CPAR AAA VM-Bereitstellung

Inhalt

Einführung

Dieses Dokument beschreibt Cisco Prime Access Registrars (CPARs) VM-Bereitstellung für Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting (AAA) Dieses Verfahren gilt für eine OpenStack-Umgebung unter Verwendung der NEWTON-Version, in der CPAR von ESC nicht verwaltet wird und CPAR direkt auf dem virtuellen System (VM) installiert wird, das auf OpenStack bereitgestellt wird.

Verfasst von Karthikeyan Dachanamoorthy, Cisco Advanced Services.

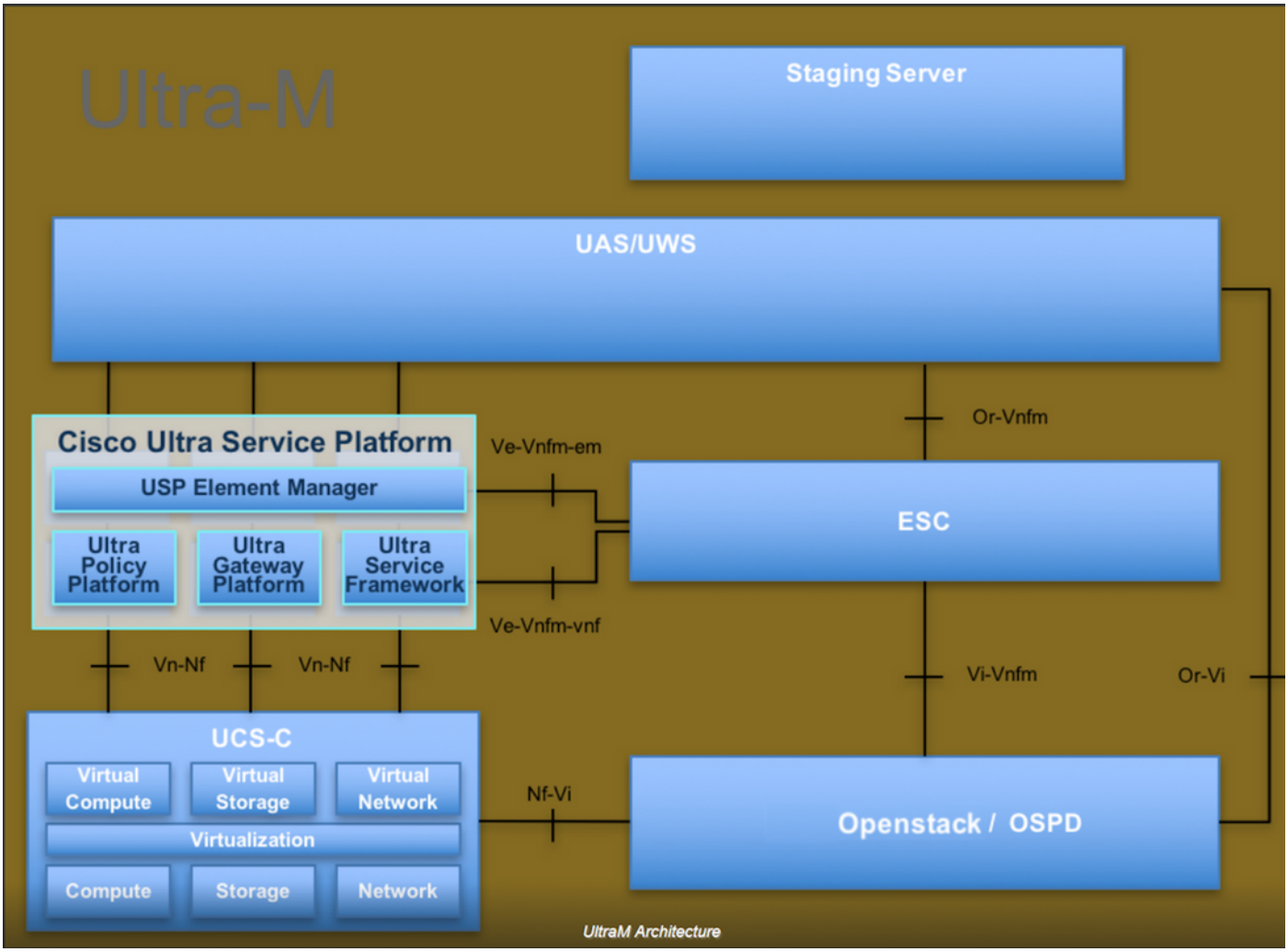
Hintergrundinformationen

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.

Bereitstellungsmethode für CPAR VM-Instanzen

Melden Sie sich bei der Horizon Interface an.

Stellen Sie sicher, dass diese erfüllt sind, bevor Sie mit der VM-Instanz-Bereitstellung beginnen.

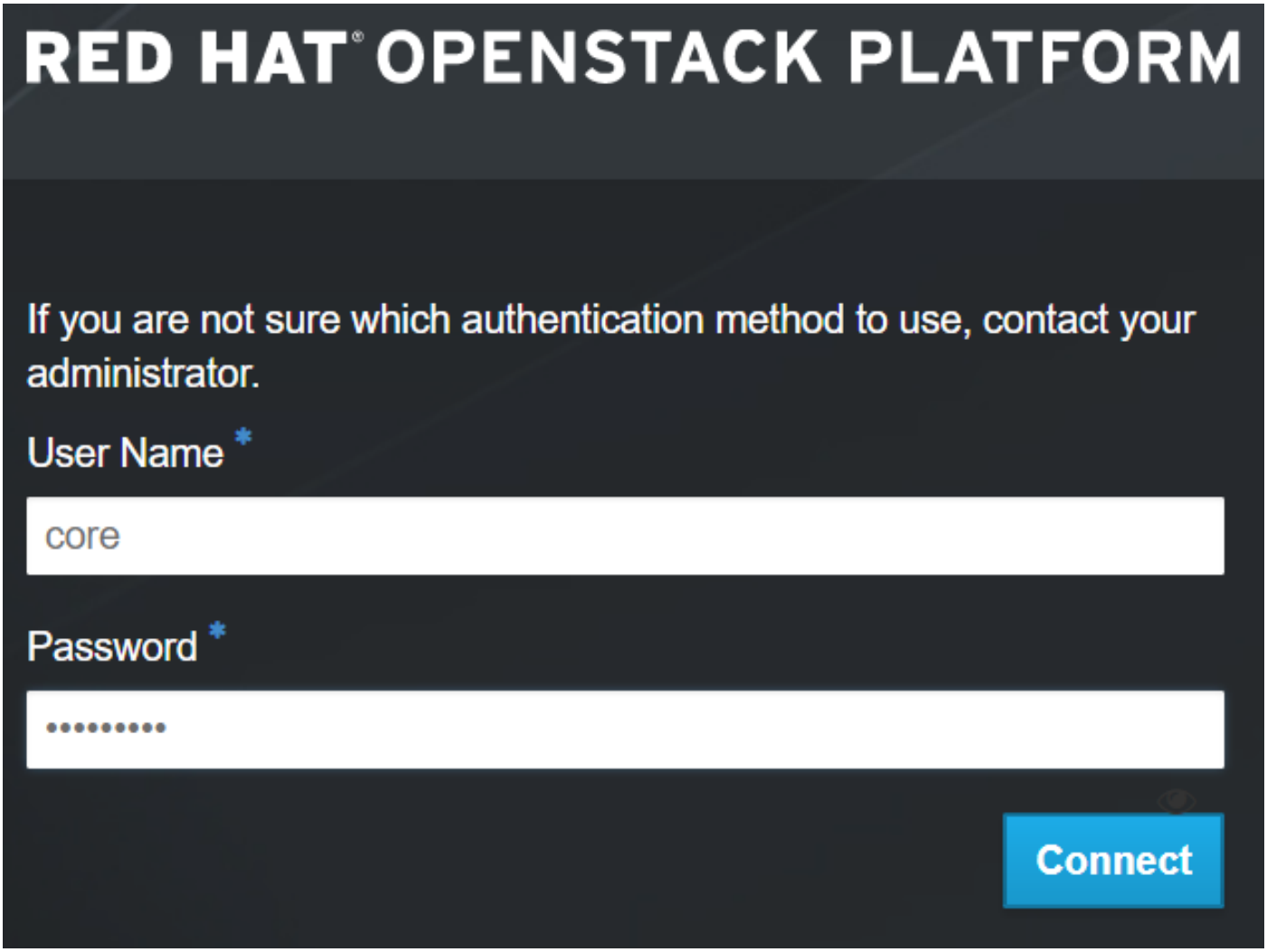
- Secure Shell (SSH)-Konnektivität mit der VM oder dem Server
- Aktualisieren Sie den Hostnamen und den gleichen Hostnamen in **/etc/hosts.**
- Die Liste enthält das RPM, das für die Installation der CPAR-GUI erforderlich ist.

Required 64-bit rpms for Relevant RHEL OS Versions

rpm	RHEL OS Version 6.6	RHEL OS Version 7.0	RHEL OS Version 7.2
glibc	Yes	Yes	Yes
gdome2	Yes	Yes	Yes
glib	Yes	Yes	Yes
glib2	Yes	Yes	Yes
libgcc	Yes	Yes	Yes
libstdc++	Yes	Yes	Yes
libxml2	Yes	Yes	Yes
ncurses	No	No	No
nspr	Yes	Yes	Yes
nss	No	No	No
zlib	Yes	Yes	Yes
nss-softokn-freebl	Yes	Yes	Yes
ncurses-libs	Yes	Yes	Yes
nss-util	Yes	Yes	Yes
gamin	Yes	Yes	Yes
libselinux	Yes	Yes	Yes

Schritt 1: Öffnen Sie über die Horizon-Schnittstelle einen beliebigen Internet-Browser und eine entsprechende IP-Adresse.

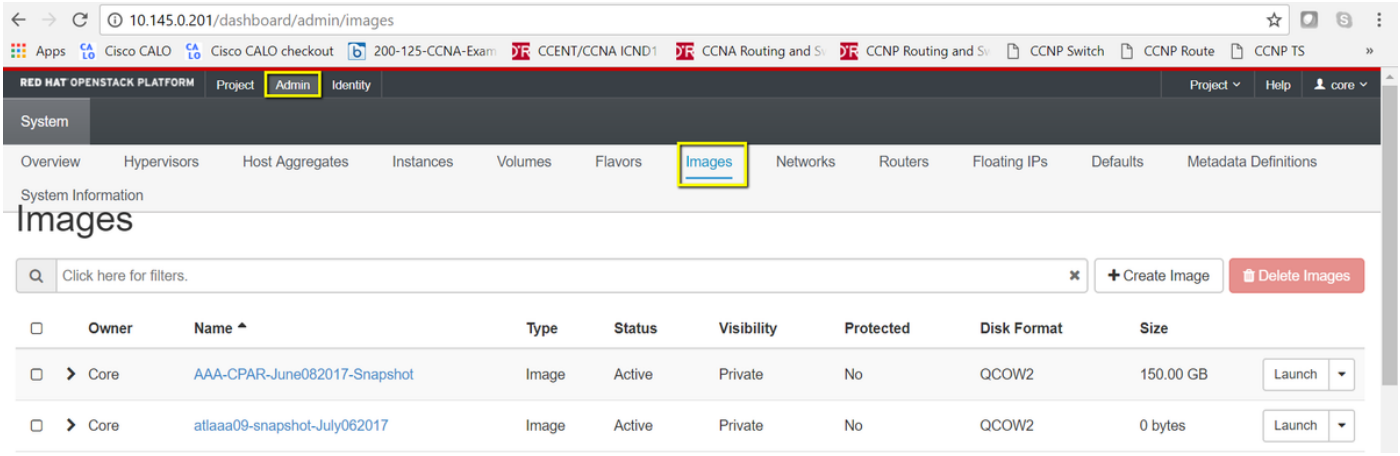
Schritt 2: Geben Sie die entsprechenden Benutzeranmeldeinformationen ein, und klicken Sie auf die Schaltfläche **Verbinden**.



RHEL-Bild in Horizon hochladen

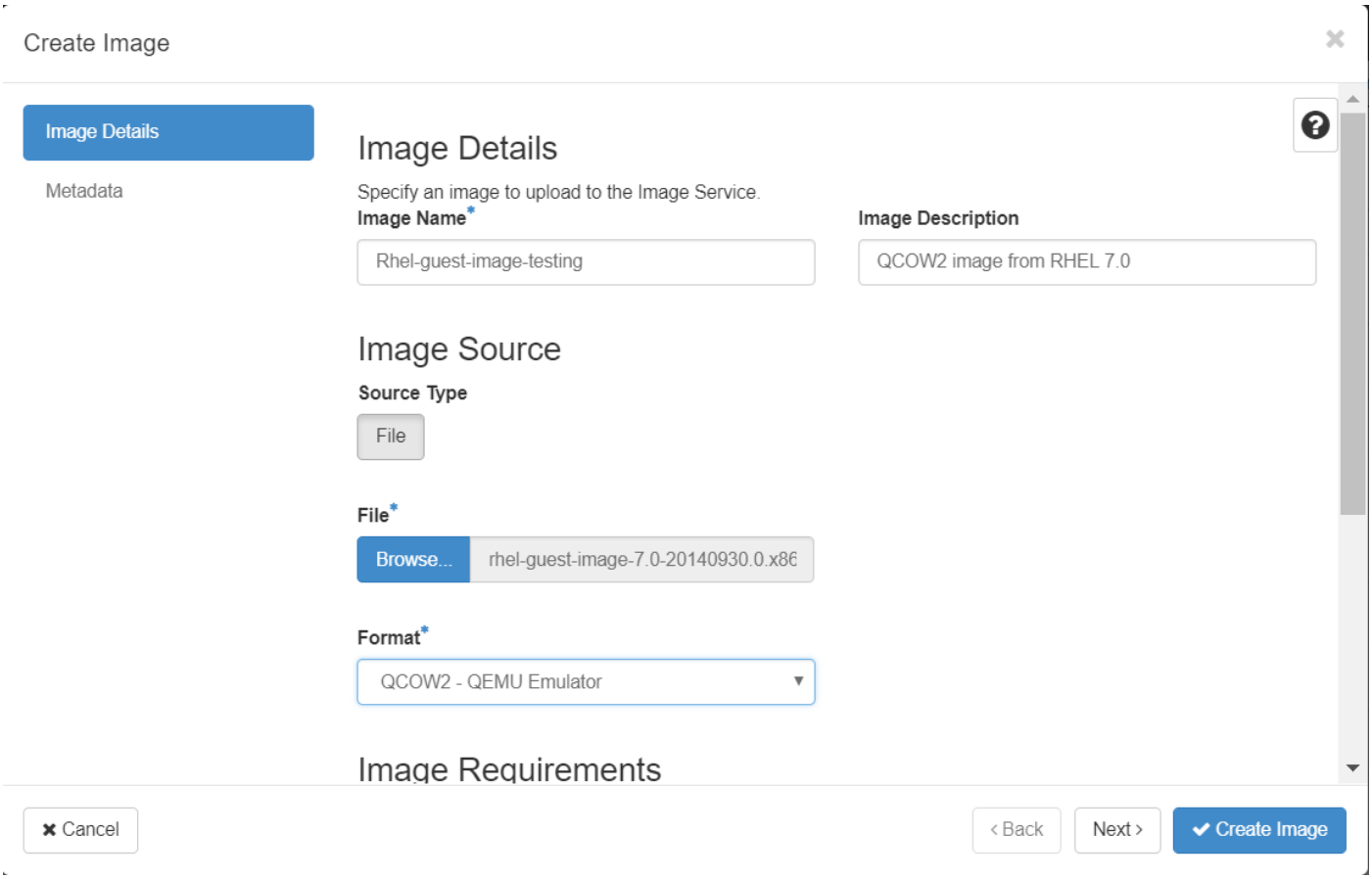
Schritt 1: Navigieren Sie zu **Content Repository**, und laden Sie die Datei mit dem Namen **Rhel-Image** herunter. Dies ist ein angepasstes QCOW2 Red Hat-Image für CPAR AAA-Projekt.

Schritt 2: Wechseln Sie zurück zur Registerkarte Horizont und folgen Sie der Route **Admin > Images** wie im Bild gezeigt.



Schritt 3: Klicken Sie auf die Schaltfläche **Bild erstellen**. Füllen Sie die als **Bildname** und **Bildbeschreibung** bezeichneten Dateien aus, und wählen Sie die QCOW2-Datei aus, die zuvor unter Schritt 1 heruntergeladen wurde. durch Klicken auf **Durchsuchen** im Dateibereich und

Auswahl der Option **QCOW2-QUEMU-Emulator** im Abschnitt **Formatierung**.
Klicken Sie dann auf **Bild erstellen** wie im Bild gezeigt.



Neuen Typ erstellen

Aromen stellen die Ressourcenvorlage dar, die in der Architektur jeder Instanz verwendet wird.

Schritt 1: Navigieren Sie im oberen Horizon-Menü zu **Admin > Flavors** (**Admin > Aromen),** wie im Bild gezeigt.

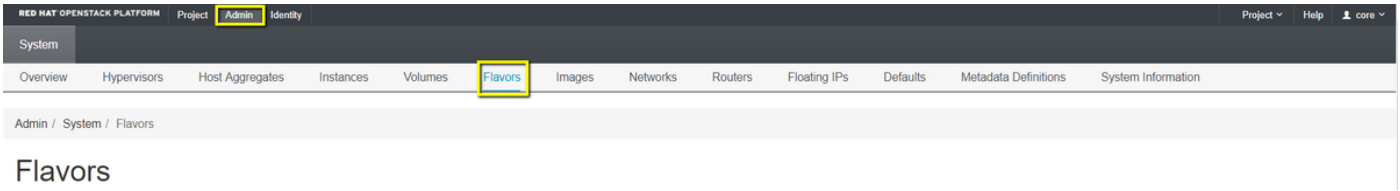


Abbildung 4 Abschnitt "Horizon Flavors".

Schritt 2: Klicken Sie auf die Schaltfläche **Create Flavor** (Typ erstellen).

Schritt 3: Geben Sie im Fenster **Create Flavor (Typ erstellen)** die entsprechenden Ressourceninformationen ein. Dies ist die Konfiguration für den CPAR-Typ:

vCPUs 36

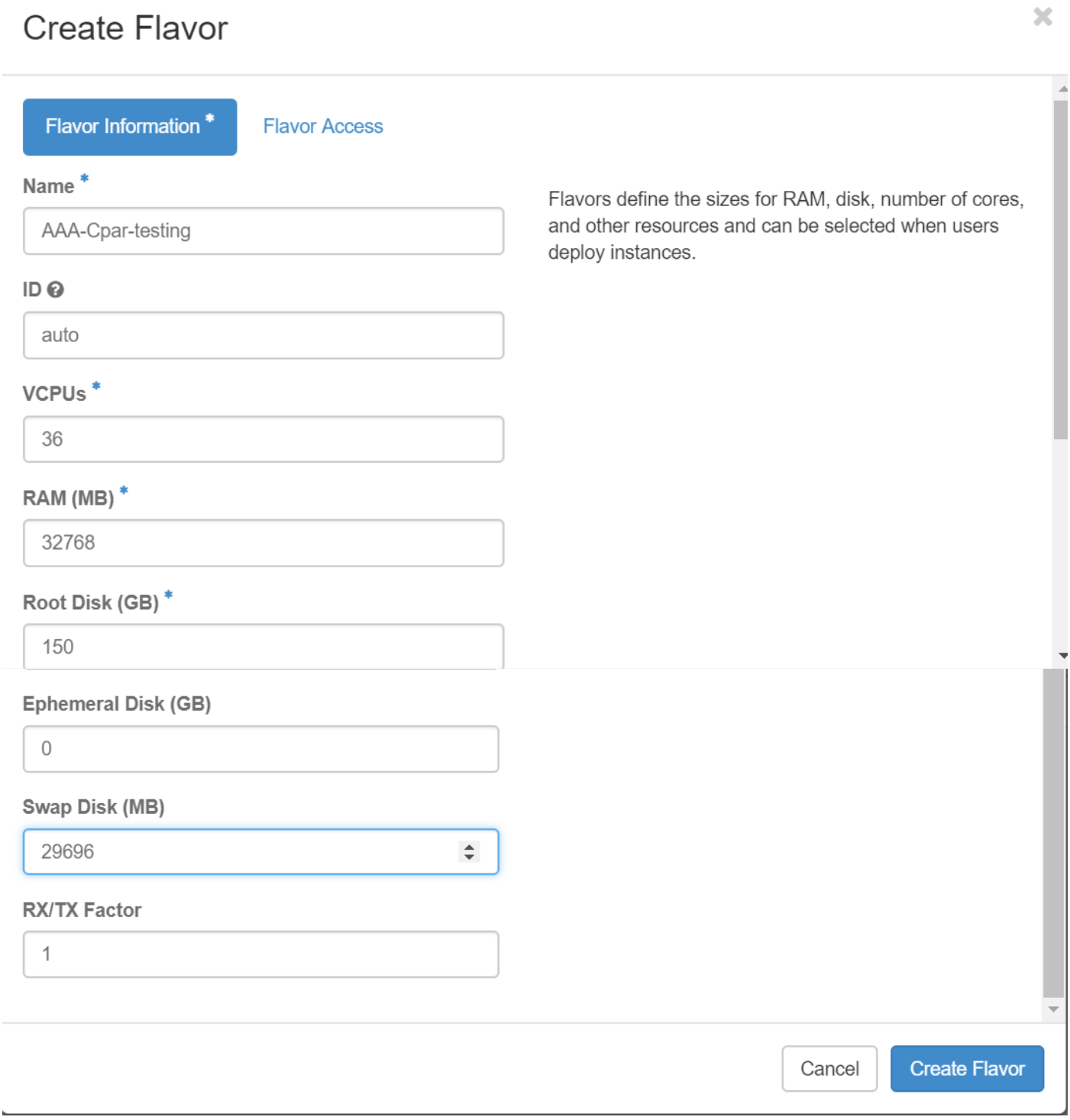
RAM (MB) 32768

Root Disk (GB) 150

Ephemeral Disk (GB) 0

Swap Disk (MB) 29696

RX/TX Factor 1

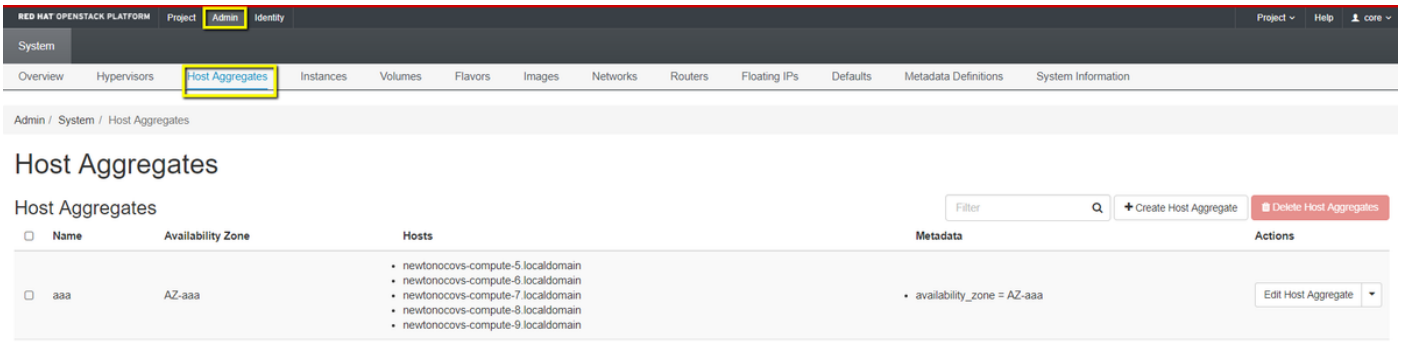


Schritt 4: Klicken Sie im gleichen Fenster auf **Flavor Access** und wählen Sie das Projekt aus, in dem diese Flavor-Konfiguration verwendet werden soll (d. h. Core).

Schritt 5: Klicken Sie auf **Flavour erstellen**.

Erstellen einer Host-Aggregations-/Verfügbarkeitszone

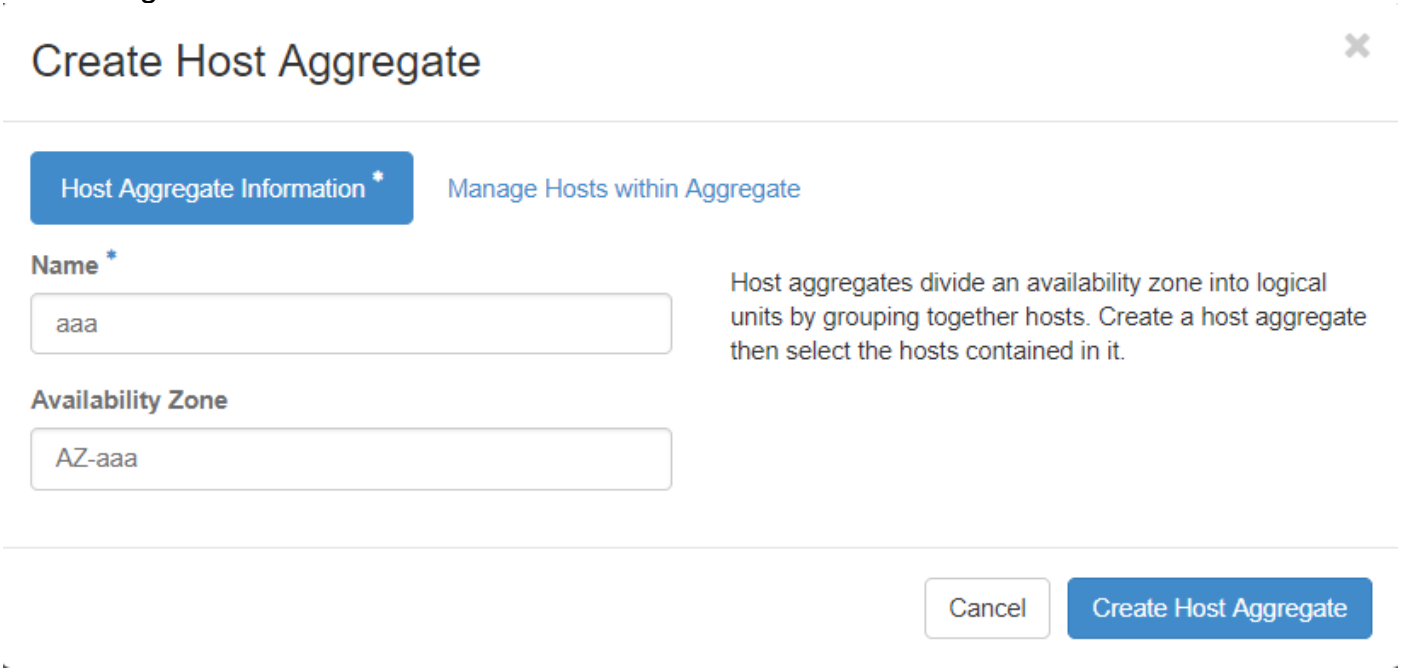
Schritt 1: Navigieren Sie im oberen Horizon-Menü zu **Admin > Host Aggregates (Admin > Host-Aggregate),** wie im Bild gezeigt.



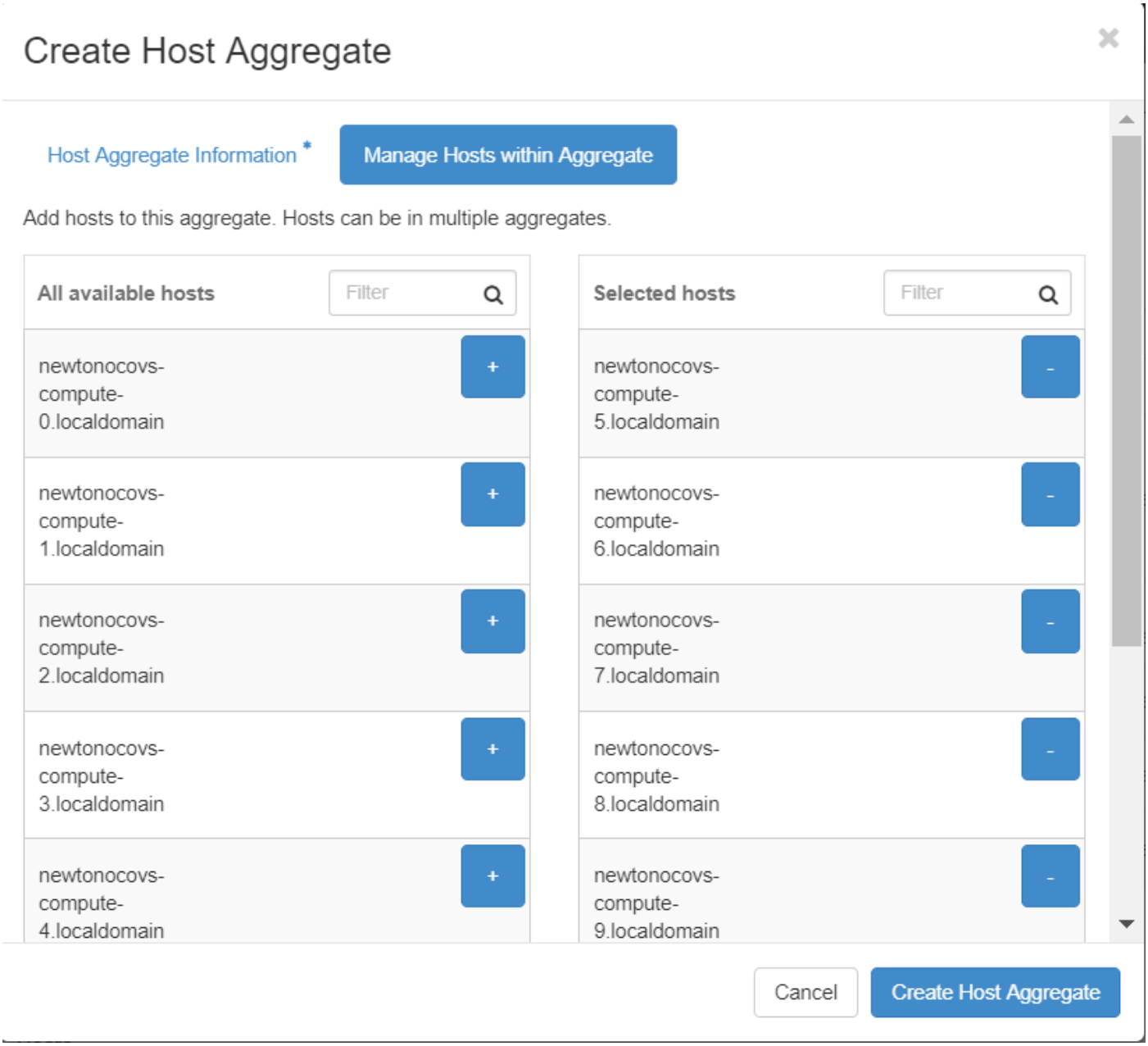
Schritt 2: Klicken Sie auf die Schaltfläche **Create Host Aggregate (Host-Aggregat erstellen**).

Schritt 3: Geben Sie im Label **Host Aggregate Information*** die Felder **Name** und **Verfügbarkeit Zone** mit den entsprechenden Informationen ein. Für die Produktionsumgebung werden diese Informationen derzeit wie im Bild gezeigt verwendet:

- Name: **Aaa**
- Verfügbarkeitszone: **AZ-aaa**



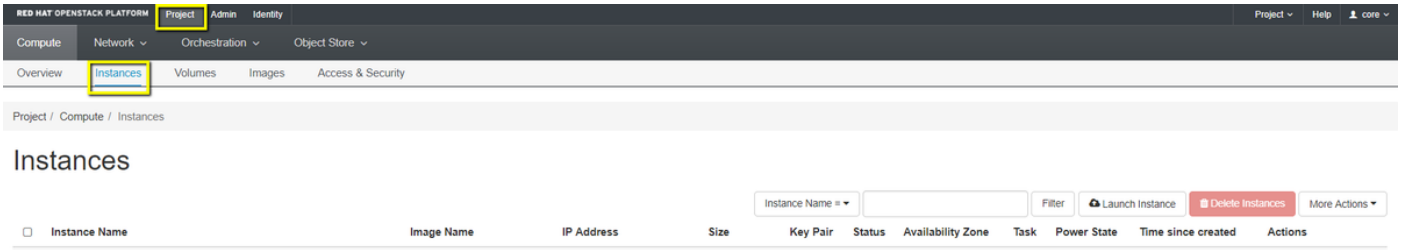
Schritt 4: Klicken Sie auf die Registerkarte **Manage Hosts (Hosts verwalten), und** klicken Sie auf die Schaltfläche **+** für die Hosts, die der neuen Verfügbarkeitszone hinzugefügt werden sollen.



Schritt 5: Klicken Sie abschließend auf die **Schaltfläche "Host Aggregate erstellen"**.

Neue Instanz starten

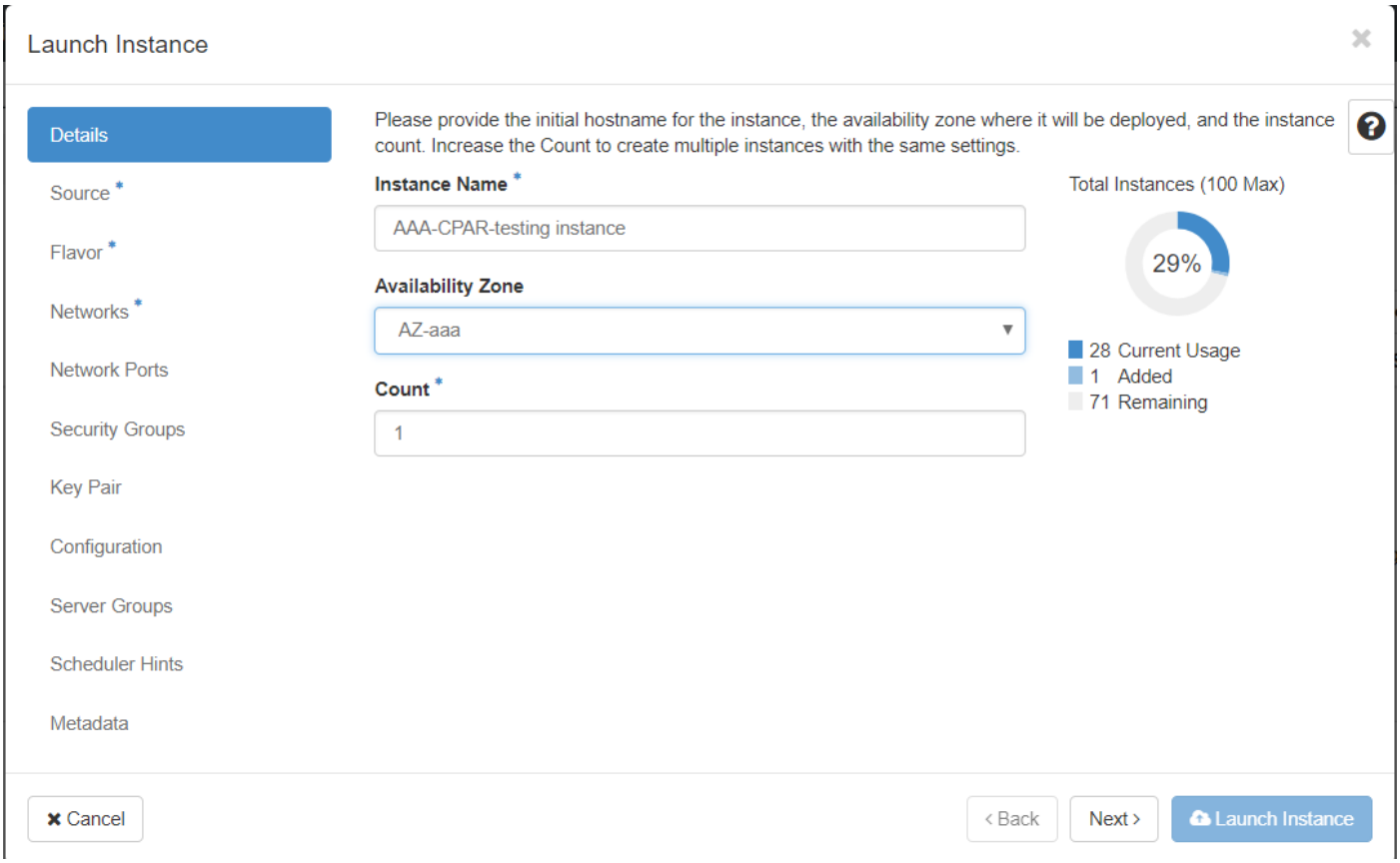
Schritt 1: Navigieren Sie im oberen Horizon-Menü zu **Projekt > Instanzen** wie im Bild gezeigt.



Schritt 2: Klicken Sie auf die Schaltfläche **Instanz starten**.

Schritt 3: Geben Sie auf der Registerkarte **Details** einen geeigneten **Instanznamen** für das neue

virtuelle System ein, wählen Sie die entsprechende **Verfügbarkeitszone** (d. h. AZ-aaa) aus, und legen Sie **Count** auf 1 fest, wie im Bild gezeigt.

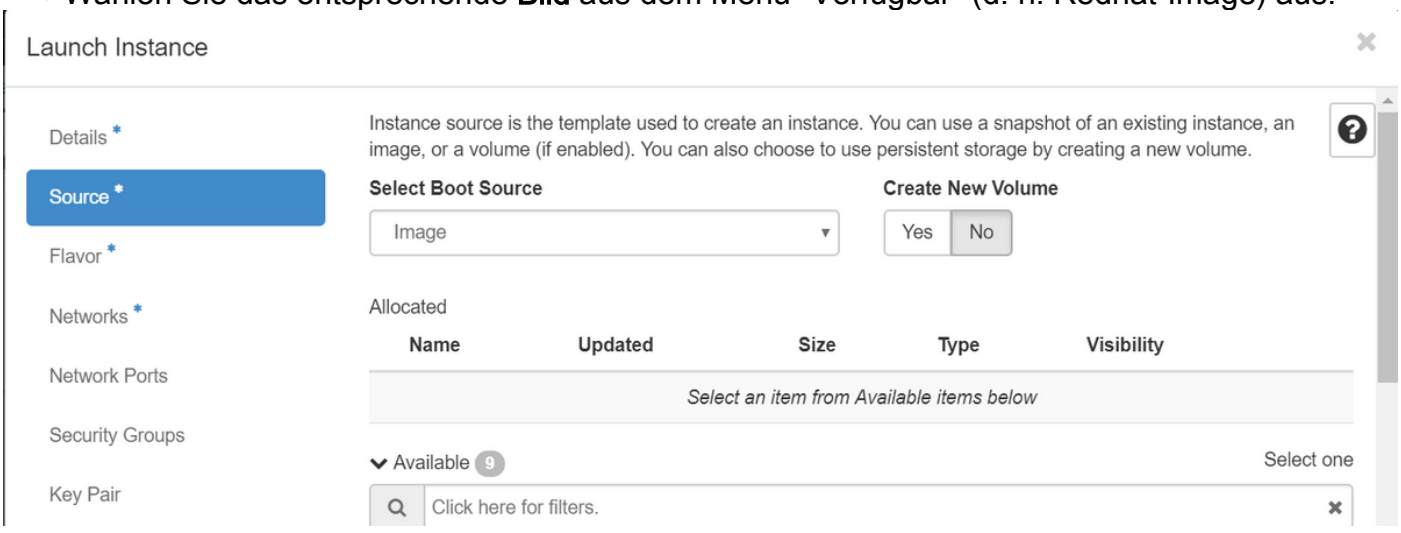


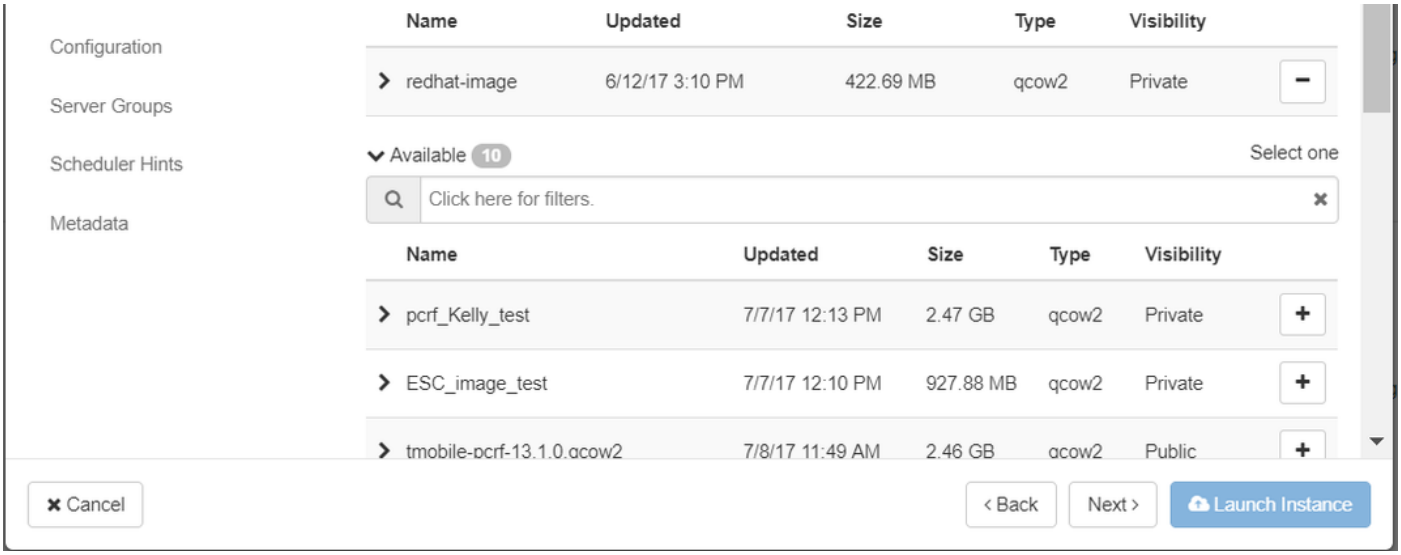
Schritt 4: Klicken Sie auf die Registerkarte **Quelle**, und wählen Sie eine der folgenden Verfahren aus und führen Sie sie aus:

1. Starten einer Instanz basierend auf einem RHEL-Image.

Legen Sie die Konfigurationsparameter wie folgt fest:

- **Startquelle** auswählen: Bild
- **Neues Volumen** erstellen: Nein
- Wählen Sie das entsprechende **Bild** aus dem Menü **"**Verfügbar" (d. h. Redhat-Image) aus.

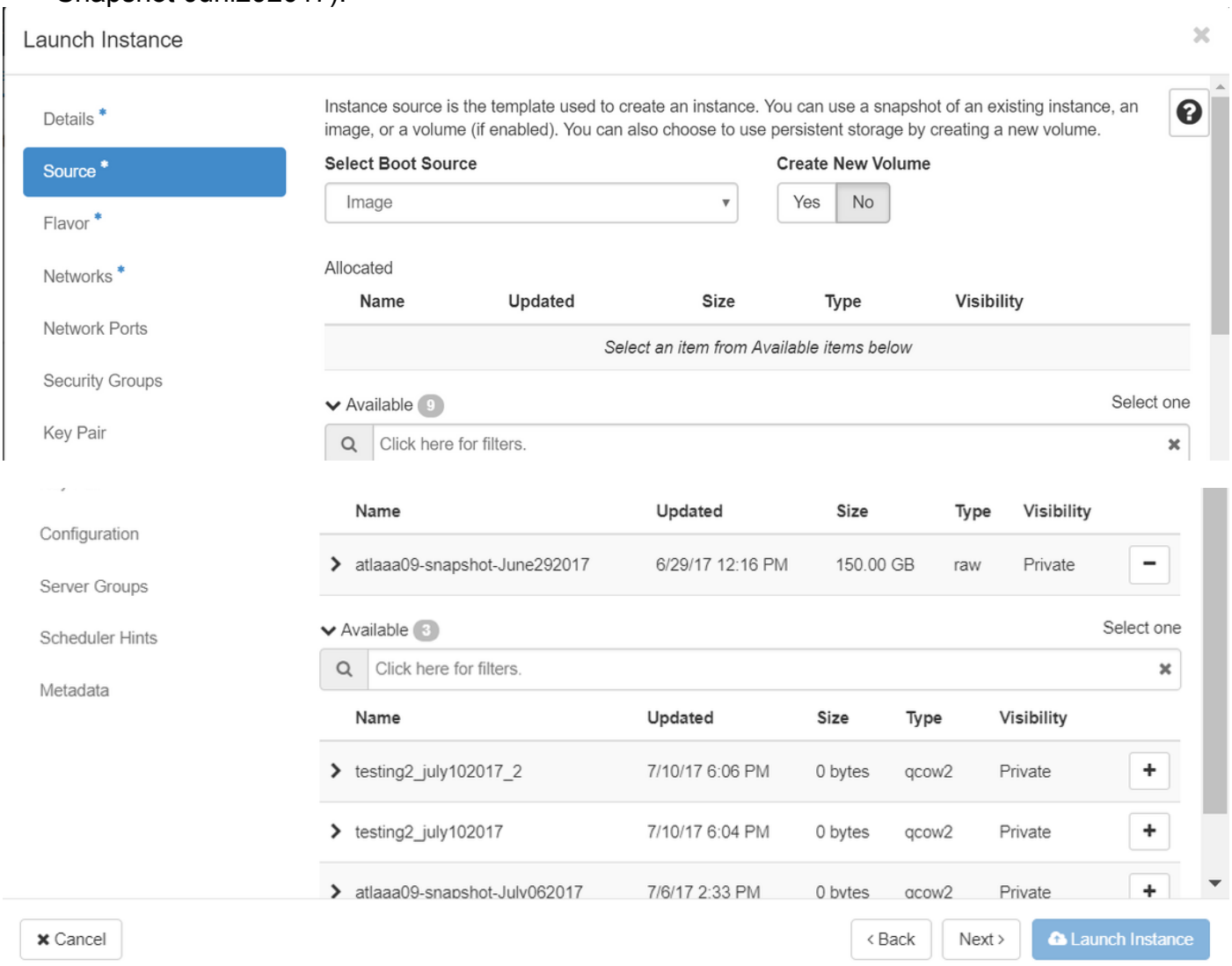




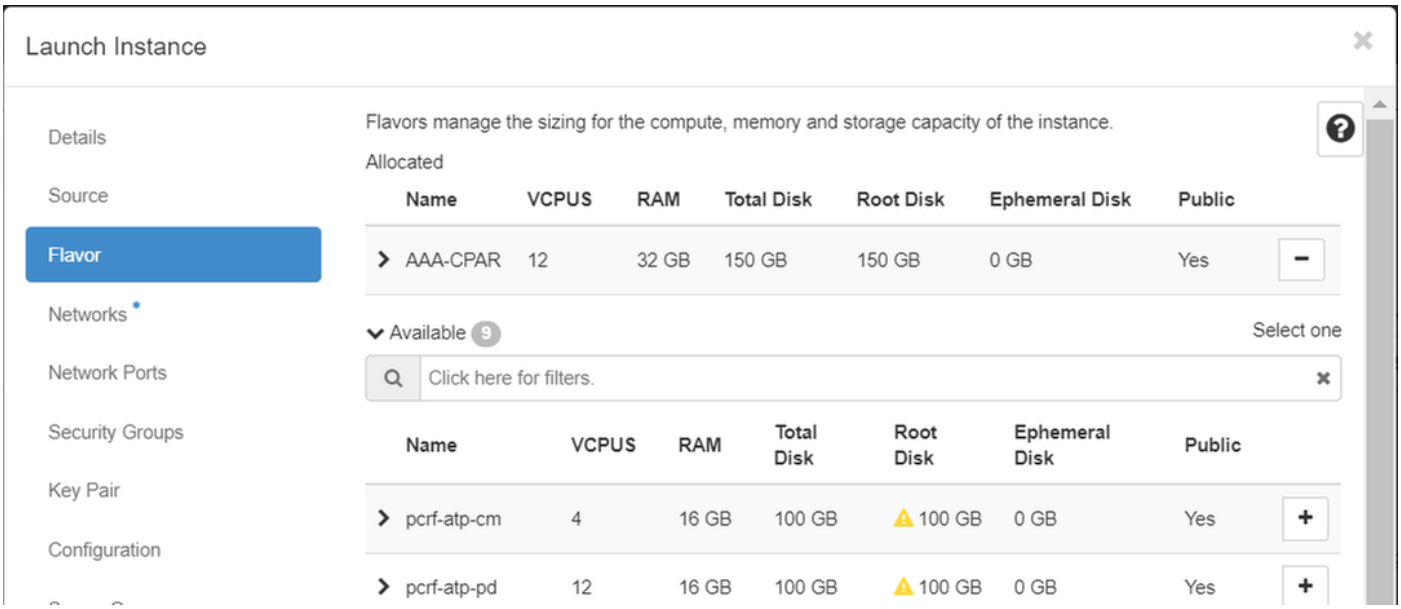
2. Starten einer Instanz auf Basis eines Snapshots.

Legen Sie die Konfigurationsparameter wie folgt fest:

- **Startquelle** auswählen: InstanzSnapshot
- **Neues Volumen** erstellen: Nein
- Wählen Sie den entsprechenden Snapshot aus dem Menü "Verfügbar" aus (d. h. aaa09-Snapshot-Juni292017).

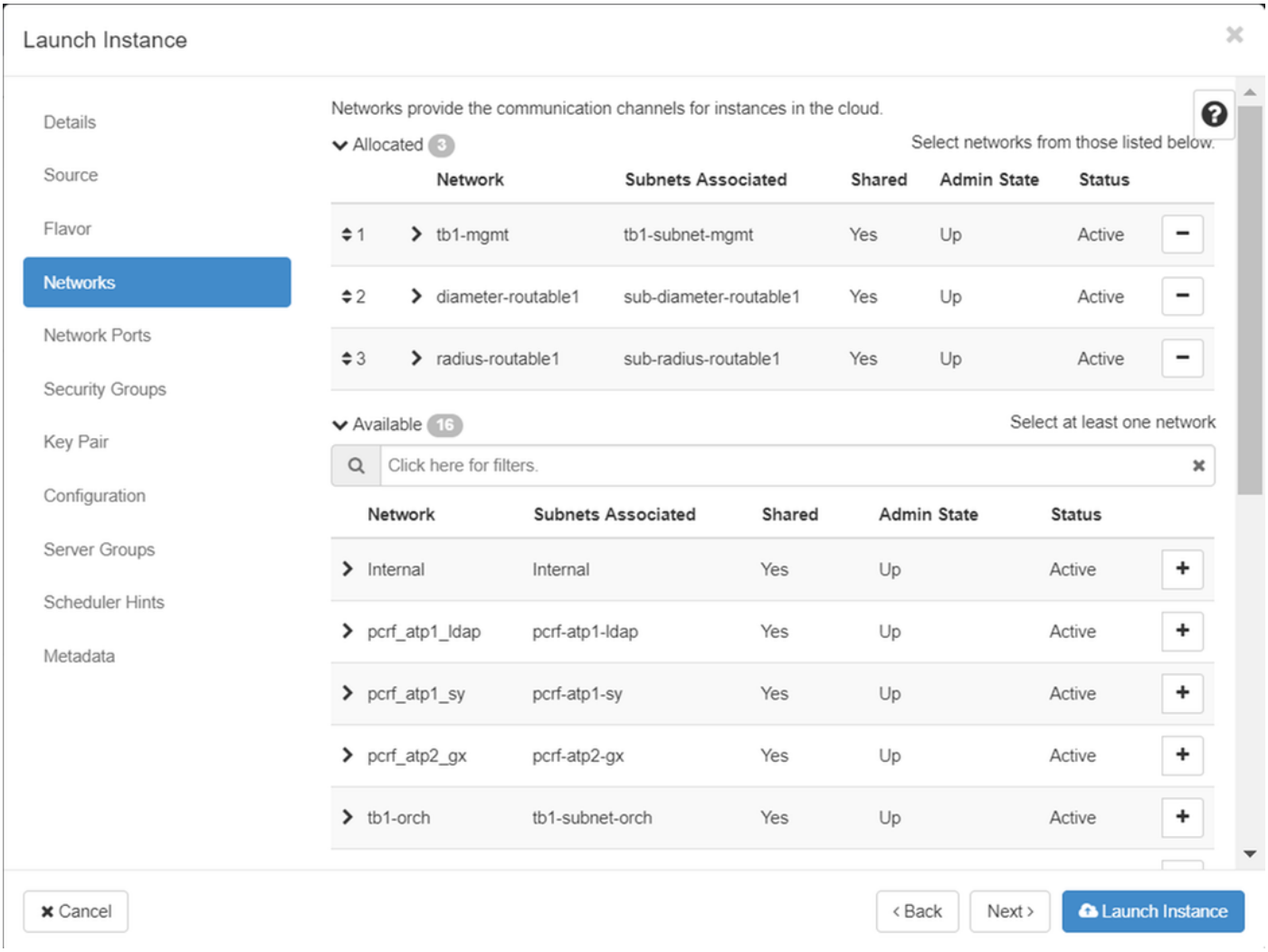


Schritt 5: Klicken Sie auf die Registerkarte **Flavor** und wählen Sie den im Abschnitt **Neuer Geschmack erstellen** erstellten Geschmack aus.



Schritt 6: Klicken Sie auf die Registerkarte **Netzwerke**, und wählen Sie die entsprechenden Netzwerke aus, die für jede Ethernet-Schnittstelle der neuen Instanz/VM verwendet werden. Diese Konfiguration wird derzeit für die Produktionsumgebung verwendet:

- eth0 = **tb1-mgmt**
- eth1 = **routbar mit Durchmesser1**
- eth2 = **Radius-routbar1**



Schritt 7: Klicken Sie abschließend auf die Schaltfläche **Instanz starten**, um die Bereitstellung der neuen Instanz zu starten.

Erstellen und Zuweisen einer Floating-IP-Adresse

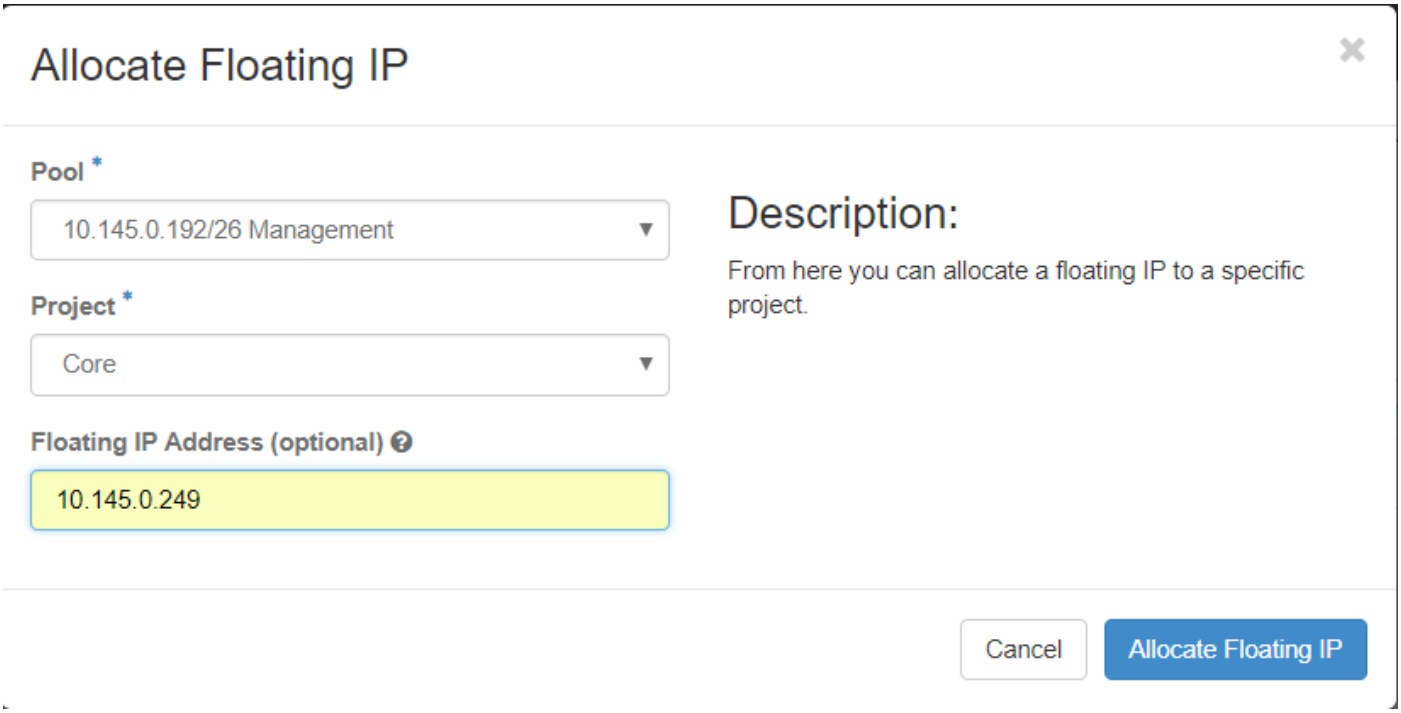
Eine Floating-IP-Adresse ist eine routbare Adresse, d. h., sie ist von der Außenseite der Ultra M/OpenStack-Architektur aus erreichbar und kann mit anderen Knoten aus dem Netzwerk kommunizieren.

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:

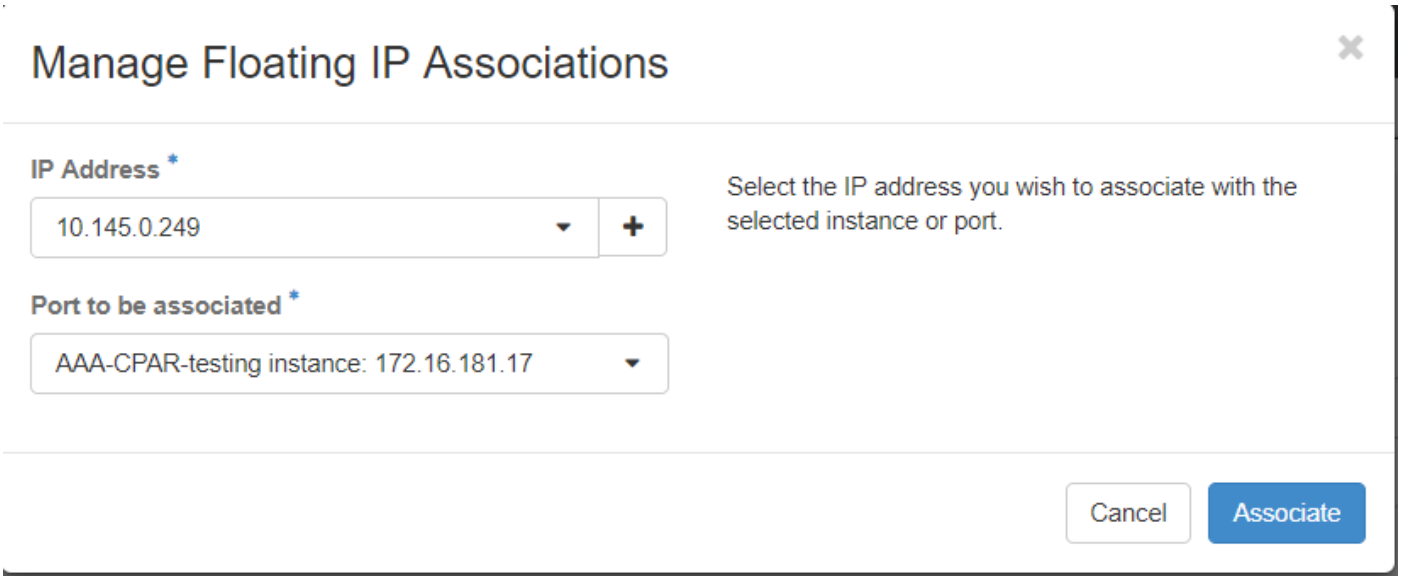


Schritt 4: Klicken Sie auf die Schaltfläche **Zuweisen von Floating-IP**.

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 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 abschließend auf die Schaltfläche **Zuordnen**.

SSH aktivieren

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

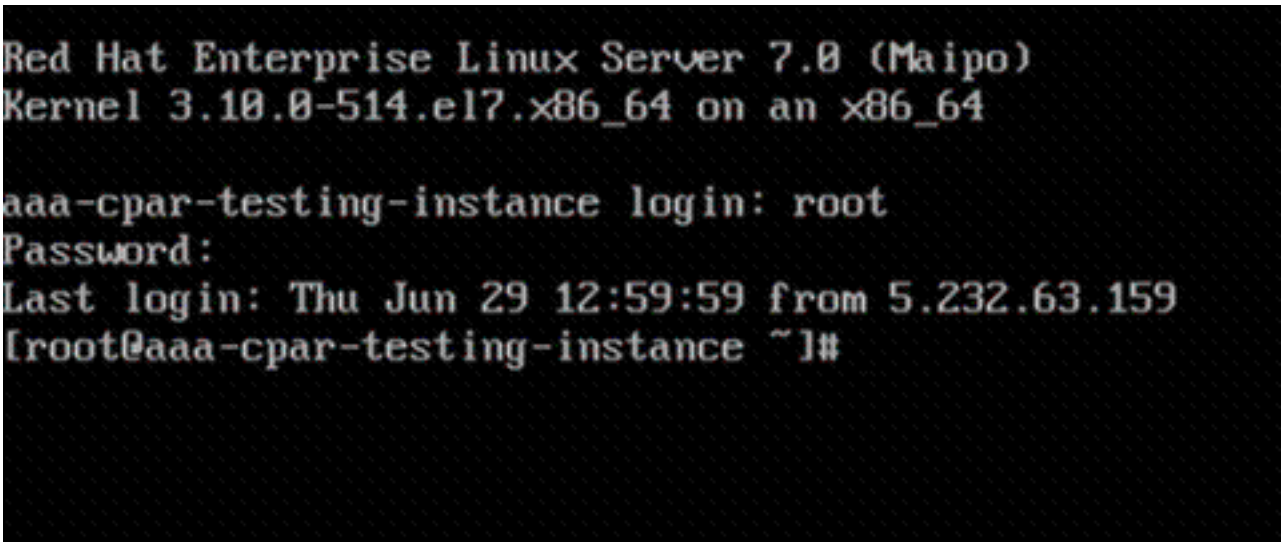
Schritt 2: Klicken Sie auf den Namen der im Abschnitt **Neue Instanz starten** erstellten Instanz/VM.

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

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

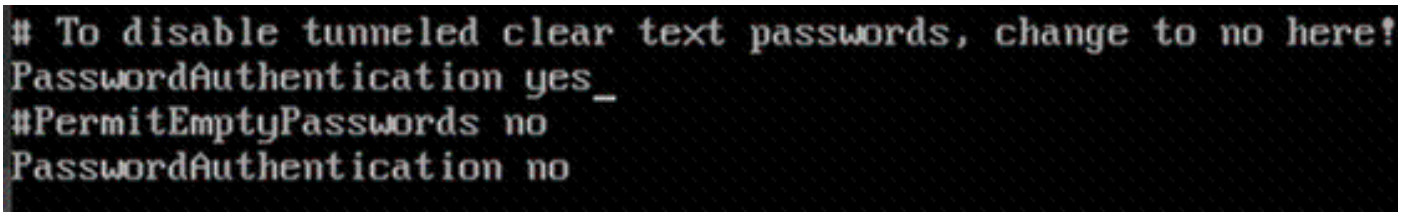
Benutzername: **xxxxx**

Kennwort: **xxxxx**



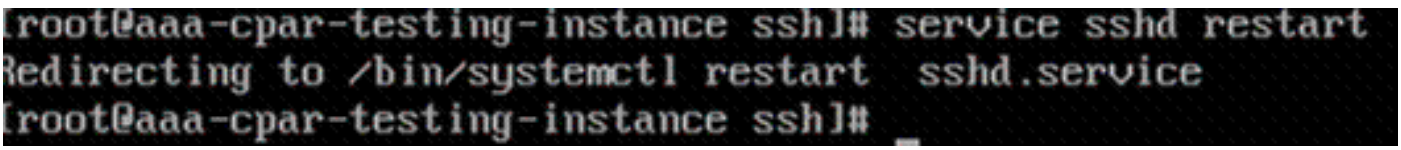
Schritt 5: Geben Sie in der CLI den Befehl **vi /etc/ssh/sshd_config** ein, um die SSH-Konfiguration zu bearbeiten.

Schritt 6: Wenn die SSH-Konfigurationsdatei geöffnet ist, drücken Sie **I**, um die Datei zu bearbeiten. Suchen Sie dann nach dem Abschnitt hier, 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 mit der Floating-IP-Adresse herzustellen, die der Instanz (d. h. 10.145.0.249) und dem Benutzer-**Root** zugewiesen wurde.

```
[2017-07-13 12:12.09]  ~
[dieaguil.DIEAGUIL-CWRQ7] ➤ ssh root@10.145.0.249
Warning: Permanently added '10.145.0.249' (RSA) to the list of known hosts
.
root@10.145.0.249's password:
X11 forwarding request failed on channel 0
Last login: Thu Jul 13 12:58:18 2017
[root@aaa-cpar-testing-instance ~]#
[root@aaa-cpar-testing-instance ~]#
```

Einrichten einer SSH-Sitzung

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

```
[dieaguil.DIEAGUIL-CWRQ7] ➤ ssh root@10.145.0.59
X11 forwarding request failed on channel 0
Last login: Wed Jun 14 17:12:22 2017 from 5.232.63.147
[root@dalaaa07 ~]#
```

CPAR-Software und -Lizenzen hochladen

Schritt 1: Laden Sie das entsprechende Installationsskript für die CPAR-Version (**CSCOar-x.x.x-lnx26_64-install.sh**) von der Cisco Software-Plattform herunter: https://software.cisco.com/download/release.html?mdfid=286309432&flowid=&softwareid=284671441&release=7.2.2.3&relind=AVAILABLE&rellifecycle=&reltype=latest

Cisco Prime Access Registrar for RHEL
CSCOar-7.2.2.3-lnx26_64-install.sh

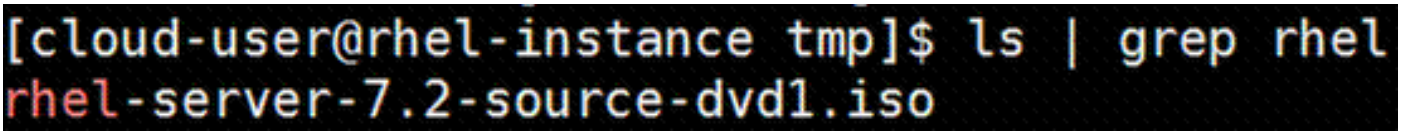
Schritt 2: Laden Sie die Datei **CSCOar-x.x.x.x-lnx26_64-install.sh** in das neue **VM/Server** im **/tmp**-Verzeichnis hoch.

Schritt 3: Laden Sie die entsprechende(n) Lizenzdatei(en) in das neue VM/Server-Verzeichnis **/tmp** hoch.

```
[cloud-user@rhel-instance tmp]$ ls
CSCOar-7.2.2.2-lnx26_64-install.sh  PAR20170317174119435O.lic
```

RHEL/CentOS-Image hochladen

Laden Sie die entsprechende RHEL- oder CentOS**.iso-**Datei in das **VM/Server/tmp-**Verzeichnis.



Yum Repository erstellen

Yum ist ein Linux-Tool, das den Benutzer bei der Installation neuer RPMs mit all ihren Abhängigkeiten unterstützt. Dieses Tool wird bei der Installation der verpflichtenden CPAR-RPMs und beim Upgrade des Kernels verwendet.

Schritt 1: Navigieren Sie zum Verzeichnis **/mnt** mit dem Befehl **cd/mnt,** und erstellen Sie ein neues Verzeichnis mit dem Namen **disk1**, und führen Sie den Befehl mkdir **disk1 aus**.

Schritt 2: Navigieren Sie zum Verzeichnis **/tmp** mit dem Befehl **cd /tmp**, in dem die Datei RHEL oder CentOS**.iso** zuvor hochgeladen wurde, und befolgen Sie die Schritte, die in Abschnitt 3.3 erwähnt wurden.

Schritt 3: Montieren Sie das RHEL/CentOS-Image in das Verzeichnis, das in Schritt 1 erstellt wurde. mit dem Befehl **mount -o loop <Name der ISO-Datei> /mnt/disk1**.

Schritt 4: Erstellen Sie in **/tmp** ein neues Verzeichnis mit dem Namen **repo** unter Verwendung des Befehls **mkdir repo**. Ändern Sie dann die Berechtigungen dieses Verzeichnisses, und führen Sie den Befehl **chmod -R o-w+r repo aus**.

Schritt 5: Navigieren Sie mithilfe des Befehls **cd /mnt/disk1 zum** Verzeichnis Packages des RHEL/CentOS-Images (gemountet auf Schritt 3.). Kopieren Sie alle Packages-Verzeichnisdateien in **/tmp/repo** mit dem Befehl **cp -v * /tmp/repo.**

Schritt 6: Wechseln Sie zurück zum Repo-Verzeichnis, führen Sie **cd /tmp/repo aus**, und verwenden Sie die folgenden Befehle:

```
rpm -Uhvdeltarpm-3.6-3.el7.x86_64.rpm

rpm-Uvh python-deltarpm-3.6-3.el7.x86_64.rpm

rpm -Uvh createrepo-0.9.9-26.el7.noarch.rpm
```

> Diese Befehle installieren die drei erforderlichen RPMs, um Yum zu installieren und zu verwenden. Die zuvor erwähnte RPM-Version kann unterschiedlich sein und hängt von der RHEL/CentOS-Version ab. Wenn eine dieser RPMs nicht im Verzeichnis /Packages enthalten ist, besuchen Sie die Website https://rpmfind.net, von der Sie sie herunterladen können.

Schritt 7: Erstellen Sie ein neues RPM-Repository mit dem Befehl **createrepo /tmp/repo**.

Schritt 8: Navigieren Sie zum Verzeichnis **/etc/yum.repos.d/**mit dem Befehl **cd /etc/yum.repos.d/**. Erstellen Sie eine neue Datei mit dem Namen **myrepo.repo**, die diese Datei mit dem Befehl **vi**

myrepo.repo enthält:

```
[local]

name=MyRepo

baseurl=file:///tmp/repo

enabled=1

gpgcheck=0
```

Drücken Sie **I**, um den Einfügemodus zu aktivieren. Drücken Sie zum Speichern und Schließen die ESC-Taste, und geben Sie dann ":wq!" ein. und drücken Sie die Eingabetaste.

Installation der erforderlichen CPAR-RPMs

Schritt 1: Navigieren Sie mit dem Befehl **cd /tmp/repo zum Verzeichnis /tmp/repo**.

Schritt 2: Installieren Sie die erforderlichen CPAR-RPMs, und führen Sie die folgenden Befehle aus:

```
yum install bc-1.06.95-13.el7.x86_64.rpm

yum install jre-7u80-linux-x64.rpm

yum install sharutils-4.13.3-8.el7.x86_64.rpm

yum install unzip-6.0-16.el7.x86_64.rpm
```

> **Hinweis**: Die Version der RPMs kann unterschiedlich sein und hängt von der RHEL/CentOS-Version ab. Wenn eine dieser RPMs nicht im Verzeichnis /Packages enthalten ist, besuchen Sie die Website https://rpmfind.net, auf der sie heruntergeladen werden können. Um **Java SE 1.7** RPM herunterzuladen, lesen Sie http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase7-521261.html und laden Sie jre**-7u80-**linux**-x64.rpm herunter**.

Kernel-Upgrade auf Version 3.10.0-693.1.1.el7

Schritt 1: Navigieren Sie zum Verzeichnis **/tmp/repo** mit dem Befehl **cd /tmp/repo**.

Schritt 2: Installieren Sie **kernel-3.10.0-514.el7.x86_64** RPM und führen Sie den Befehl **yum install kernel-3.10.0-693.1.1.el7.x86_64.rpm aus**.

Schritt 3: Starten Sie VM/Server mithilfe des Befehls **reboot** neu.

Schritt 4: Wenn der Computer wieder startet, überprüfen Sie, ob die Kernel-Version aktualisiert wurde und führen Sie den Befehl **uname -r aus**. Die Ausgabe muss **3.10.0-693.1.1.el7.x86_64 lauten**.

Netzwerkparameter einrichten

Ändern des Hostnamens

Schritt 1: Öffnen Sie im Schreibmodus die Datei **/etc/hosts** und führen Sie den Befehl **vi /etc/hosts aus**.

Schritt 2: Drücken Sie **I**, um den Einfügemodus zu aktivieren, und schreiben Sie die entsprechenden Informationen zum Hostnetzwerk. Befolgen Sie dieses Format:

```
<Diameter interface IP>          <Host's FQDN>          <VM/Server's hostname>
```

Beispiel: **10.178.7.37 aaa07.aaa.epc.mnc30.mcc10.3gppnetwork.org aaa07**

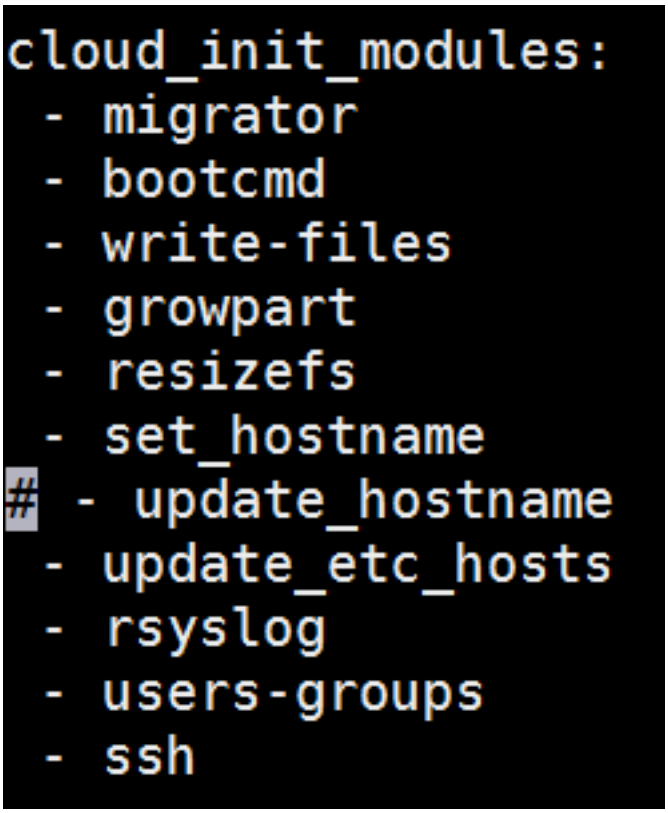
Schritt 3: Speichern Sie die Änderungen, schließen Sie die Datei, indem Sie die ESC-Taste drücken und anschließend "**:wq!**" schreiben. und die Eingabetaste drücken.

Schritt 4: Führen Sie den Befehl **hostnametl set-hostname <Host's FQDN>aus**. Beispiel: **hostnameTL set-hostname aaa.epc.mnc.mcc.3gppnetwork.org**.

Schritt 5: Starten Sie den Netzwerkdienst mit dem Befehl service network restart neu.

Schritt 6: Überprüfen Sie, ob die Hostnamenänderungen übernommen wurden, und führen Sie die folgenden Befehle aus: **hostname -a**, **hostname -f**, der den Hostnamen und den FQDN von VM/Server anzeigen soll.

Schritt 7: Öffnen **/etc/cloud/cloud_config** mit dem Befehl **vi /etc/cloud/cloud_config** und fügen Sie "**#**" vor Zeile "**- update hostname**" ein. Dadurch wird verhindert, dass der Hostname nach einem Neustart geändert wird. Die Datei sollte wie folgt aussehen:



Einrichten der Netzwerkschnittstellen

Schritt 1: Navigieren Sie zu directory **/etc/sysconfig/network-scripts** unter Verwendung von **cd /etc/sysconfig/network-scripts**.

Schritt 2: Öffnen Sie ifcfg**-eth0** mit dem Befehl **vi ifcfg-eth0**. Dies ist die Verwaltungsschnittstelle. Die Konfiguration sollte wie folgt aussehen.

```
DEVICE="eth0"

BOOTPROTO="dhcp"

ONBOOT="yes"

TYPE="Ethernet"

USERCTL="yes"

PEERDNS="yes"

IPV6INIT="no"

PERSISTENT_DHCLIENT="1"
```

Nehmen Sie alle erforderlichen Änderungen vor, speichern Sie die Datei, indem Sie ESC drücken und die Datei eingeben: wq**!**.

Schritt 3: Erstellen Sie die eth1-Netzwerkkonfigurationsdatei mit dem Befehl **vi ifcfg-eth1**. Dies ist die **Durchmesser-Schnittstelle**. Sie können den Einfügemodus aufrufen, indem Sie **I** drücken und diese Konfiguration eingeben.

```
DEVICE="eth1"

BOOTPROTO="none"

ONBOOT="yes"

TYPE="Ethernet"

USERCTL="yes"

PEERDNS="yes"

IPV6INIT="no"

IPADDR= <eth1 IP>

PREFIX=28

PERSISTENT_DHCLIENT="1"
```

Ändern Sie **<eth1 IP>** für die entsprechende **IP-Adresse** für diese Instanz. Speichern und schließen Sie die Datei, sobald alles in Ordnung ist.

Schritt 4: Erstellen Sie eine eth2-Netzwerkkonfigurationsdatei mit dem **Befehl "commandvi ifcfg-eth2"**. Dies ist die **Radius-Schnittstelle**. Wechseln Sie zum Einfügemodus, indem Sie **I** drücken, und geben Sie die folgende Konfiguration ein:

```
DEVICE="eth2"
```

```
BOOTPROTO="none"

ONBOOT="yes"

TYPE="Ethernet"

USERCTL="yes"

PEERDNS="yes"

IPV6INIT="no"

IPADDR= <eth2 IP>

PREFIX=28

PERSISTENT_DHCLIENT="1"
```

Ändern Sie **<eth2 IP>** die entsprechende **Radius-IP-Adresse** für diese Instanz. Speichern und schließen Sie die Datei, sobald alles in Ordnung ist.

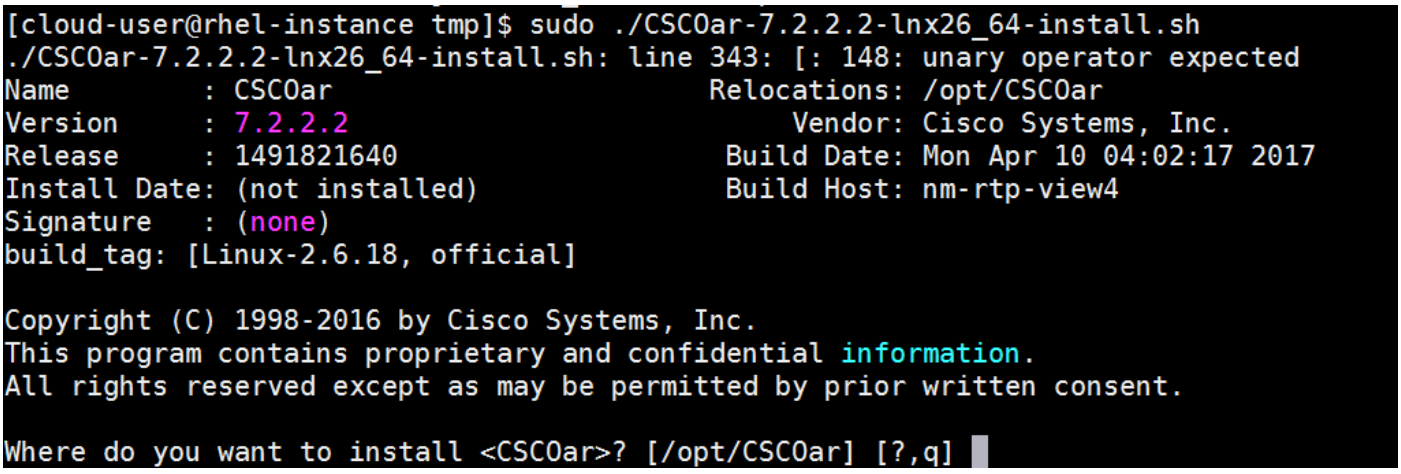
Schritt 5: Starten Sie den Netzwerkdienst mit dem Befehl **service network restart neu**. Überprüfen Sie, ob die Netzwerkkonfigurationsänderungen mithilfe des Befehls **ifconfig** übernommen wurden. Jede Netzwerkschnittstelle sollte über eine IP entsprechend der Netzwerkkonfigurationsdatei (ifcfg-ethx) verfügen. Wenn eth1 oder eth2 nicht automatisch booten, führen Sie den Befehl **ifup ethx aus**.

CPAR installieren

Schritt 1: Navigieren Sie zum Verzeichnis **/tmp**, indem Sie den Befehl **cd /tmp** ausführen.

Schritt 2: Ändern Sie die Berechtigungen für die Datei **./CSCOar-x.x.x.x.x-lnx26_64-install.sh** mit dem Befehl **chmod 775 ./CSCOar-x.x.x.x.-lnx26_64-install.sh**.

Schritt 3: Starten Sie das Installationsskript mit dem Befehl **./CSCOar-x.x.x.x.-lnx26_64-install.sh**.



Schritt 4: Bei der Frage **Wo möchten Sie <CSCOar> installieren? [/opt/CSCOar] [?,q]**, drücken Sie die **Eingabetaste**, um den Standardspeicherort auszuwählen (**/opt/CSCOar/**).

Schritt 5: Nach der Frage **Wo befinden sich die FLEXlm-Lizenzdateien? [] [?,q]** geben Sie den Speicherort der Lizenz(en) an, die **/tmp** sein sollte.

Schritt 6: Für Frage **Wo ist die J2RE installiert? [] [?,q]** geben Sie das Verzeichnis ein, in dem Java

installiert ist. Beispiel: **/usr/java/jre1.8.0_144/.**

Überprüfen Sie, ob es sich um die entsprechende Java-Version für die aktuelle CPAR-Version handelt.

Schritt 7: Überspringen Sie die Oracle-Eingaben, indem Sie die **Eingabetaste** drücken, da Oracle in dieser Bereitstellung nicht verwendet wird.

Schritt 8: Überspringen Sie die Funktionalität von **SIGTRAN-M3UA**, indem Sie die **Eingabetaste** drücken. Diese Funktion ist für diese Bereitstellung nicht erforderlich.

Schritt 9: Für Frage **Soll CPAR als Non-Root-Benutzer ausgeführt werden? [n] [y,n,?,q]** drücken Sie die **Eingabetaste**, um die Standardantwort "n" zu verwenden.

Schritt 10: Frage **Möchten Sie die Beispielkonfiguration jetzt installieren? [n] [y,n,?,q]** drücken Sie die **Eingabetaste**, um die Standardantwort "n" zu verwenden.

Schritt 11: Warten Sie, bis der CPAR-Installationsprozess abgeschlossen ist, und überprüfen Sie dann, ob alle CPAR-Prozesse ausgeführt werden. Navigieren Sie zu Verzeichnis **/opt/CSCOar/bin**, und führen Sie den Befehl **./arstatus aus**. Die Ausgabe sollte wie folgt aussehen:

```
[root@dalaaa06 bin]# ./arstatus
Cisco Prime AR RADIUS server running        (pid: 1192)
Cisco Prime AR Server Agent running         (pid: 1174)
Cisco Prime AR MCD lock manager running     (pid: 1177)
Cisco Prime AR MCD server running           (pid: 1191)
Cisco Prime AR GUI running                  (pid: 1194)
SNMP Master Agent running                 (pid: 1193)
```

SNMP konfigurieren

CPAR-SNMP festlegen

Schritt 1: Öffnen Sie die Datei **snmpd.conf** mit dem Befehl **/cisco-ar/ucd-snmp/share/snmp/snmpd.conf**, um die erforderliche SNMP-Community, die Trap-Community und die IP-Adresse des Trap-Empfängers einzuschließen: Fügen Sie die Zeile **trap2sink xxx.xxx.xxx.xxx cparaasnmp 162 ein**.

Schritt 2: Führen Sie den Befehl **cd /opt/CSCOar/bin aus**, und melden Sie sich mit dem Befehl **./aregcmd bei der CPAR-CLI an,** und geben Sie die Administratorberechtigungen ein.

Schritt 3: Wechseln Sie zu **/Radius/Advanced/SNMP**, und geben Sie den Befehl set **MasterAgentEnabled TRUE aus**. Speichern Sie die Änderungen mithilfe des Befehls **save** und **quit** CPAR CLI Ausgabed Exit.

```
[ //localhost/Radius/Advanced/SNMP ]
    Enabled = TRUE
    TracingEnabled = FALSE
    InputQueueHighThreshold = 90
    InputQueueLowThreshold = 60
    DiaInputQueueHighThreshold = 90
    DiaInputQueueLowThreshold = 60
    MasterAgentEnabled = TRUE
```

Schritt 4: Stellen Sie sicher, dass die CPAR-OIDs über den Befehl **snmpwalk -v2c -c public 127.0.0.1.1** verfügbar sind.

```
[root@snqaaa06 snmp]# snmpwalk -v2c -c public 127.0.0.1 .1
SNMPv2-MIB::sysDescr.0 = STRING: Linux snqaaa06.aaa.epc.mnc300.mcc310.3gppnetwork.org 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (131896) 0:21:58.96
SNMPv2-MIB::sysContact.0 = STRING: Me <me@somewhere.org>
SNMPv2-MIB::sysName.0 = STRING: snqaaa06.aaa.epc.mnc300.mcc310.3gppnetwork.org
SNMPv2-MIB::sysLocation.0 = STRING: Right here, right now.
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
```

Wenn das Betriebssystem den Befehl **snmpwalk** nicht erkennt, navigieren Sie zu **/tmp/repo**, und führen Sie **yum install net-snmp-libs-5.5-49.el6.x86_64.rpm aus**.

BS-SNMP festlegen

Schritt 1: Bearbeiten Sie die Datei **/etc/sysconfig/snmpd,** um Port 50161 für den SNMP-Listener des Betriebssystems anzugeben. Andernfalls wird der Standard-Port 161 verwendet, der derzeit vom CPAR SNMP-Agent verwendet wird.

```
[root@snqaaa06 snmp]# cat /etc/sysconfig/snmpd
# snmpd command line options
# '-f' is implicitly added by snmpd systemd unit file
# OPTIONS="-LS0-6d"
OPTIONS="-LS0-5d -Lf /dev/null -p /var/run/snmpd.pid -x TCP:50161 UDP:50161"
```

Schritt 2: Starten Sie den SNMP-Dienst mit dem Befehl **service snmpd restart neu.**

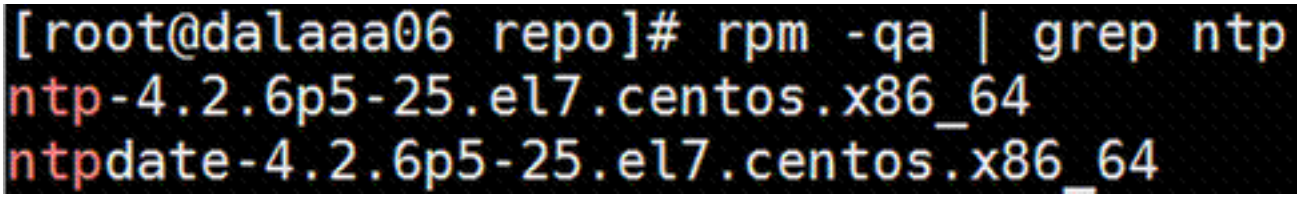
```
[root@snqaaa06 bin]# service snmpd restart
Redirecting to /bin/systemctl restart  snmpd.service
```

Schritt 3: Überprüfen Sie, ob die Betriebssystem-OIDs abgefragt werden können, indem Sie den Befehl **snmpwalk -v2c -c public 127.0.0.1:50161.1 eingeben.**

```
[root@snqaaa06 snmp]# snmpwalk -v2c -c public 127.0.0.1:50161 .1
SNMPv2-MIB::sysDescr.0 = STRING: Linux snqaaa06.aaa.epc.mnc300.mcc310.3gppnetwork.org 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3466) 0:00:34.66
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysName.0 = STRING: snqaaa06.aaa.epc.mnc300.mcc310.3gppnetwork.org
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
```

NTP konfigurieren

Schritt 1: Stellen Sie sicher, dass die NTP-RPMs bereits installiert sind, führen Sie den Befehl **rpm -qa aus. | grep ntp**. Die Ausgabe sollte wie in diesem Bild aussehen.



Wenn die RPMs nicht installiert sind, navigieren Sie zum Verzeichnis **/tmp/repo** unter Verwendung von **cd /tmp/repo,** und führen Sie die folgenden Befehle aus:

```
yum install ntp-4.2.6p5-25.el7.centos.x86_64

yum install ntpdate-4.2.6p5-25.el7.centos.x86:64
```

Schritt 2: Öffnen Sie die **/etc/ntp.conf**-Datei mit dem Befehl **vi /etc/ntp.conf**, und fügen Sie die entsprechenden IPs der NTP-Server für diesen VM/Server hinzu.

Schritt 3: Schließen Sie die Datei **ntp.conf**, und starten Sie den Dienst ntpd mit dem Befehl **service ntpd restart neu**.

Schritt 4: Stellen Sie sicher, dass der VM/Server nun mit dem Befehl **ntpq -p** an die NTP-Server angeschlossen ist.

Verfahren zur Sicherung/Wiederherstellung der CPAR-Konfiguration (optional)

> **Hinweis**: Dieser Abschnitt sollte nur ausgeführt werden, wenn eine vorhandene CPAR-Konfiguration in diesem neuen VM/Server repliziert wird. Dieses Verfahren funktioniert nur für Szenarien, in denen dieselbe CPAR-Version sowohl in Quell- als auch in Zielinstanzen verwendet wird.

Erfassen Sie die CPAR-Konfigurationssicherungsdatei von einer vorhandenen CPAR-Instanz.

Schritt 1: Öffnen Sie eine neue SSH-Sitzung mit der entsprechenden VM, wo die Sicherungsdatei mithilfe von Root-Anmeldeinformationen abgerufen wird.

Schritt 2: Navigieren Sie zum Verzeichnis **/opt/CSCOar/bin** mit dem Befehl **cd /opt/CSCOar/bin**.

Schritt 3: Beenden Sie die CPAR-Dienste, und führen Sie den Befehl **./arserver stop** aus, um dies zu tun.

Schritt 4: Überprüfen Sie, ob der CPAR-Dienst mit dem Befehl **./arstatus** beendet wurde, und suchen Sie nach der Meldung **Cisco Prime Access Registrar Server Agent not running**.

Schritt 5: Um eine neue Sicherung zu erstellen, führen Sie den Befehl **./mcdadmin -e /tmp/config.txt aus**. Geben Sie auf Anfrage die CPAR-Administratoranmeldeinformationen ein.

Schritt 6: Navigieren Sie zum Verzeichnis **/tmp** mit dem Befehl **cd /tmp**. Die Datei **config.txt** dient als Sicherung dieser CPAR-Instanzkonfiguration.

Schritt 7: Laden Sie die **config.txt-**Datei auf das neue VM/Server hoch, auf dem die Sicherung wiederhergestellt werden soll. Verwenden Sie den Befehl **scp config.txt root@<new VM/Server IP>:/tmp**.

Schritt 8: Wechseln Sie zurück zum Verzeichnis **/opt/CSCOar/bin** mit dem Befehl **cd /opt/CSCOar/bin**, und holen Sie CPAR mit dem Befehl **./arserver start** erneut ein.

Wiederherstellen der CPAR-Konfigurations-Sicherungsdatei im neuen VM/Server

Schritt 1: Navigieren Sie im neuen VM/Server zum Verzeichnis **/tmp** mit dem Befehl **cd/tmp,** und überprüfen Sie, ob die Datei **config.txt** in Schritt 7 hochgeladen wurde. des Abschnitts Erhalt der CPAR-Konfigurationssicherungsdatei von einer vorhandenen CPAR-Instanz. Wenn die Datei nicht vorhanden ist, lesen Sie den entsprechenden Abschnitt, und überprüfen Sie, ob der **Befehl scp** erfolgreich ausgeführt wurde.

Schritt 2: Navigieren Sie zum Verzeichnis **/opt/CSCOar/bin** mit dem Befehl **cd /opt/CSCOar/bin,** und deaktivieren Sie den CPAR-Dienst, indem Sie den Befehl **./arserver stop** ausführen.

Schritt 3: Um die Sicherung wiederherzustellen, führen Sie den Befehl **./mcdadmin -coi /tmp/config.txt aus**.

Schritt 4: Schalten Sie den CPAR-Dienst erneut ein, indem Sie den Befehl **./arserver start eingeben**.

Schritt 5: Überprüfen Sie abschließend den CPAR-Status mit dem Befehl **./arstatus**. Die Ausgabe sollte so aussehen.

```
[root@dalaaa06 bin]# ./arstatus
Cisco Prime AR RADIUS server running        (pid: 1192)
Cisco Prime AR Server Agent running         (pid: 1174)
Cisco Prime AR MCD lock manager running     (pid: 1177)
Cisco Prime AR MCD server running           (pid: 1191)
Cisco Prime AR GUI running                  (pid: 1194)
SNMP Master Agent running                 (pid: 1193)
```