

Ersatz defekter Komponenten auf dem Server UCS C240 M4 - CPAR

Inhalt

[Einführung](#)

[Hintergrundinformationen](#)

[Abkürzungen](#)

[Workflow des MoP](#)

[Voraussetzungen](#)

[Sicherung](#)

[Komponenten-RMA - Computing-Knoten](#)

[Identifizieren von im Compute-Knoten gehosteten VMs](#)

[1. Herunterfahren der CPAR-Anwendung](#)

[2. VM-Snapshot-Aufgabe](#)

[VM-Snapshot](#)

[Graceful Power Aus](#)

[Ersetzen einer fehlerhaften Komponente aus dem Computing-Knoten](#)

[VMs wiederherstellen](#)

[Instanz mit Snapshot wiederherstellen](#)

[Floating-IP-Adresse erstellen und zuweisen](#)

[SSH aktivieren](#)

[SSH-Sitzung einrichten](#)

[Komponenten-RMA - OSD-Computing-Knoten](#)

[Identifizieren von VMs, die im OSD-Computing-Knoten gehostet werden](#)

[1. Herunterfahren der CPAR-Anwendung](#)

[2. VM-Snapshot-Aufgabe](#)

[VM-Snapshot](#)

[CEPH im Servicemodus aktivieren](#)

[Graceful Power Aus](#)

[Ersetzen einer fehlerhaften Komponente aus dem OSD-Computing-Knoten](#)

[CEPH aus dem Servicemodus verschieben](#)

[VMs wiederherstellen](#)

[Instanz mit Snapshot wiederherstellen](#)

[Komponenten-RMA - Controller-Knoten](#)

[Vorabprüfung](#)

[Controller-Cluster in Servicemodus verschieben](#)

[Ersetzen einer fehlerhaften Komponente aus dem Controller-Knoten](#)

[Power-On-Server](#)

Einführung

Dieses Dokument beschreibt die erforderlichen Schritte zum Ersetzen fehlerhafter Komponenten,

die hier in einem Unified Computing System (UCS)-Server in einer Ultra-M-Konfiguration aufgeführt sind.

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 auf OpenStack bereitgestellten virtuellen System installiert wird.

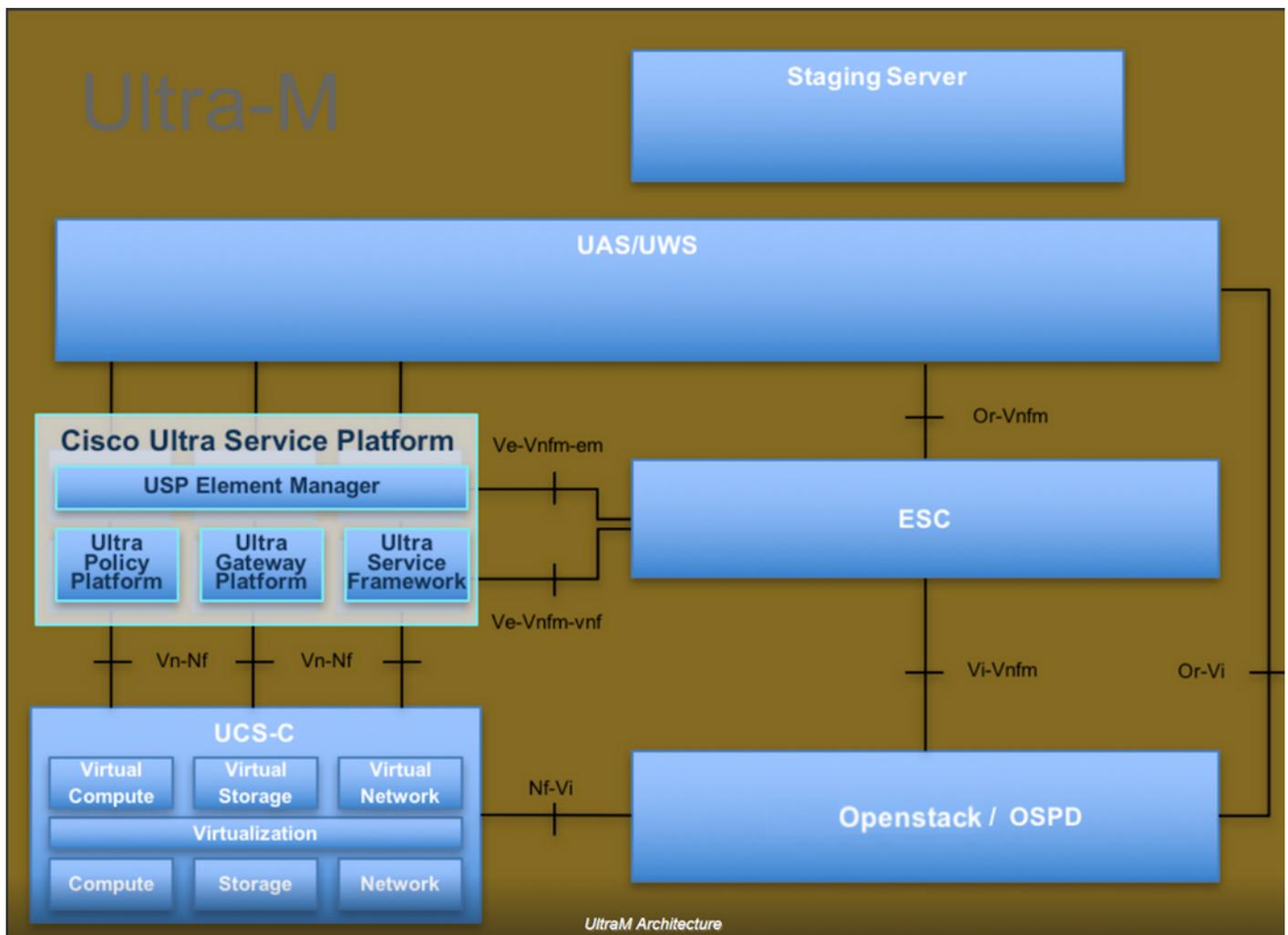
- DIMM-Austauschmodul (Dual In-Line Memory Module)
- FlexFlash-Controller-Fehler
- SSD-Fehler (Solid State Drive)
- Trusted Platform Module (TPM) Failure
- RAID-Cache-Fehler
- RAID-Controller/Hot-Bus-Adapter (HBA)-Fehler
- Fehler der PCI-Risierkarte
- PCIe-Adapter Intel X520 10G-Fehler
- Modularer LAN-on-Motherboard (MLOM)-Fehler
- RMA für Lüftereinschübe
- CPU-Ausfall

Hintergrundinformationen

Ultra-M ist eine vorkonfigurierte und validierte Kernlösung für virtualisierte mobile Pakete, die die Bereitstellung von VNFs vereinfacht. OpenStack ist der Virtualized Infrastructure Manager (VIM) für Ultra-M und besteht aus den folgenden Knotentypen:

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

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



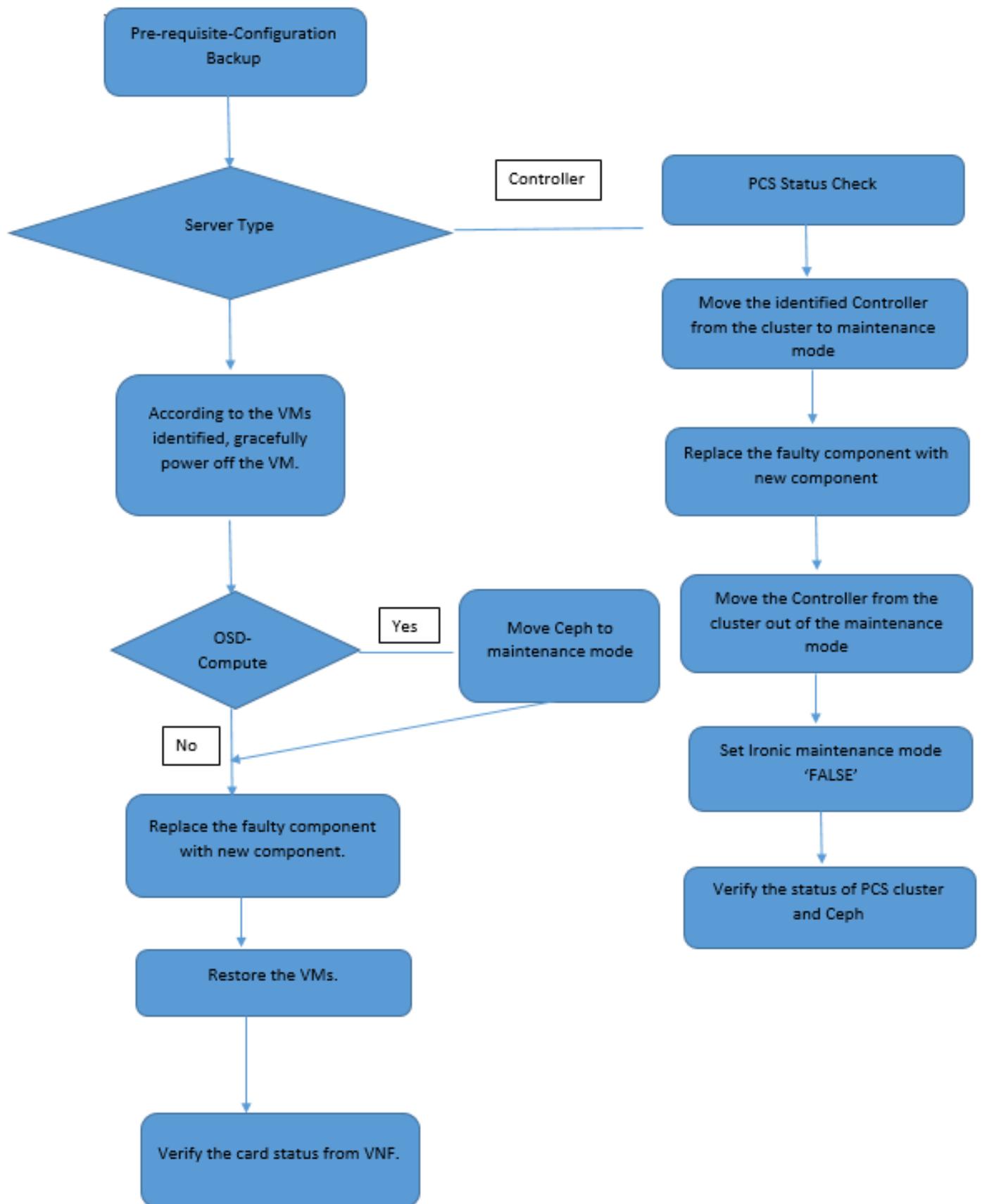
Dieses Dokument richtet sich an Mitarbeiter von Cisco, die mit der Cisco Ultra-M-Plattform vertraut sind. Es beschreibt die Schritte, die für OpenStack und Redhat OS erforderlich sind.

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

Abkürzungen

MoP	Verfahrensweise
OSD	Objektspeicherdatenträger
OSPD	OpenStack Platform Director
HDD	Festplattenlaufwerk
SSD	Solid-State-Laufwerk
VIM	Virtueller Infrastrukturmanager
VM	Virtuelles System
EM	Element Manager
USA	Ultra-Automatisierungsservices
UUID	Universeller Identifikator

Workflow des MoP



Voraussetzungen

Sicherung

Bevor Sie eine fehlerhafte Komponente austauschen, ist es wichtig, den aktuellen Zustand Ihrer

Red Hat OpenStack Platform-Umgebung zu überprüfen. Es wird empfohlen, den aktuellen Zustand zu überprüfen, um Komplikationen zu vermeiden, wenn der Austauschprozess eingeschaltet 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. Darüber hinaus wird empfohlen, die StarOS-Konfiguration zu sichern, insbesondere wenn der Rechner-/OSD-Computing-Knoten, der ersetzt werden soll, als Host für die Control Function (CF) Virtual Machine (VM) fungiert.

Hinweis: Wenn der Server der Controller-Knoten ist, fahren Sie mit dem Abschnitt "" fort, andernfalls fahren Sie mit dem nächsten Abschnitt fort. Stellen Sie sicher, dass Sie über den Snapshot der Instanz verfügen, sodass Sie das virtuelle System bei Bedarf wiederherstellen können. Befolgen Sie die Anweisungen zum Erstellen eines Snapshots des virtuellen Systems.

Komponenten-RMA - Computing-Knoten

Identifizieren von im Compute-Knoten gehosteten VMs

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

```
[stack@a103-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 der UUID, die zweite

Spalte dem VM-Namen und die dritte Spalte dem Hostnamen, in dem die VM vorhanden ist. Die Parameter aus dieser Ausgabe werden in den nachfolgenden Abschnitten verwendet.

Sicherung: SNAPSHOT-PROZESS

1. Herunterfahren der CPAR-Anwendung

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

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

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

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

Die Meldung "Cisco Prime Access Registrar Server Agent heruntergefahren" wird angezeigt. muss erscheinen.

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

```
ERROR:      You cannot 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, beenden Sie diesen Prozess mit dem folgenden Befehl:

```
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
```

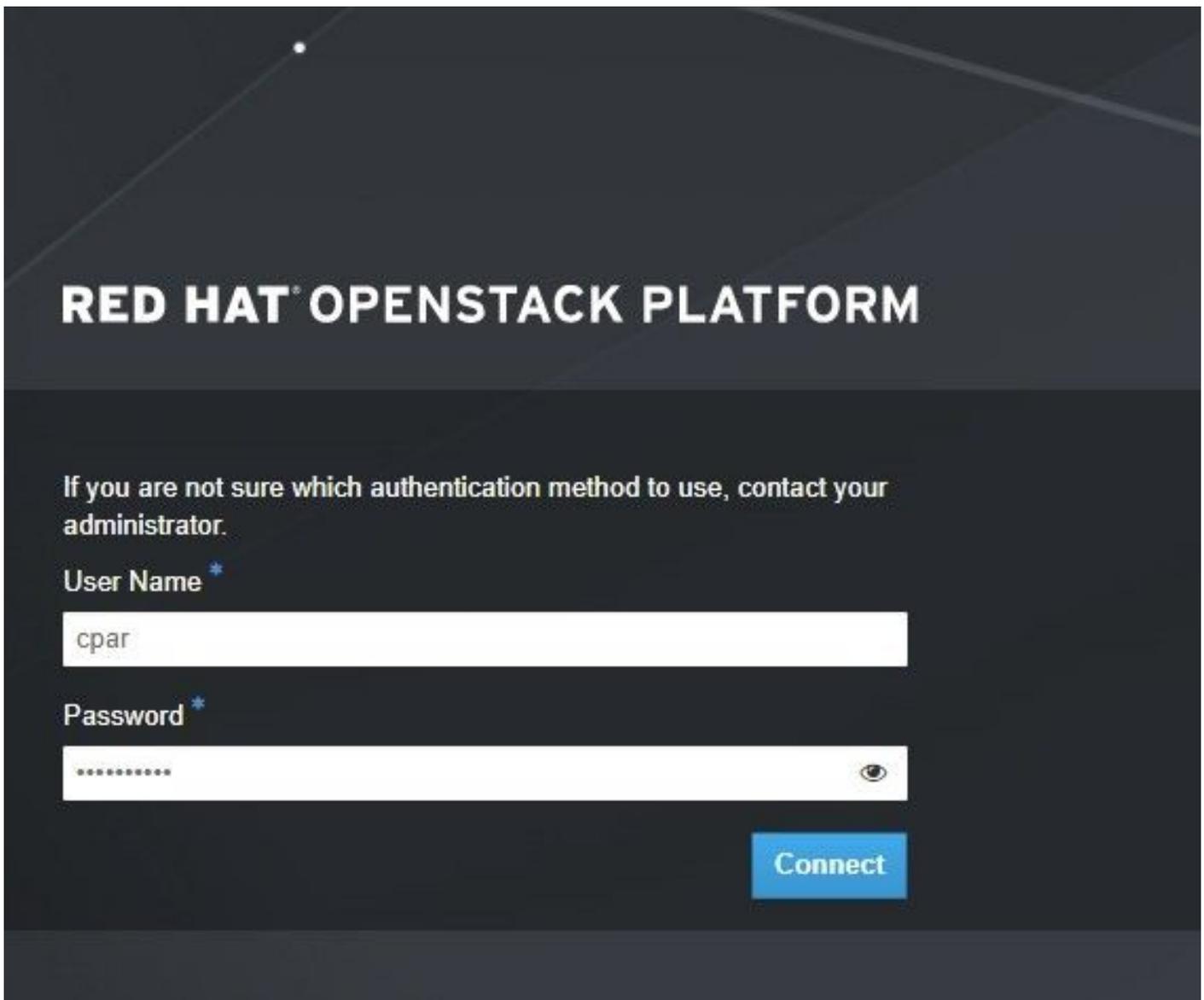
Diese Meldungen müssen angezeigt werden:

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

2. VM-Snapshot-Aufgabe

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

Wenn Sie auf Horizon zugreifen, wird dieser Bildschirm angezeigt.



RED HAT OPENSTACK PLATFORM

If you are not sure which authentication method to use, contact your administrator.

User Name *

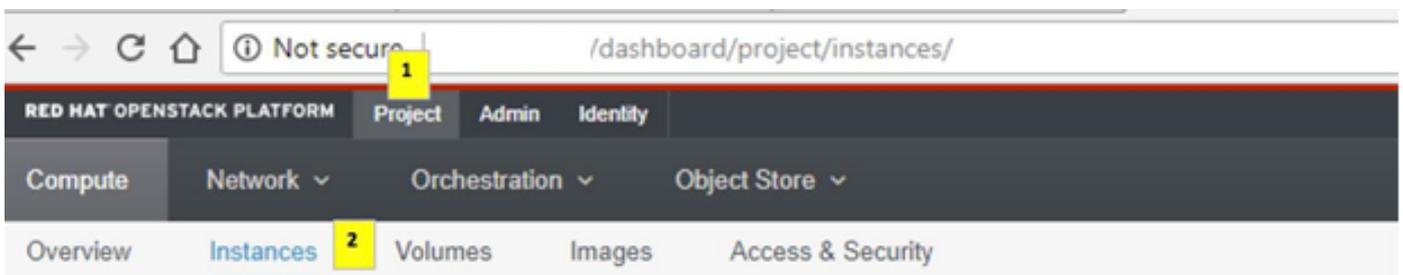
cpar

Password *

.....

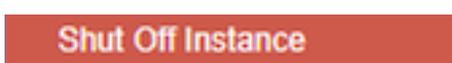
Connect

Schritt 2: Navigieren Sie zu **Projekt > Instanzen** wie in diesem 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 **Aktionen > Deaktivierte Instanz** wie in diesem Bild gezeigt, und bestätigen Sie Ihre Auswahl.



Schritt 4: Überprüfen Sie, ob die Instanz tatsächlich heruntergefahren wurde, indem Sie Status = **Shutoff** und Power State = **Shut Down (Herunterfahren)** wie in diesem Bild gezeigt überprüfen.

Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
AAA-CPAR	-	Shutoff	AZ-dalaaa09	None	Shut Down	3 months, 2 weeks	Start Instance

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.

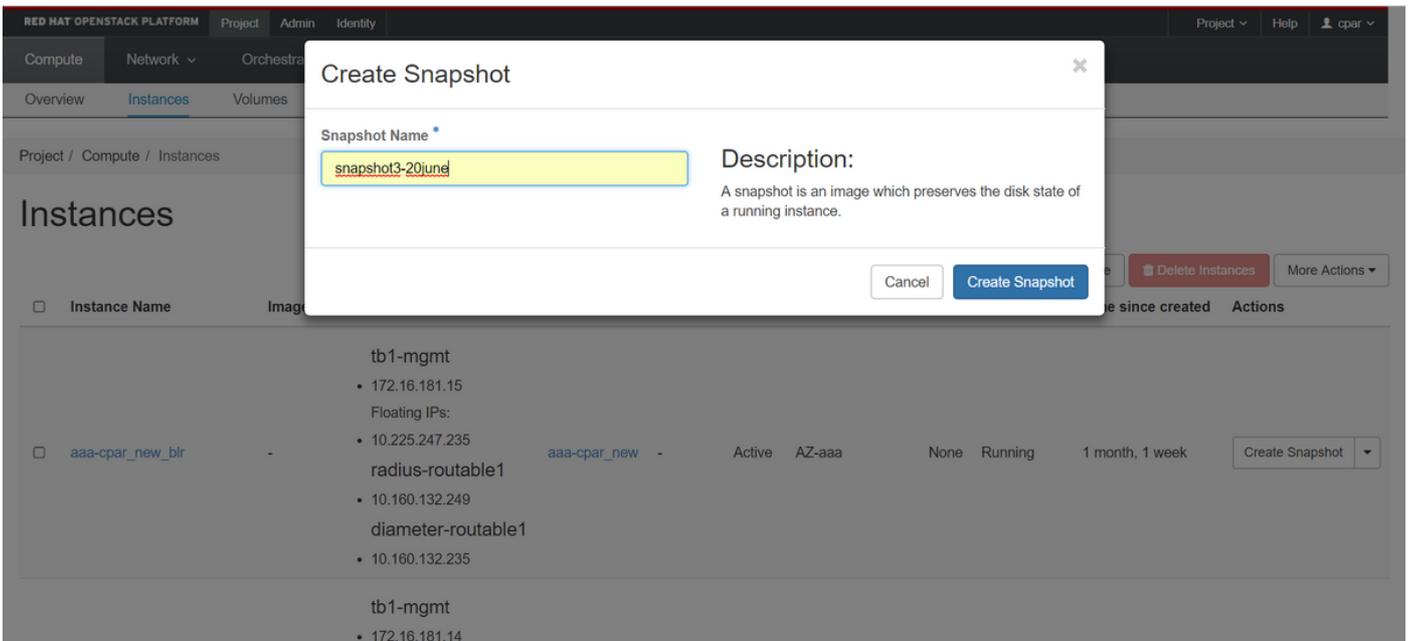
Die vier QCOW2-Dateien werden parallel erstellt.

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)

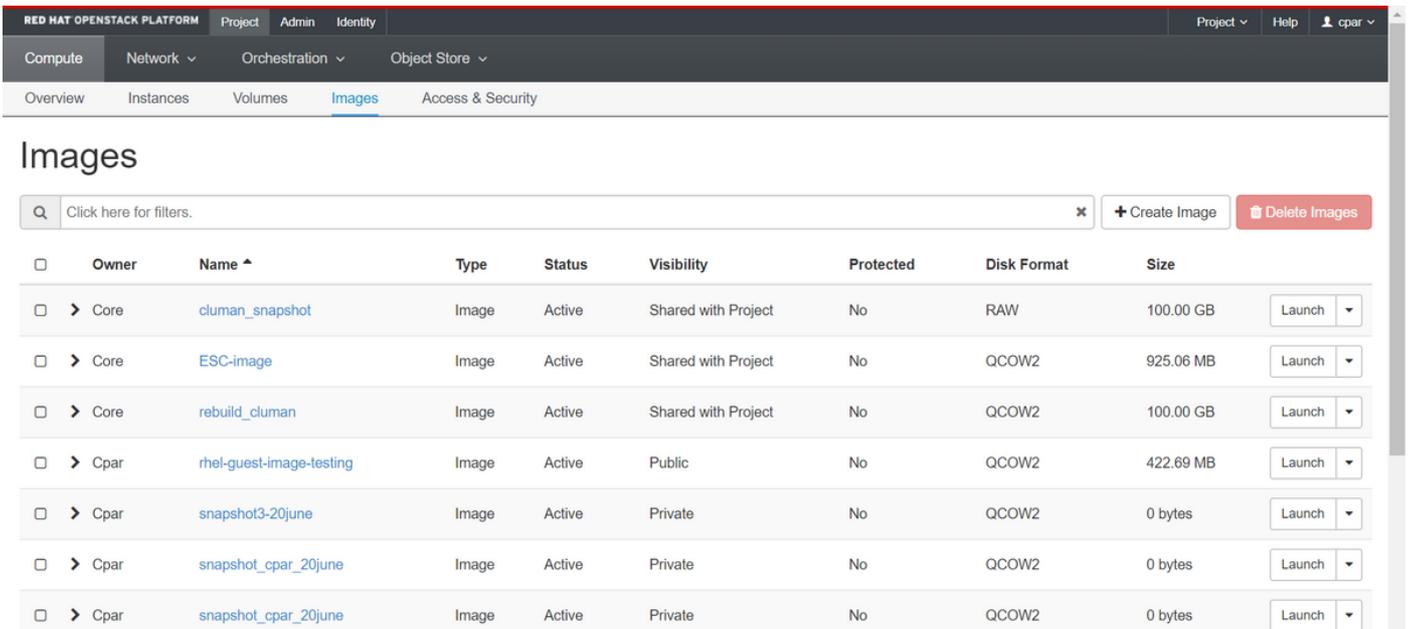
1. Melden Sie sich bei der Horizon GUI von POD an.
2. Navigieren Sie nach der Anmeldung im oberen Menü zu **PROJECT > COMPUTE > INSTANZEN**, und suchen Sie die AAA-Instanzen, wie in diesem Bild gezeigt.

The screenshot shows the OpenStack Horizon interface for the 'Instances' page. The breadcrumb navigation is 'Project / Compute / Instances'. The main heading is 'Instances'. Below the heading, there are several buttons: 'Instance Name =', 'Filter', 'Launch Instance', 'Delete Instances', and 'More Actions'. A table lists instances with the following columns: Instance Name, Image Name, IP Address, Size, Key Pair, Status, Availability Zone, Task, Power State, Time since created, and Actions. One instance, 'aaa-cpar_new_blr', is selected. Its details are shown below the table: Image Name is '-', IP Address is '10.225.247.235', Size is 'aaa-cpar_new', Key Pair is '-', Status is 'Active', Availability Zone is 'AZ-aaa', Task is 'None', Power State is 'Running', and Time since created is '1 month, 1 week'. The 'Actions' column for this instance has a 'Create Snapshot' button. The footer of the page shows the URL '10.225.247.214/dashboard/project/images/.../create/'.

3. Klicken Sie auf **Snapshot erstellen**, um mit der Snapshot-Erstellung fortzufahren (diese muss für die entsprechende AAA-Instanz ausgeführt werden), wie in diesem Bild gezeigt.



4. Sobald der Snapshot ausgeführt wurde, navigieren Sie zum Menü **Bilder**, und überprüfen Sie, ob alle fertig gestellt sind und keine Probleme melden, wie in diesem Bild dargestellt.



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, müssen Sie den Snapshot mithilfe des Befehls **Glance image-list** auf OSPD-Ebene identifizieren.

```
[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 |
```

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

6. Sobald Sie den herunterzuladenden Snapshot identifiziert haben (der in grün gekennzeichnet ist), können Sie ihn im QCOW2-Format mit dem Befehl **glance image-download** wie hier dargestellt 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 kann einige Zeit dauern, diese Aktion abzuschließen, sobald sie abgeschlossen ist, kann sich das Bild im Verzeichnis **/tmp** befinden.
- Beim Senden des Prozesses an den Hintergrund wird der Prozess auch beendet, wenn die Verbindung verloren geht.
- Führen Sie den Befehl **disown -h aus**, sodass der Prozess bei Verlust der SSH-Verbindung weiterhin auf dem OSPD ausgeführt wird und abgeschlossen wird.

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

Eine Empfehlung besteht darin, das Dokument vorübergehend mithilfe von SFTP sftproot@x.x.x.x in das OSPD-Verzeichnis eines anderen Standorts zu übertragen, wobei x.x.x.x die IP-Adresse eines Remote-OSPD ist. Um die Übertragung zu beschleunigen, kann das Ziel an mehrere OSPDs gesendet werden. 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-Adresse eines Remote-OSPD ist) ausführen, 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. Sie können den Instanznamen mit dem Status-Shutoff sehen.

```
[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 |
+-----+-----+-----+-----+
-----+
-----+

```

Ersetzen einer fehlerhaften Komponente aus dem Computing-Knoten

Schalten Sie den angegebenen Server aus. Die Schritte zum Ersetzen einer fehlerhaften Komponente auf dem UCS C240 M4 Server können wie folgt beschrieben werden:

[Ersetzen der Serverkomponenten](#)

VMs wiederherstellen

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 früherer VM-Snapshot verfügbar ist, stellen Sie eine Verbindung zum OSPD-Knoten her, an den die Sicherung gesendet wurde, und senden Sie die Sicherung über SFTP zurück an den ursprünglichen OSPD-Knoten. Mit sftpboot@x.x.x.x, wobei x.x.x.x die IP-Adresse eines ursprünglichen OSPD ist. Speichern Sie die Snapshot-Datei im `/tmp`-Verzeichnis.

Schritt 2: Stellen Sie eine Verbindung zum OSPD-Knoten her, wo die Instanz wie im Bild gezeigt erneut bereitgestellt werden kann.

```
Last login: wed May 9 06:42:27 2018 from 10.169.119.213
[root@daucs01-ospd ~]#
```

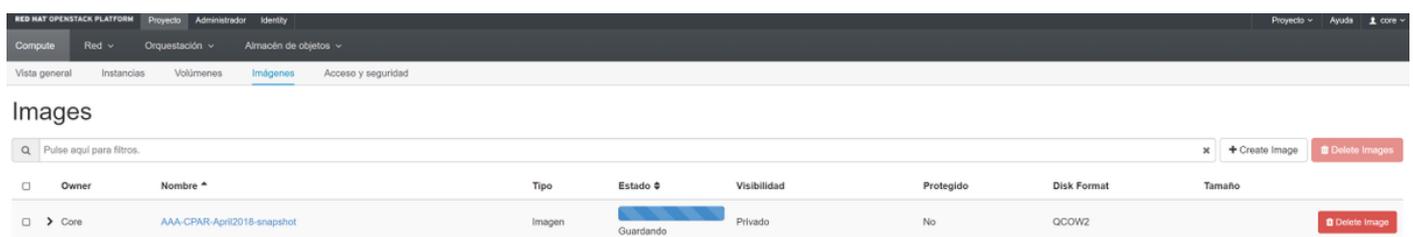
Rufen Sie die Umgebungsvariablen mit dem folgenden Befehl auf:

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

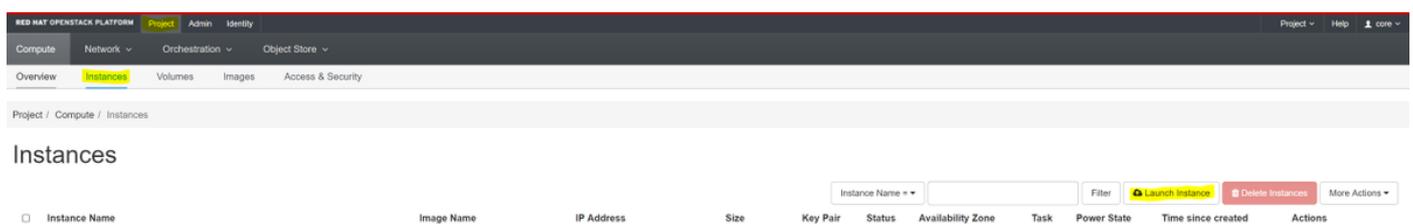
Schritt 3: Um den Schnappschuss als Bild zu verwenden, muss er in den Horizont als solches hochgeladen werden. Führen Sie dazu den nächsten Befehl aus.

```
#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 in diesem Bild gezeigt werden.



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



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

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *

Availability Zone

Count *

Total Instances (100 Max)

27%

- 26 Current Usage
- 1 Added
- 73 Remaining

Details

Source *

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

✕ Cancel

< Back

Next >

Launch Instance

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

Instance source is the template used to create an instance. You can use a snapshot of an existing instance, an image, or a volume (if enabled). You can also choose to use persistent storage by creating a new volume.

Source

Select Boot Source: Create New Volume:

Allocated

Name	Updated	Size	Type	Visibility	
> AAA-CPAR-April2018-snapshot	5/10/18 9:56 AM	5.43 GB	qcow2	Private	-

▼ Available 8 Select one

✕

Name	Updated	Size	Type	Visibility	
> redhat72-image	4/10/18 1:00 PM	469.87 MB	qcow2	Private	+
> tmobile-pcrf-13.1.1.qcow2	9/9/17 1:01 PM	2.46 GB	qcow2	Public	+
> tmobile-pcrf-13.1.1.iso	9/9/17 8:13 AM	2.76 GB	iso	Private	+
> AAA-Temporary	9/5/17 2:11 AM	180.00 GB	qcow2	Private	+
> CPAR_AAATEMPLATE_AUGUST222017	8/22/17 3:33 PM	16.37 GB	qcow2	Private	+
> tmobile-pcrf-13.1.0.iso	7/11/17 7:51 AM	2.82 GB	iso	Public	+
> tmobile-pcrf-13.1.0.qcow2	7/11/17 7:48 AM	2.46 GB	qcow2	Public	+
> ESC-image	6/27/17 12:45 PM	925.06 MB	qcow2	Private	+

✕ Cancel

Schritt 7: Wählen Sie auf der Registerkarte **Flavor** die AAA-Variante aus, indem Sie auf das +-Zeichen klicken, wie in diesem Bild gezeigt.

Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> AAA-CPAR	36	32 GB	180 GB	180 GB	0 GB	No	-

Networks *
Select one

Network Ports
Click here for filters.

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> pcrf-oam	10	24 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-pd	12	16 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-qns	10	16 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-arb	4	16 GB	100 GB	100 GB	0 GB	Yes	+
> esc-flavor	4	4 GB	0 GB	0 GB	0 GB	Yes	+
> pcrf-sm	10	104 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-cm	6	16 GB	100 GB	100 GB	0 GB	Yes	+

✕ Cancel < Back Next > Launch Instance

Schritt 8: Navigieren Sie schließlich zur Registerkarte **Netzwerk**, 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 in diesem Bild gezeigt.

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud. ?

▼ Allocated 3 Select networks from those listed below.

	Network	Subnets Associated	Shared	Admin State	Status	
1	radius-routable1	radius-routable-subnet	Yes	Up	Active	-
2	diameter-routable1	sub-diameter-routable1	Yes	Up	Active	-
3	tb1-mgmt	tb1-subnet-mgmt	Yes	Up	Active	-

▼ Available 16 Select at least one network

	Network	Subnets Associated	Shared	Admin State	Status	
	Internal	Internal	Yes	Up	Active	+
	pcrf_dap2_ldap	pcrf_dap2_ldap	Yes	Up	Active	+
	pcrf_dap2_usd	pcrf_dap2_usd	Yes	Up	Active	+
	tb1-orch	tb1-subnet-orch	Yes	Up	Active	+
	pcrf_dap1_usd	pcrf_dap1_usd	Yes	Up	Active	+
	pcrf_dap1_sy	pcrf_dap1_sy	Yes	Up	Active	+
	pcrf_dap1_gx	pcrf_dap1_gx	Yes	Up	Active	+
	pcrf_dap1_nap	pcrf_dap1_nap	Yes	Up	Active	+
	pcrf_dap2_sy	pcrf_dap2_sy	Yes	Up	Active	+
	pcrf_dap2_rx	pcrf_dap2_rx	Yes	Up	Active	+

✕ Cancel
< Back
Next >
Launch Instance

Klicken Sie abschließend auf **Instanz starten**, um diese zu erstellen. Der Fortschritt kann in Horizont überwacht werden:

RED HAT OPENSTACK PLATFORM Proyecto Administrador Identity Proyecto - Ayuda 1 con

Sistema

Vista general Hipervisores Agregados de host **Instancias** Volúmenes Sabores Imágenes Redes Routers IPs flotantes Predeterminados Definiciones de los metadatos Información del Sistema

Administrador / Sistema / Instancias

Instancias

Proyecto= Filtrar Eliminar instancias

<input type="checkbox"/>	Proyecto	Host	Nombre	Nombre de la imagen	Dirección IP	Tamaño	Estado	Tarea	Estado de energía	Tiempo desde su creación	Acciones
<input type="checkbox"/>	Core	pod1-stack-compute-5.localdomain	dalaaa10	AAA-CPAR-April2019-snapshot	tb1-mgmt • 172.16.181.11 radius-routable1 • 10.178.6.56 diameter-routable1 • 10.178.6.40	AAA-CPAR	Construir	Generando	Sin estado	1 minuto	Editar instancia

Nach einigen Minuten ist die Instanz vollständig bereitgestellt und einsatzbereit, wie in diesem Bild gezeigt.

Core	pod1-stack-compute-5.localdomain	dalaaa10	AAA-CPAR-April2018-snapshot	tb1-mgmt	AAA-CPAR	Activo	Ninguno	Ejecutando	8 minutos	Editar instancia
				<ul style="list-style-type: none"> 172.16.181.16 IPs flotantes: 10.145.0.62 radius-routable1 10.178.6.56 diameter-routable1 10.178.6.40 						

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 **IP dem 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:

Allocate Floating IP ✕

Pool *

10.145.0.192/26 Management ▼

Project *

Core ▼

Floating IP Address (optional) ⓘ

10.145.0.249

Description:

From here you can allocate a floating IP to a specific project.

Cancel
Allocate Floating IP

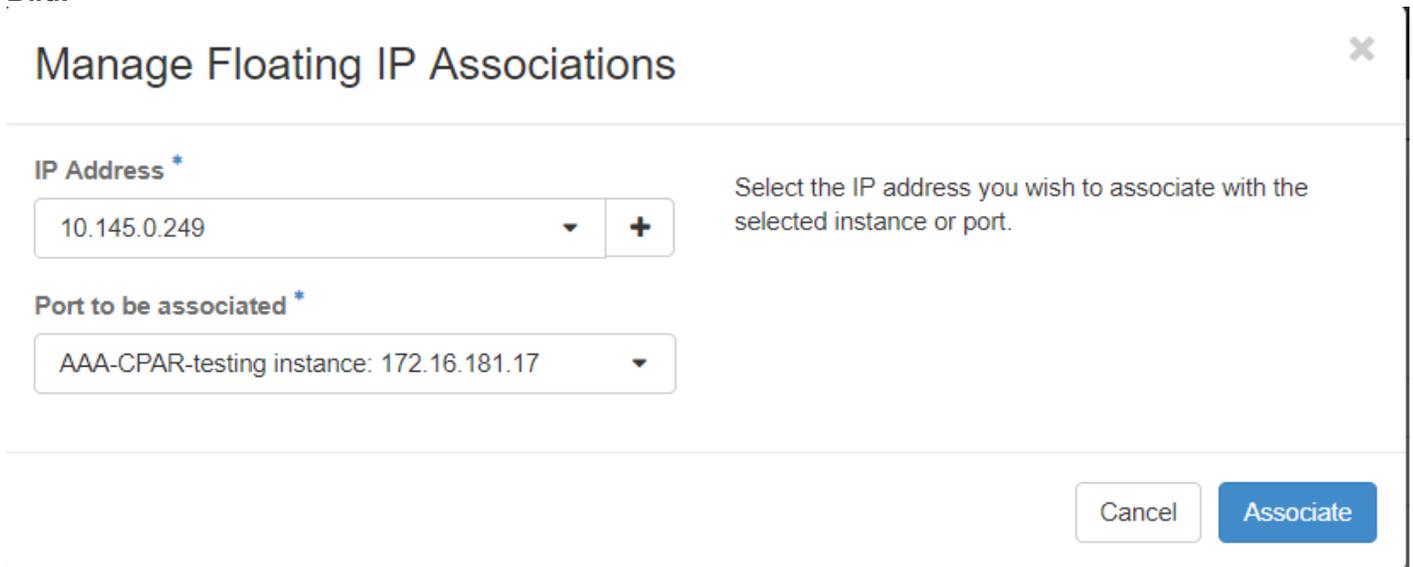
Schritt 4: Klicken Sie auf die Schaltfläche **Floating-IP zuweisen**.

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, wird ein Menü angezeigt. Wählen Sie die Option **Zuordnen zu (Floating-IP)** aus.

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

Bild.



Manage Floating IP Associations

IP Address *

10.145.0.249 +

Port to be associated *

AAA-CPAR-testing instance: 172.16.181.17

Cancel Associate

Select the IP address you wish to associate with the selected instance or port.

Schritt 8: Klicken Sie abschließend 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 die Registerkarte Konsole. Dadurch 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: root Kennwort: cisco123

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-514.el7.x86_64 on an x86_64

aaa-cpar-testing-instance login: root
Password:
Last login: Thu Jun 29 12:59:59 from 5.232.63.159
[root@aaa-cpar-testing-instance ~]#
```

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. Suchen Sie dann nach dem Abschnitt, und ändern Sie die erste Zeile von PasswordAuthentication no in PasswordAuthentication yes (Kennwort-Authentifizierung), wie in diesem Bild gezeigt.

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes_
#PermitEmptyPasswords no
PasswordAuthentication no
```

Schritt 7: Drücken Sie ESC und führen Sie :wq! aus, um die Dateiänderungen sshd_config zu speichern. Schritt 8: Führen Sie den Befehl service sshd restart aus, wie im Bild gezeigt.

```
[root@aaa-cpar-testing-instance ssh]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@aaa-cpar-testing-instance ssh]#
```

Schritt 9: Um die SSH-Konfigurationsänderungen ordnungsgemäß zu testen, öffnen Sie jeden SSH-Client, und versuchen Sie, eine sichere Remote-Verbindung mit der unverankerten IP der Instanz (d. h. 10.145.0.249) und dem Root des Benutzers herzustellen, wie im Bild gezeigt.

```
[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 ~]#
```

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.

```
[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 Instanzstart
Befolgen Sie diese Schritte, sobald die Aktivität abgeschlossen ist 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 > Instanz starten.
Schritt 2: Überprüfen Sie, ob der Status der Instanz aktiv ist und der Betriebszustand ausgeführt wird, wie in diesem Bild gezeigt.

Instances

Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
		diameter-routable1								
		• 10.160.132.231								
		radius-routable1								
<input type="checkbox"/>	dlaaa04	dlaaa01-sept092017	AAA-CPAR	-	Active	AZ-dlaaa04	None	Running	3 months	Create Snapshot
		• 10.160.132.247								
		tb1-mgmt								
		• 172.16.181.16								
		Floating IPs:								
		• 10.250.122.114								

9. Statusprüfung nach Aktivität
Schritt 1: Führen Sie den Befehl /opt/CSCOAr/bin/arstatus auf Betriebssystemebene aus:

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

Schritt 2: Führen Sie den Befehl /opt/CSCOAr/bin/aregcmd auf Betriebssystemebene aus, und

geben Sie die Administratorberechtigungen ein. Stellen Sie sicher, dass CPAR Health 10 von 10 und die CPAR-CLI verlassen.

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

PAR-ADD-TPS 7.2(2000TPS:)

PAR-RDDR-TRX 7.2()

PAR-HSS 7.2()

Radius/

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

Schritt 3: Führen Sie den Befehl netstat aus | grep-Durchmesser und überprüfen, ob alle DRA-Verbindungen hergestellt sind. Die 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@aaa02 logs]# netstat | grep diameter
tcp        0      0 0 aaa02.aaa.epc.:77 mp1.dra01.d:diameter ESTABLISHED
tcp        0      0 0 aaa02.aaa.epc.:36 tsa6.dra01:diameter ESTABLISHED
tcp        0      0 0 aaa02.aaa.epc.:47 mp2.dra01.d:diameter ESTABLISHED
tcp        0      0 0 aaa02.aaa.epc.:07 tsa5.dra01:diameter ESTABLISHED
tcp        0      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 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 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 dem folgenden Befehl verwendet:

```
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. **Komponenten-RMA - OSD-Computing-**

KnotenIdentifizieren von VMs, die im OSD-Computing-Knoten gehostet

werdenIdentifizieren Sie die VMs, die auf dem OSD-Compute-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 |
```

Hinweis: In der hier gezeigten Ausgabe entspricht die erste Spalte der UUID, die zweite Spalte dem VM-Namen und die dritte Spalte dem Hostnamen, in dem die VM vorhanden ist. Die Parameter aus dieser Ausgabe werden in den nachfolgenden Abschnitten verwendet. Sicherung: SNAPSHOT-PROZESS 1. Herunterfahren der CPAR-Anwendung Schritt 1: Öffnen Sie einen mit dem TMO-Produktionsnetzwerk verbundenen SSH-Client, und stellen Sie eine Verbindung zur CPAR-Instanz her. Es ist wichtig, nicht alle vier AAA-Instanzen an einem Standort gleichzeitig herunterzufahren, sondern dies auf eine Weise zu tun. Schritt 2: Führen Sie zum Herunterfahren der CPAR-Anwendung den folgenden Befehl aus:

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

Die Meldung "Cisco Prime Access Registrar Server Agent heruntergefahren" wird angezeigt. muss erscheinen. Hinweis: Wenn ein Benutzer eine CLI-Sitzung geöffnet hat, funktioniert der Befehl arserver stop nicht, und die folgende Meldung wird angezeigt:

```
ERROR: You cannot 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, beenden Sie den Prozess mit dem folgenden Befehl:

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

Wiederholen Sie anschließend Schritt 1. Schritt 3: Stellen Sie sicher, dass die CPAR-Anwendung tatsächlich durch Ausführen des Befehls 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
```

2. VM-Snapshot-Aufgabe Schritt 1: Geben Sie die Horizon GUI-Website ein, die der aktuell bearbeiteten Website (Stadt) entspricht. Wenn Sie auf Horizon zugreifen, kann dieser Bildschirm angezeigt werden.

RED HAT® OPENSTACK PLATFORM

If you are not sure which authentication method to use, contact your administrator.

User Name *

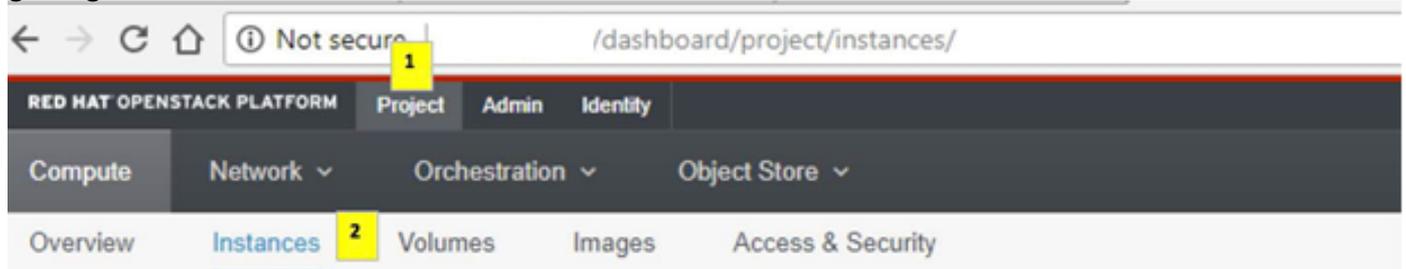
cpar

Password *

.....

Connect

Schritt 2: Navigieren Sie zu Projekt > Instanzen wie in diesem Bild gezeigt.



Wenn der Benutzer CPAR verwendet hat, können in diesem Menü nur die 4 AAA-Instanzen angezeigt werden. 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 abbrechen > Instanz abschalten), wie im Bild gezeigt,

und bestätigen Sie Ihre Auswahl. **Shut Off Instance** Schritt 4: Überprüfen Sie, ob die Instanz tatsächlich heruntergefahren wurde, indem Sie Status = Shutoff und Power State = Shut Down (Herunterfahren) wie im Bild gezeigt überprüfen.

Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
AAA-CPAR	-	Shutoff	AZ-dalaaa09	None	Shut Down	3 months, 2 weeks	Start Instance

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 - 1 Stunde) (25 Minuten für Instanzen, die ein qcow-Image als Quelle und 1 Stunde für Instanzen, die ein Rohbild als Quelle verwenden)

1. Anmeldung bei der Horizon GUI von POD OpenStack
2. Navigieren Sie nach der Anmeldung zum Abschnitt Projekt > Computing > Instanzen im oberen Menü, und suchen Sie die AAA-Instanzen, wie in diesem Bild gezeigt.

RED HAT OPENSTACK PLATFORM Project Admin Identity Project Help cpar

Compute Network Orchestration Object Store

Overview Instances Volumes Images Access & Security

Project / Compute / Instances

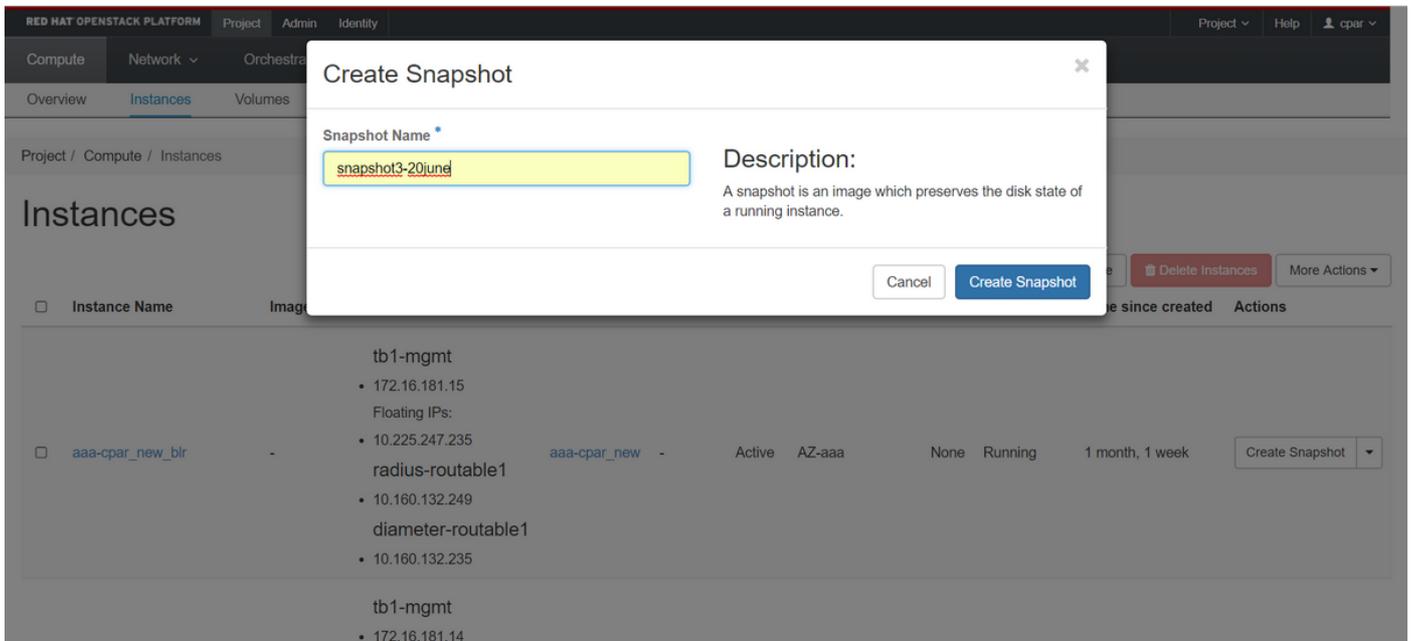
Instances

Instance Name = Filter Launch Instance Delete Instances More Actions

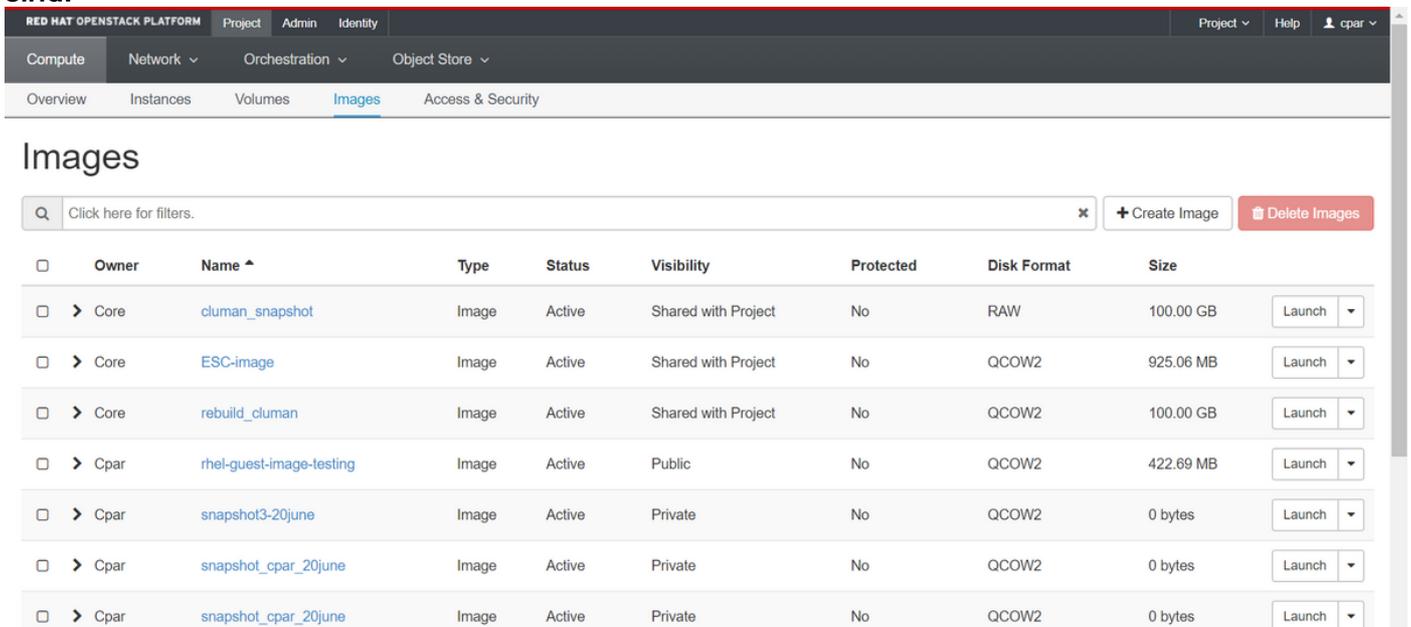
Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input type="checkbox"/> aaa-cpar_new_blr	-	tb1-mgmt • 172.16.181.15 Floating IPs: • 10.225.247.235 radius-routable1 • 10.160.132.249 diameter-routable1 • 10.160.132.235	aaa-cpar_new	-	Active	AZ-aaa	None	Running	1 month, 1 week	Create Snapshot

10.225.247.214/dashboard/project/images/.../create/

3. Klicken Sie auf Snapshot erstellen, um mit der Snapshot-Erstellung fortzufahren (diese muss für die entsprechende AAA-Instanz ausgeführt werden), wie im Bild gezeigt.



4. Sobald der Snapshot ausgeführt wurde, navigieren Sie zum Menü Bilder, und überprüfen Sie, ob alle fertig gestellt sind und keine Probleme melden, wie in diesem Bild zu sehen sind.



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, müssen Sie den Snapshot mithilfe des Befehls Glance image-list auf OSPD-Ebene identifizieren.

```
[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 |
```

+-----+
6. Sobald Sie den herunterzuladenden Snapshot (der in grün gekennzeichnet ist) identifizieren, können Sie ihn im QCOW2-Format mit dem Befehl `glance image-download` wie hier dargestellt 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 kann einige Zeit dauern, diese Aktion abzuschließen, sobald sie abgeschlossen ist, kann sich das Bild im Verzeichnis `/tmp` befinden.
- Beim Senden des Prozesses an den Hintergrund wird der Prozess auch beendet, wenn die Verbindung verloren geht.
- Führen Sie den Befehl `disown -h` aus, sodass der Prozess bei Verlust der SSH-Verbindung weiterhin auf dem OSPD ausgeführt wird und abgeschlossen wird.

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 kann einige Zeit in Anspruch nehmen (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 Dateintegrität 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 Sie die Dateiübertragung starten, müssen Sie überprüfen, ob das Ziel über genügend freien Speicherplatz verfügt. Führen Sie den Befehl `df -khin` aus, um den Speicherplatz zu überprüfen. Eine Empfehlung besteht darin, das Dokument vorübergehend mithilfe von SFTP sftproot@x.x.x.x an das OSPD-Projekt eines anderen Standorts zu übertragen, wobei `x.x.x.x` die IP-Adresse eines Remote-OSPD ist. Um die Übertragung zu beschleunigen, kann das Ziel an mehrere OSPDs gesendet werden. 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-Adresse eines Remote-OSPD ist) ausführen, um die Datei in ein anderes OSPD-Projekt zu übertragen.

CEPH im Servicemodus aktivieren

Hinweis: Wenn die fehlerhafte Komponente auf dem Knoten OSD-Compute ausgetauscht werden soll, legen Sie die Ceph in Maintenance (Wartung) auf dem Server ein, bevor Sie mit dem

Austausch der Komponente fortfahren.

- Überprüfen Sie, ob der Status ceph 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
```

- Melden Sie sich beim OSD Compute-Knoten 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 Zustand "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 können den Instanznamen mit dem Status-Shutoff sehen.

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

```
Request to stop server aaa2-21 has been accepted.
```

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

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

ID	Name	Status	Task State
46b4b9eb-ala6-425d-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		

Ersetzen einer fehlerhaften Komponente aus dem OSD-Computing-Knoten
 Schalten Sie den angegebenen Server aus. Die Schritte zum Ersetzen einer fehlerhaften Komponente auf dem UCS C240 M4 Server können wie folgt beschrieben werden: [Ersetzen der Serverkomponenten](#)
 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
```

VMs wiederherstellen
 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 VMSnapshot verfügbar ist, stellen Sie eine Verbindung zum OSPD-Knoten her, an den die Sicherung gesendet wurde, und setzen Sie die Sicherung wieder auf den ursprünglichen OSPD-Knoten zurück. Verwenden Sie [sftproot@x.x.x.x](#), wobei x.x.x.x die IP-Adresse eines 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 erneut bereitgestellt wird.

```
Last login: wed May 9 06:42:27 2018 from 10.169.119.213
[root@daucs01-ospd ~]#
```

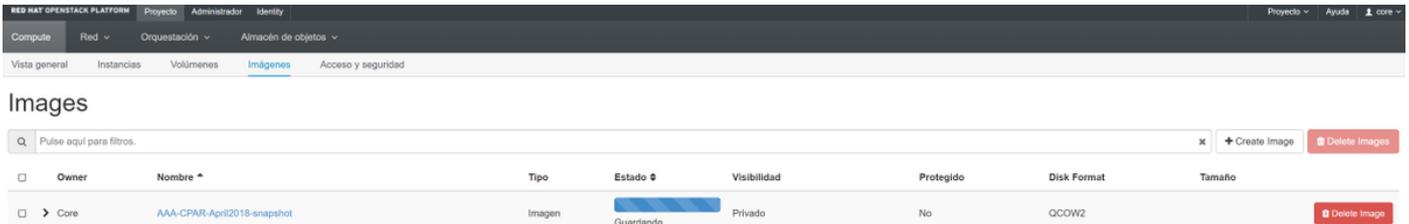
Rufen Sie die Umgebungsvariablen mit dem folgenden Befehl auf:

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

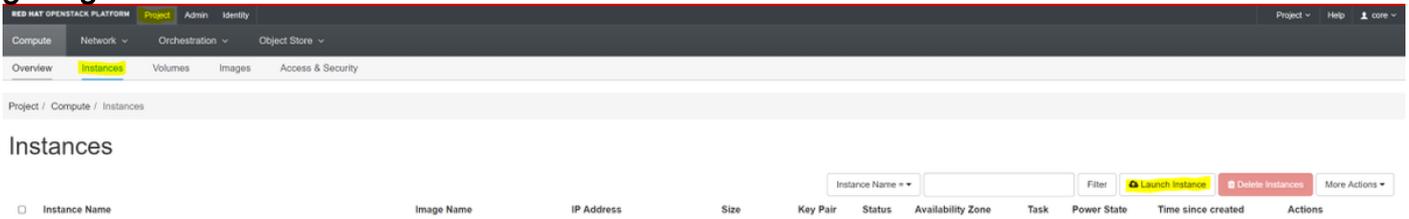
Schritt 3: Um den Snapshot als Bild zu verwenden, muss er in Horizon als solches hochgeladen werden. Führen Sie dazu den nächsten Befehl aus.

```
#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 Launch Instance (Ladestation), wie in diesem Bild gezeigt.



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

Launch Instance

Details

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *
dalaaa10

Availability Zone
AZ-dalaaa10

Count *
1

Total Instances (100 Max)
27%
26 Current Usage
1 Added
73 Remaining

Schritt 6: Wählen Sie auf der Registerkarte Quelle das Bild aus, um die Instanz zu erstellen. Wählen Sie im Menü Startquelle auswählen die Option Bild, eine Liste der Bilder wird angezeigt.

Wählen Sie die Datei aus, die zuvor hochgeladen wurde, indem Sie auf das + Zeichen klicken.

Launch Instance



Instance source is the template used to create an instance. You can use a snapshot of an existing instance, an image, or a volume (if enabled). You can also choose to use persistent storage by creating a new volume.

Source

Select Boot Source: Create New Volume:

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Allocated

Name	Updated	Size	Type	Visibility	
> AAA-CPAR-April2018-snapshot	5/10/18 9:56 AM	5.43 GB	qcow2	Private	-

Available 8 Select one

Click here for filters.

Name	Updated	Size	Type	Visibility	
> redhat72-image	4/10/18 1:00 PM	469.87 MB	qcow2	Private	+
> tmobile-pcrf-13.1.1.qcow2	9/9/17 1:01 PM	2.46 GB	qcow2	Public	+
> tmobile-pcrf-13.1.1.iso	9/9/17 8:13 AM	2.76 GB	iso	Private	+
> AAA-Temporary	9/5/17 2:11 AM	180.00 GB	qcow2	Private	+
> CPAR_AAATEMPLATE_AUGUST222017	8/22/17 3:33 PM	16.37 GB	qcow2	Private	+
> tmobile-pcrf-13.1.0.iso	7/11/17 7:51 AM	2.82 GB	iso	Public	+
> tmobile-pcrf-13.1.0.qcow2	7/11/17 7:48 AM	2.46 GB	qcow2	Public	+
> ESC-image	6/27/17 12:45 PM	925.06 MB	qcow2	Private	+

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

Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> AAA-CPAR	36	32 GB	180 GB	180 GB	0 GB	No	-

Networks *
Network Ports
Security Groups
Key Pair
Configuration
Server Groups
Scheduler Hints
Metadata

Available 7 Select one

Q Click here for filters. ✕

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> pcrf-oam	10	24 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-pd	12	16 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-qns	10	16 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-arb	4	16 GB	100 GB	100 GB	0 GB	Yes	+
> esc-flavor	4	4 GB	0 GB	0 GB	0 GB	Yes	+
> pcrf-sm	10	104 GB	100 GB	100 GB	0 GB	Yes	+
> pcrf-cm	6	16 GB	100 GB	100 GB	0 GB	Yes	+

✕ Cancel < Back Next > Launch Instance

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 in diesem Bild gezeigt.

Networks provide the communication channels for instances in the cloud.

▼ Allocated **3** Select networks from those listed below.

	Network	Subnets Associated	Shared	Admin State	Status	
1	radius-routable1	radius-routable-subnet	Yes	Up	Active	-
2	diameter-routable1	sub-diameter-routable1	Yes	Up	Active	-
3	tb1-mgmt	tb1-subnet-mgmt	Yes	Up	Active	-

▼ Available **16** Select at least one network

Click here for filters.

	Network	Subnets Associated	Shared	Admin State	Status	
	Internal	Internal	Yes	Up	Active	+
	pcrf_dap2_ldap	pcrf_dap2_ldap	Yes	Up	Active	+
	pcrf_dap2_usd	pcrf_dap2_usd	Yes	Up	Active	+
	tb1-orch	tb1-subnet-orch	Yes	Up	Active	+
	pcrf_dap1_usd	pcrf_dap1_usd	Yes	Up	Active	+
	pcrf_dap1_sy	pcrf_dap1_sy	Yes	Up	Active	+
	pcrf_dap1_gx	pcrf_dap1_gx	Yes	Up	Active	+
	pcrf_dap1_nap	pcrf_dap1_nap	Yes	Up	Active	+
	pcrf_dap2_sy	pcrf_dap2_sy	Yes	Up	Active	+
	pcrf_dap2_rx	pcrf_dap2_rx	Yes	Up	Active	+

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

RED HAT OPENSTACK PLATFORM Proyecto Administrador Identity

Sistema

Vista general Hipervisores Agregados de host **Instancias** Volúmenes Sabores Imágenes Redes Routers IPs flotantes Predeterminados Definiciones de los metadatos Información del Sistema

Administrador / Sistema / Instancias

Instancias

Proyección Filtrar

Proyecto	Host	Nombre	Nombre de la imagen	Dirección IP	Tamaño	Estado	Tarea	Estado de energía	Tiempo desde su creación	Acciones
Core	pod1-stack-compute-5.localdomain	dalaaa10	AAA-CPAR-April2018-snapshot	tb1-mgmt • 172.16.181.11 radius-routable1 • 10.178.6.56 diameter-routable1 • 10.178.6.40	AAA-CPAR	Construir	Generando	Sin estado	1 minuto	<input type="button" value="Editar instancia"/>
Core	pod1-stack-compute-5.localdomain	dalaaa10	AAA-CPAR-April2018-snapshot	tb1-mgmt • 172.16.181.16 IPs flotantes: • 10.145.0.62 radius-routable1 • 10.178.6.56 diameter-routable1 • 10.178.6.40	AAA-CPAR	Activo	Ninguno	Ejecutando	8 minutos	<input type="button" value="Editar instancia"/>

Nach einigen Minuten wird die Instanz vollständig bereitgestellt und einsatzbereit.

Erstellen und Zuweisen einer unverankerten 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 IP dem 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 wird, und die neue Floating-IP-Adresse selbst.
Beispiel:

Allocate Floating IP

Pool *
10.145.0.192/26 Management

Project *
Core

Floating IP Address (optional) ⓘ
10.145.0.249

Description:
From here you can allocate a floating IP to a specific project.

Cancel Allocate Floating IP

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

Manage Floating IP Associations

IP Address *
10.145.0.249 +

Port to be associated *
AAA-CPAR-testing instance: 172.16.181.17

Select the IP address you wish to associate with the selected instance or port.

Cancel Associate

Schritt 8: Klicken Sie abschließend 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 die Registerkarte Konsole. Dadurch wird die Befehlszeilenschnittstelle des virtuellen Systems angezeigt. Schritt 4: Geben Sie nach der Anzeige der CLI die entsprechenden Anmeldeinformationen ein, wie im Bild gezeigt: Benutzername: root Kennwort: cisco123

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-514.el7.x86_64 on an x86_64

aaa-cpar-testing-instance login: root
Password:
Last login: Thu Jun 29 12:59:59 from 5.232.63.159
[root@aaa-cpar-testing-instance ~]#
```

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. Suchen Sie dann nach diesem Abschnitt, und ändern Sie die erste Zeile von `PasswordAuthentication no` in `PasswordAuthentication yes`.

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes_
#PermitEmptyPasswords no
PasswordAuthentication no
```

Schritt 7: Drücken Sie ESC und geben Sie `:wq!t` ein, um die Dateiänderungen `sshd_config` zu speichern. Schritt 8: Führen Sie den Befehl `service sshd restart` aus.

```
[root@aaa-cpar-testing-instance ssh]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@aaa-cpar-testing-instance ssh]#
```

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

```
[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 ~]#
```

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

```
[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 InstanzstartBefolgen Sie diese Schritte, sobald die Aktivität abgeschlossen ist 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 > Instanz starten.Schritt 2: Stellen Sie sicher, dass der Status der Instanz aktiv ist und der Betriebsstatus wie im Bild gezeigt Running (Betrieb) ist.

Instances

Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
dlaaa04	dlaaa01-sept092017	<ul style="list-style-type: none"> 10.160.132.231 10.160.132.247 172.16.181.16 10.250.122.114 	AAA-CPAR	-	Active	AZ-dlaaaa04	None	Running	3 months	Create Snapshot

9. Statusprüfung nach AktivitätSchritt 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-Option für das Beenden ist.

```
[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@aaa02 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 stellen TPS dar. Sie müssen genau auf diese Werte achten. Der TPS-Wert darf 1500 nicht überschreiten.

```
[root@wscaaa04 ~]# tail -f /opt/CSC0ar/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 verwendet, indem Sie den folgenden Befehl ausführen:

```
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. **Komponenten-RMA - Controller-Knoten** Vorabprüfung

- Vom OSPD melden Sie sich beim Controller an und prüfen, ob die PCs in gutem Zustand sind
- alle drei Controller Online und Galera zeigen alle drei Controller als Master an.

Hinweis: Ein gesunder Cluster erfordert zwei aktive Controller, also überprüfen Sie, ob die beiden weiterhin aktiven Controller online und aktiv sind.

```
[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.e17_3.4-e174ec8) - partition with quorum
Last updated: Fri Jul 6 09:03:37 2018 Last 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
```

Controller-Cluster in Servicemodus verschieben

- Führen Sie das PC-Cluster auf dem Controller aus, der im Standby-Modus aktualisiert wird:

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

- Überprüfen Sie den PC-Status erneut, und stellen Sie sicher, dass der PC-Cluster auf diesem Knoten gestoppt wird:

```
[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.e17_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
```

Außerdem muss der Knoten auf den beiden anderen Controllern als Standby-Knoten angezeigt werden. Ersetzen einer fehlerhaften Komponente aus dem Controller-Knoten
Schalten Sie den angegebenen Server aus. Die Schritte zum Ersetzen einer fehlerhaften Komponente auf dem UCS C240 M4 Server können wie folgt beschrieben werden: [Ersetzen der Serverkomponenten](#)
Power-On-Server

- Schalten Sie den Server ein, und überprüfen Sie, ob der Server hochgefahren ist:

```
[stack@director ~]$ source stackrc
[stack@director ~]$ nova list
+-----+-----+-----+-----+-----+-----+
| ID | Name | Status | Task State | Power State | Networks |
+-----+-----+-----+-----+-----+-----+
| 03f15071-21aa-4bcf-8fdd-acdbde305168 | pod2-stack-compute-0 | ACTIVE | - | Running |
ctlplane=192.200.0.106 |
| 1f725ce3-948d-49e9-aed9-b99e73d82644 | pod2-stack-compute-1 | ACTIVE | - | Running |
ctlplane=192.200.0.107 |
| fbc13c78-dc06-4ac9-a3c5-595ccc147adc | pod2-stack-compute-2 | ACTIVE | - | Running |
ctlplane=192.200.0.119 |
| 3b94e0b1-47dc-4960-b3eb-d02ffe9ae693 | pod2-stack-compute-3 | ACTIVE | - | Running |
ctlplane=192.200.0.112 |
| 5dbac94d-19b9-493e-a366-1e2e2e5e34c5 | pod2-stack-compute-4 | ACTIVE | - | Running |
ctlplane=192.200.0.116 |
| b896c73f-d2c8-439c-bc02-7b0a2526dd70 | pod2-stack-controller-0 | ACTIVE | - | Running |
ctlplane=192.200.0.113 |
| 2519ce67-d836-4e5f-a672-1a915df75c7c | pod2-stack-controller-1 | ACTIVE | - | Running |
ctlplane=192.200.0.105 |
| e19b9625-5635-4a52-a369-44310f3e6a21 | pod2-stack-controller-2 | ACTIVE | - | Running |
ctlplane=192.200.0.120 |
| 6810c884-1cb9-4321-9a07-192443920f1f | pod2-stack-osd-compute-0 | ACTIVE | - | Running |
ctlplane=192.200.0.109 |
| 26d3f7b1-ba97-431f-aa6e-ba91661db45d | pod2-stack-osd-compute-1 | ACTIVE | - | Running |
ctlplane=192.200.0.117 |
| 6e4a8aa9-4870-465a-a7e2-0932ff55e34b | pod2-stack-osd-compute-2 | ACTIVE | - | Running |
ctlplane=192.200.0.103 |
+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+

```

- Melden Sie sich beim betroffenen Controller an, und entfernen Sie den Standby-Modus unter Verwendung von Standby. Stellen Sie sicher, dass der Controller mit Cluster online ist, und Galera zeigt alle drei Controller als Master an. Dies kann einige Minuten in Anspruch nehmen:

```
[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.e17_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
```

- Sie können einige der Überwachungsdienste überprüfen, z. B. um festzustellen, dass sie sich in einem einwandfreien Zustand befinden:

```
[heat-admin@pod2-stack-controller-0 ~]$ sudo ceph -s
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
```