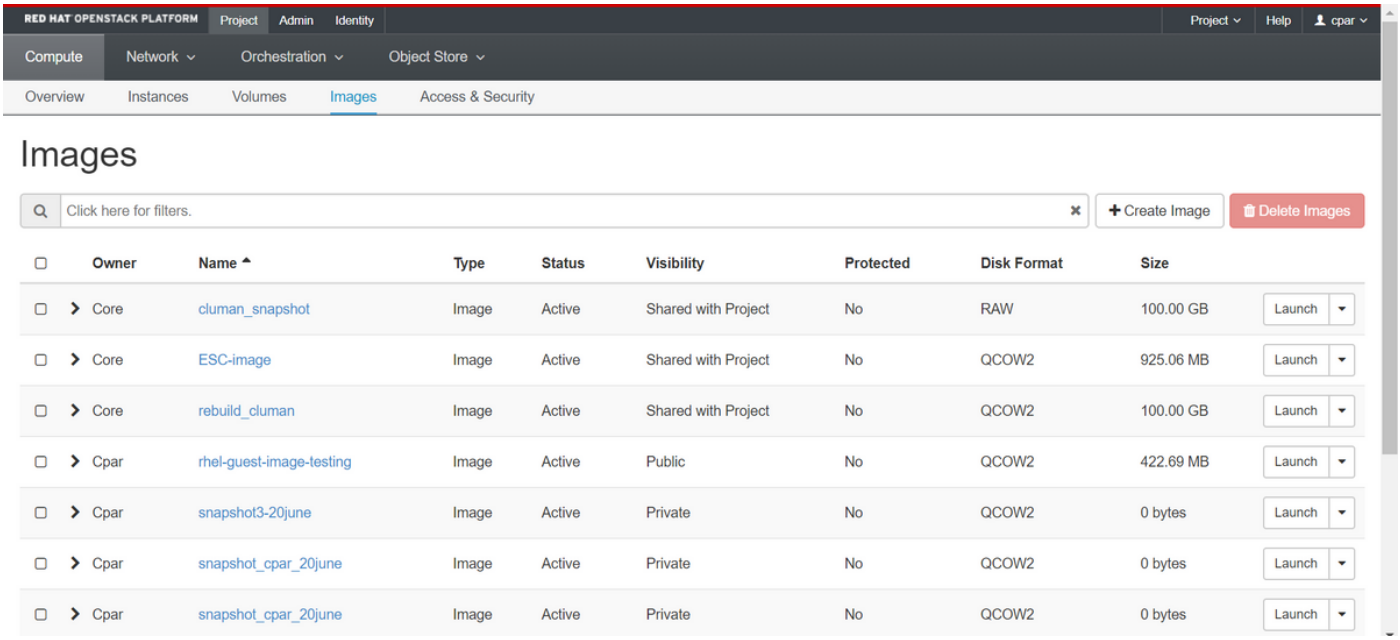
Schritt 3: Navigieren Sie nach der Anmeldung zu **Projekt > Compute > Instanzen** im oberen Menü, und suchen Sie die AAA-Instanzen, wie im Bild gezeigt.



Schritt 3: Klicken Sie auf **Snapshot erstellen**, um mit der Snapshot-Erstellung fortzufahren, wie im Bild gezeigt. Dies muss für die entsprechende AAA-Instanz ausgeführt werden.



Schritt 4: Sobald der Snapshot ausgeführt wurde, navigieren Sie zum Menü **Bilder**, und überprüfen Sie, ob alle fertig gestellt sind und kein Problem melden, wie im Bild gezeigt.



Schritt 5: Der nächste Schritt besteht darin, den Snapshot im QCOW2-Format herunterzuladen und an eine entfernte Einheit zu übertragen, falls das OSPD bei diesem Prozess verloren geht. Um dies zu erreichen, müssen Sie den Snapshot mithilfe des Befehls **Glance image-list** auf OSPD-Ebene identifizieren, wie im Bild gezeigt.

```
[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 Sie den herunterzuladenden Snapshot identifiziert haben (in diesem Fall der Snapshot, der grün markiert ist), können Sie ihn im QCOW2-Format mit dem Befehl **Glance image-download** (**Image-Download** wie hier abgebildet) herunterladen:

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

Das **&**Senden des Prozesses an den Hintergrund. Es dauert einige Zeit, bis die Aktion abgeschlossen ist. Anschließend kann das Bild im Verzeichnis **/tmp** gespeichert werden.

- Wenn Sie den Prozess an den Hintergrund senden und die Verbindung unterbrochen wird, wird der Vorgang ebenfalls beendet.
- Führen Sie den Befehl **dissown -h aus**, sodass der Prozess bei Verlust der 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 (OS) verarbeitet werden, mit ZEROES gefüllt werden kann. Der für die

Dateikomprimierung auszuführende Befehl ist **virt-sparsify**.

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

Dieser Vorgang kann einige Zeit in Anspruch nehmen (etwa 10-15 Minuten). Nach Abschluss des Vorgangs muss die Datei, die zu Ergebnissen führt, wie im nächsten Schritt angegeben an eine externe Entität 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
```

Schritt 8: 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 Sie die Dateiübertragung starten, müssen Sie überprüfen, ob das Ziel über genügend freien Speicherplatz verfügt, den Befehl **df -kh** ausführen, um den Speicherplatz zu überprüfen.

Es wird empfohlen, die Datei temporär mithilfe von SFTP **sftp** root@x.x.x.xwhere **x.x.x.x** ist die IP-Adresse eines Remote-OSPD auf das OSPD eines anderen Standorts zu übertragen.

Schritt 9: Um die Übertragung zu beschleunigen, kann das Ziel an mehrere OSPDs gesendet werden. Auf die gleiche Weise können Sie den Befehl **scp *name_of_the_file*.qcow2 root@ x.x.x.x:/tmp** (wobei **x.x.x.x** die IP einer Remote-OSPD ist) ausführen, um die Datei auf ein anderes OSPD-Projekt zu übertragen.

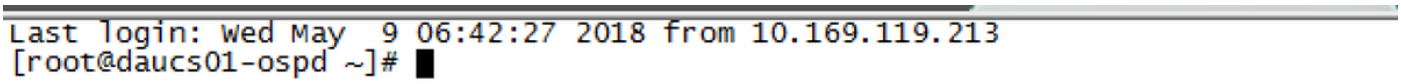
Instanz mit Snapshot wiederherstellen

Wiederherstellungsprozess

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

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

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

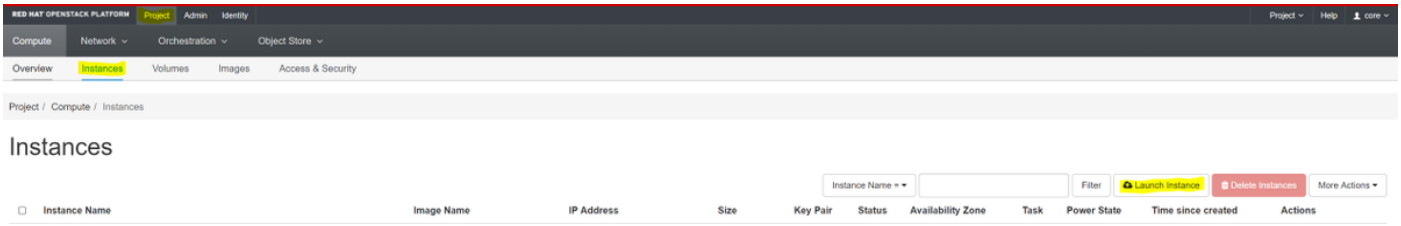


Schritt 3: Um den Snapshot als Bild zu verwenden, muss er in Horizon als solches hochgeladen werden. Verwenden Sie dazu den nächsten Befehl.

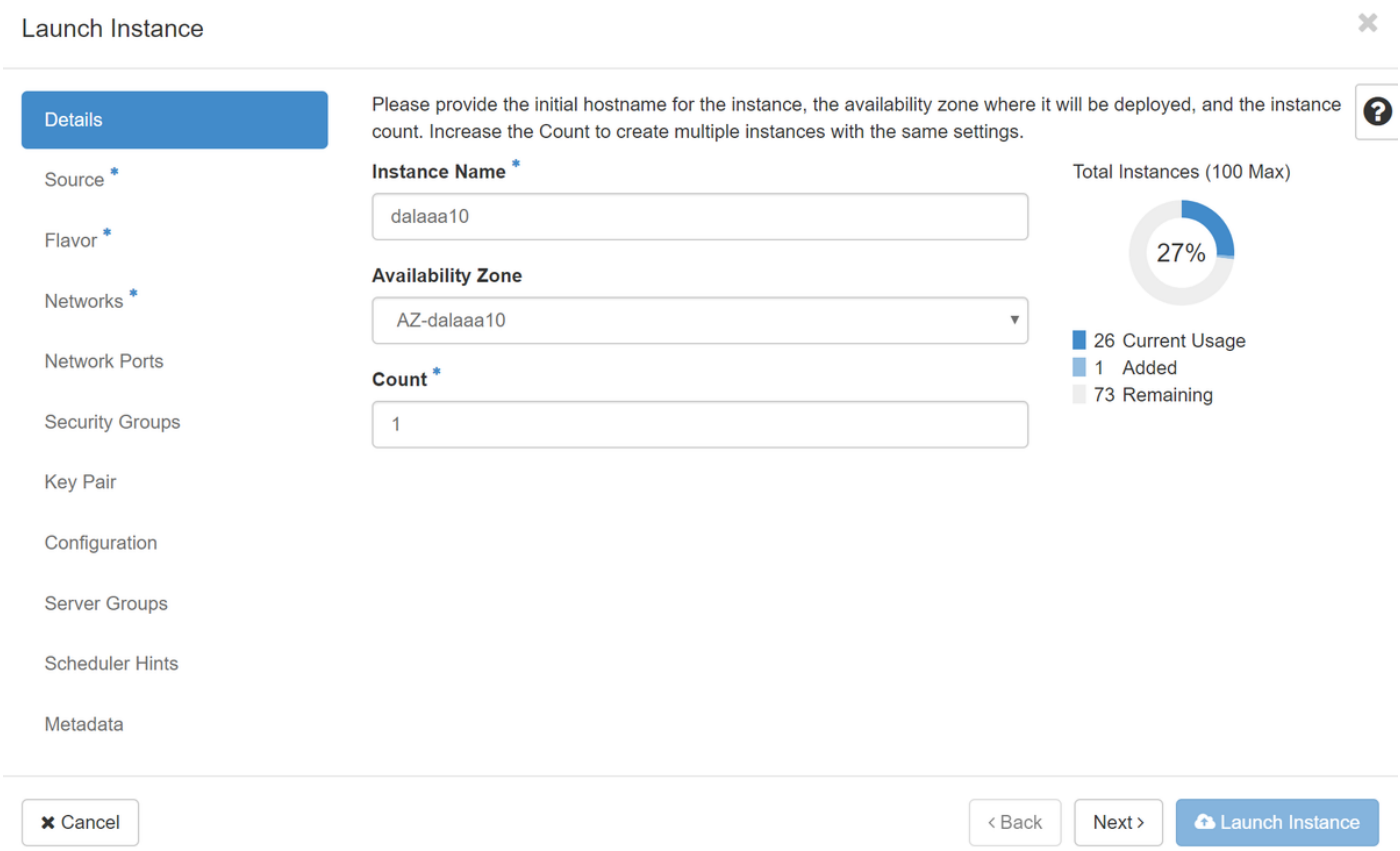
```
#glance image-create -- AAA-CPAR-Date-snapshot.qcow2 --container-format bare --disk-format qcow2 --name AAA-CPAR-Date-snapshot
```

Der Prozess kann im Horizont und wie im Bild gezeigt angezeigt werden.

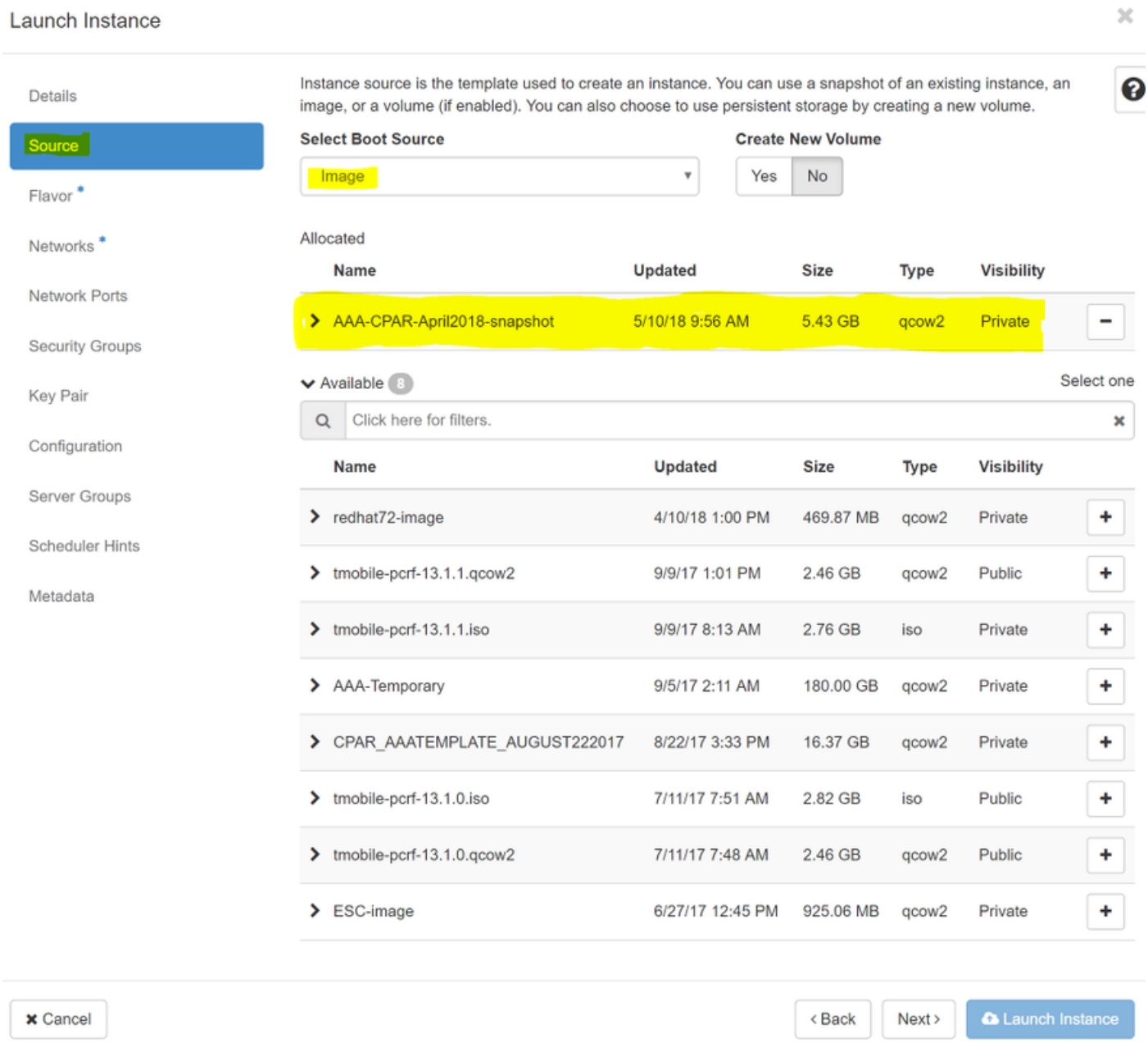
Schritt 4: Navigieren Sie in Horizon zu **Projekt > Instanzen**, und klicken Sie auf **Instanz** starten, wie im Bild gezeigt.



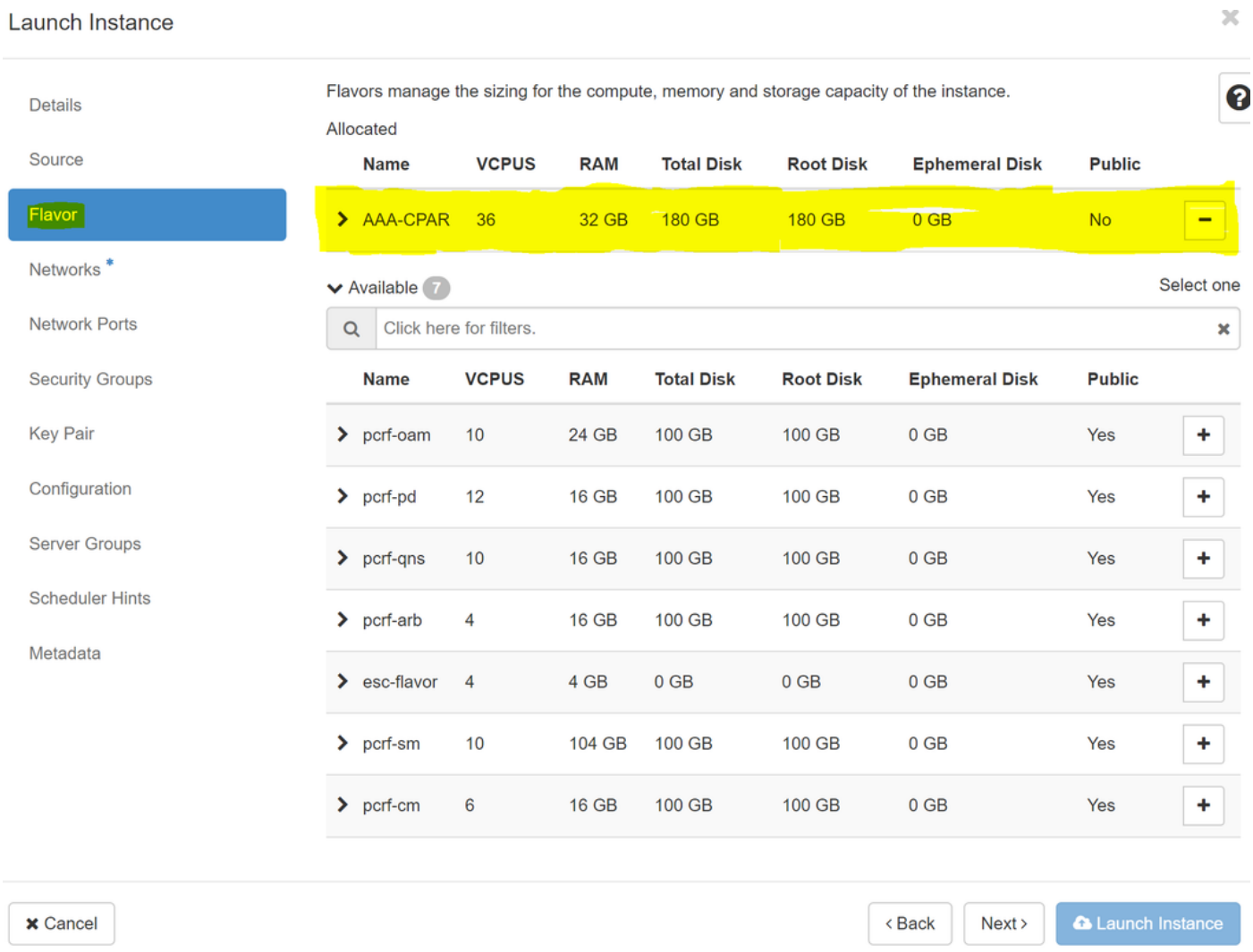
Schritt 5: Geben Sie den **Instanznamen ein** und wählen Sie die **Verfügbarkeitszone** wie im Bild gezeigt aus.



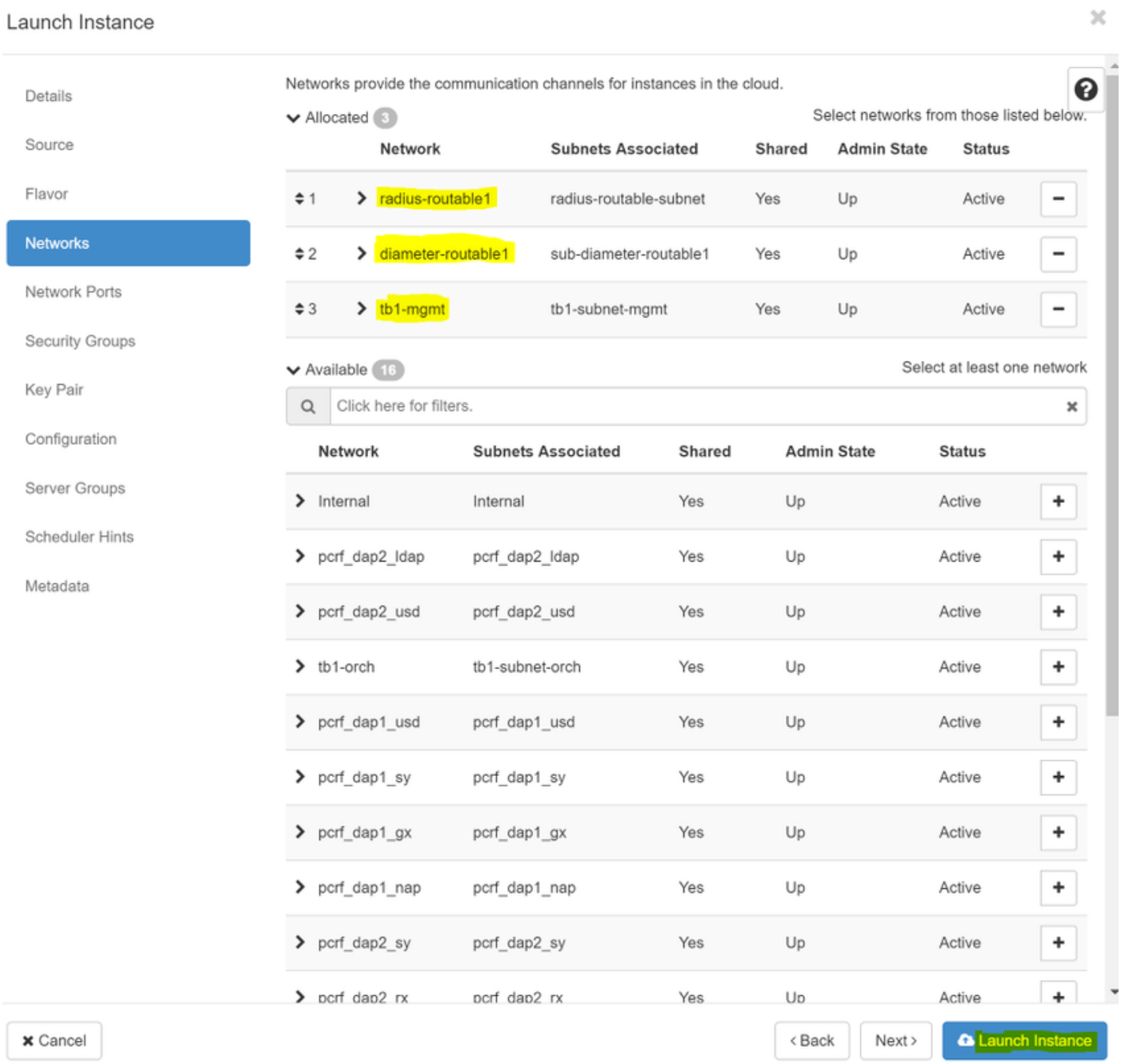
Schritt 6: Wählen Sie auf der Registerkarte Quelle das Bild aus, um die Instanz zu erstellen. Wählen Sie im Menü Boot Source (Startquelle auswählen) das **Bild aus,** und hier wird eine Bildliste angezeigt. Wählen Sie die Datei aus, die zuvor hochgeladen wurde, indem Sie auf das **+**-Zeichen klicken, wie im Bild gezeigt.



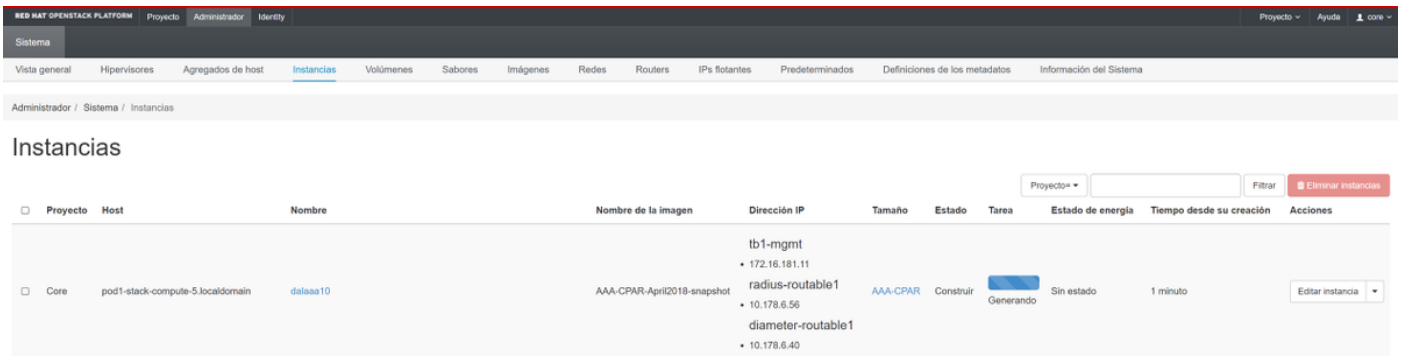
Schritt 7: Wählen Sie auf der Registerkarte Flavor den AAA-Typ aus, indem Sie auf das **+** Zeichen klicken, wie im Bild gezeigt.



Schritt 8: Navigieren Sie schließlich zur Registerkarte **Netzwerke**, und wählen Sie die Netzwerke aus, die für die Instanz benötigt werden, indem Sie auf das **+** Zeichen klicken. Wählen Sie in diesem Fall **durchmesser-soutable1**, **radius-routing1** und **tb1-mgmt aus,** wie im Bild gezeigt.



Schritt 9: Klicken Sie auf **Instanz starten**, um sie zu erstellen. Der Fortschritt kann in Horizon überwacht werden, wie im Bild gezeigt.



Schritt 10: Nach einigen Minuten ist die Instanz vollständig bereitgestellt und einsatzbereit, wie im Bild gezeigt.

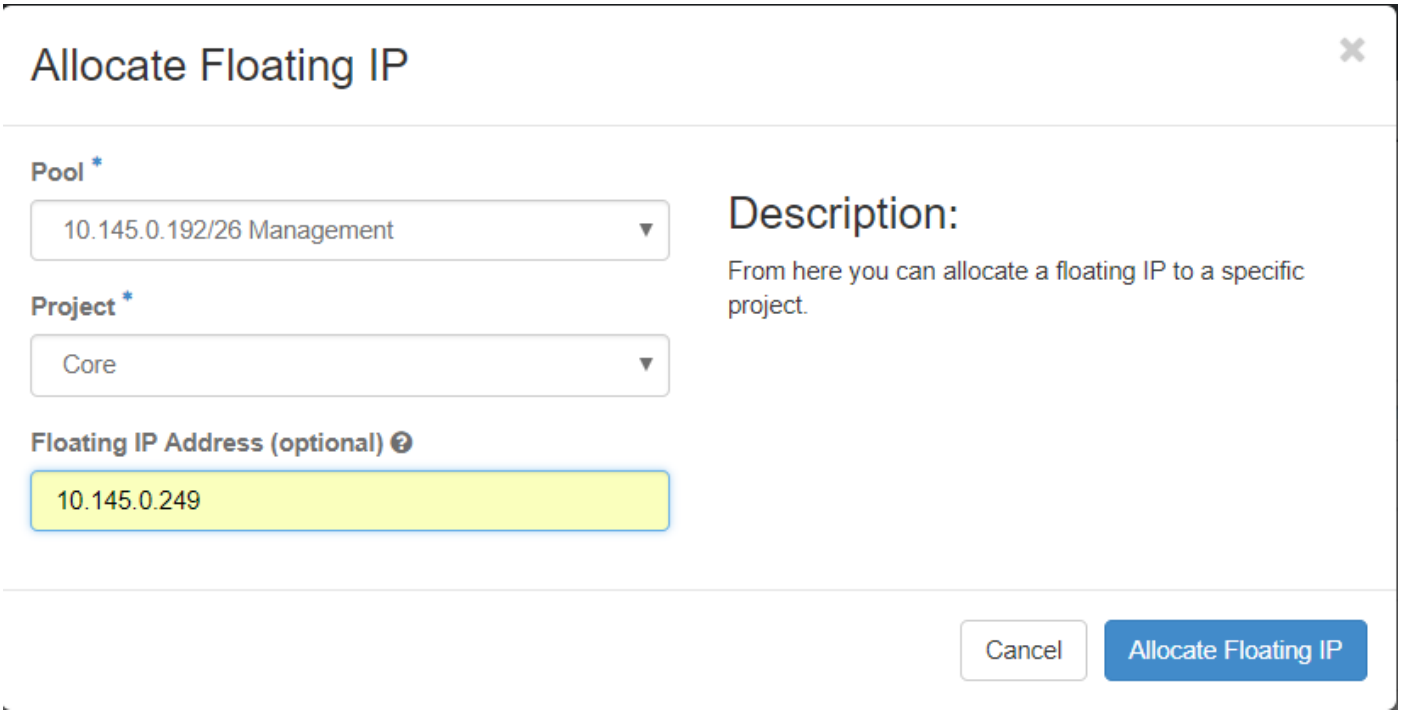
Floating-IP-Adresse erstellen und zuweisen

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 **Projekt** IP **zuweisen**.

Schritt 3: Wählen Sie im Fenster **Zuordnen von Floating-IP** den **Pool**, aus dem die neue unverankerte IP gehört, das **Projekt**, dem sie zugewiesen wird, und die neue **Floating-IP-Adresse** selbst, wie im Bild gezeigt.

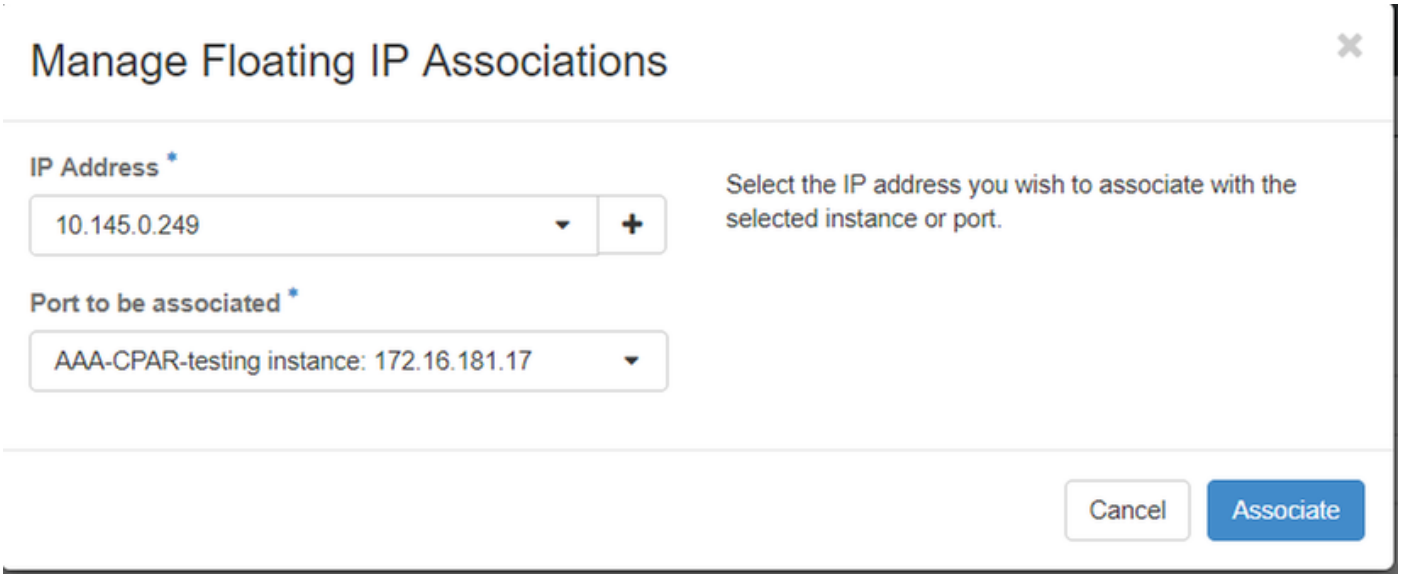


Schritt 4: Klicken Sie auf Floating-**IP zuweisen**.

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 wird angezeigt. Klicken Sie auf die Option **Unübertragbare IP zuordnen**.

Schritt 7: Wählen Sie die entsprechende unverankerte IP-Adresse aus, die im Feld **IP-Adresse** 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**,** wie im Bild
gezeigt.



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

SSH aktivieren

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

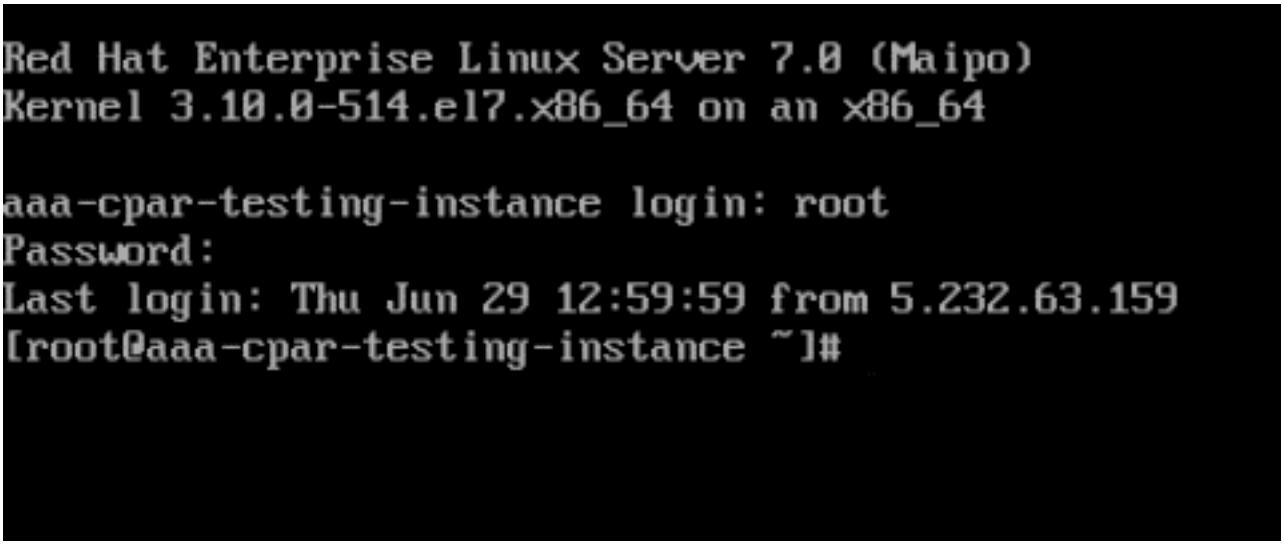
Schritt 2: Klicken Sie auf den Namen der im Abschnitt **Neue Instanz starten** erstellten Instanz/VM.

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

Schritt 4: Geben Sie nach der Anzeige der CLI die entsprechenden Anmeldeinformationen ein, wie im Bild gezeigt:

Benutzername: **Wurzel**

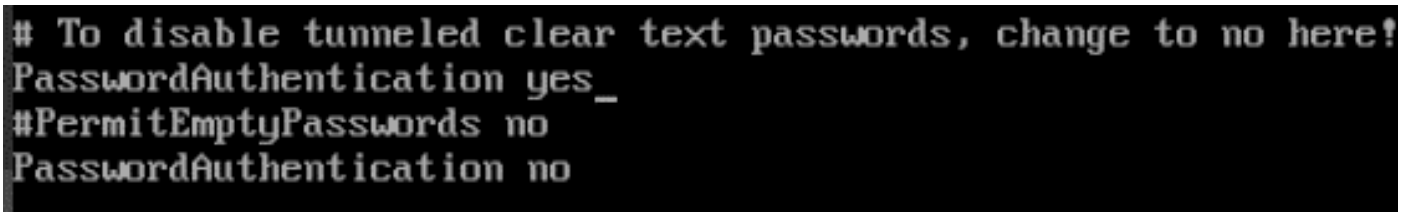
Kennwort: **<cisco123>**



Schritt 5: Führen Sie in der CLI den Befehl **vi /etc/ssh/sshd_config aus**, um die SSH-Konfiguration zu bearbeiten.

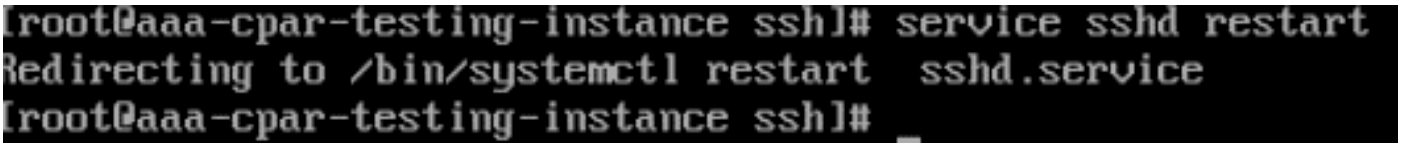
Schritt 6: Wenn die SSH-Konfigurationsdatei geöffnet ist, drücken Sie **I**, um die Datei zu

bearbeiten. Ändern Sie dann die erste Zeile von **PasswordAuthentication no** in **PasswordAuthentication yes (Kennwortauthentifizierung)**, wie im Bild gezeigt.

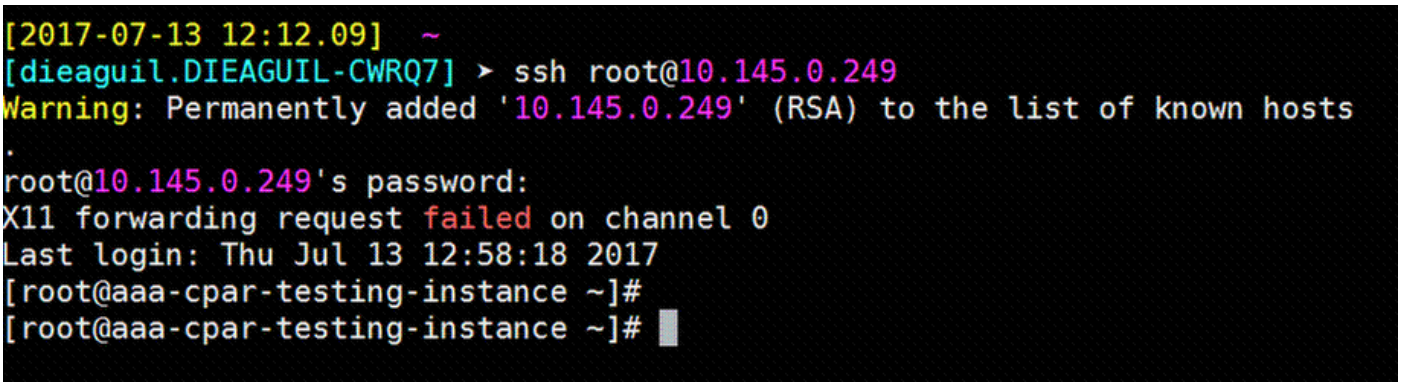


Schritt 7: Drücken Sie **ESC** und geben Sie **:wq!** ein, um die Dateiänderungen **sshd_config** zu speichern.

Schritt 8: Führen Sie den Befehl **service sshd restart aus, wie im Bild gezeigt.**

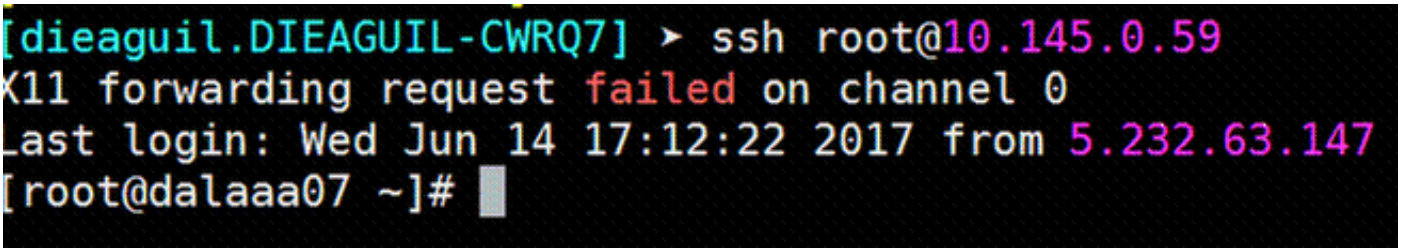


Schritt 9: Um zu überprüfen, ob die SSH-Konfigurationsänderungen ordnungsgemäß angewendet wurden, öffnen Sie einen beliebigen SSH-Client, und versuchen Sie, eine sichere Remote-Verbindung mit der Floating-IP-Adresse herzustellen, die der Instanz zugewiesen ist (d. h. **10.145.0.249**), und dem Benutzer-**Root** wie im Bild gezeigt.



SSH-Sitzung einrichten

Schritt 1: Öffnen Sie eine SSH-Sitzung mit der IP-Adresse des entsprechenden VM/Servers, auf dem die Anwendung wie im Image gezeigt installiert ist.



CPAR-Instanzstart

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

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

Schritt 2: Überprüfen Sie, ob der Status der Instanz **aktiv** ist und der Betriebsstatus **ausgeführt** wird, wie im Bild gezeigt.

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 7.3(100TPS:)

                  PAR-ADD-TPS 7.3(2000TPS:)

                  PAR-RDDR-TRX 7.3()

                  PAR-HSS 7.3()

    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 Protokoll des TelePresence Server (TPS) die von CPAR verarbeiteten Anforderungen anzeigt. Die hervorgehobenen Werte stellen TPS dar. Sie müssen genau auf diese Werte achten.

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 in name_radius_1_log nach "error"- oder "alarm"-Meldungen:

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

Schritt 6: Führen Sie den folgenden Befehl aus, um die Speichergröße zu überprüfen, die vom CPAR-Prozess verwendet wird:

```
top | 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 muss kleiner als 7 GB sein. Dies ist der maximal zulässige Wert auf Anwendungsebene.