Instantané et récupération de la machine virtuelle CPAR

Contenu

Introduction

Ce document décrit une procédure pas à pas pour sauvegarder (instantané) les instances AAA (Authentication, Authorization, and Accounting).

Informations générales

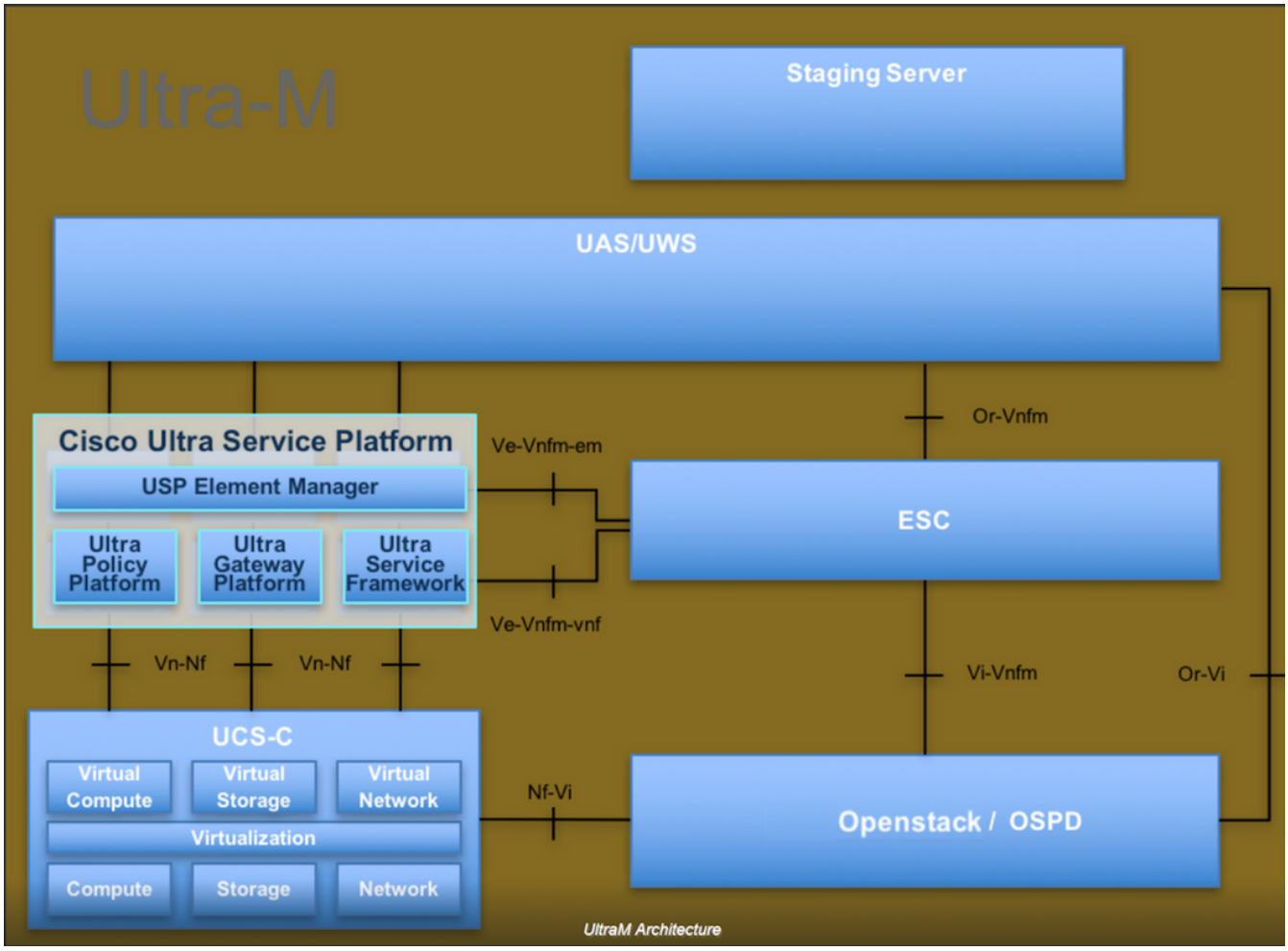
Il est impératif d'exécuter cette commande par site et un site à la fois afin de minimiser l'impact sur le trafic de l'abonné.

Cette procédure s'applique à un environnement Openstack avec l'utilisation de la version NEWTON où Elastic Services Controller (ESC) ne gère pas Cisco Prime Access Registrar (CPAR) et CPAR est installé directement sur la machine virtuelle (VM) déployée sur Openstack.

Ultra-M est une solution de coeur de réseau mobile virtualisé préemballée et validée, conçue pour simplifier le déploiement de Virtual Network Functions (VNF). OpenStack est le gestionnaire d'infrastructure virtualisée (VIM) pour Ultra-M et comprend les types de noeuds suivants :

- Calcul
- Disque de stockage d'objets - Calcul (OSD - Calcul)
- Contrôleur
- Plate-forme OpenStack - Director (OSPD)
- L'architecture de haut niveau d'Ultra-M et les composants impliqués sont représentés dans cette image

:



Ce document est destiné au personnel de Cisco qui connaît la plate-forme Cisco Ultra-M et décrit en détail les étapes requises pour effectuer les opérations sur les systèmes d'exploitation OpenStack et Redhat.

> **Note**: La version Ultra M 5.1.x est prise en compte afin de définir les procédures de ce document.

Impact du réseau

En général, lorsque le processus CPAR est arrêté, la dégradation des indicateurs de performance clés est attendue, car lorsque vous arrêtez l'application, il faut jusqu'à 5 minutes pour envoyer le déroutement de l'homologue de diamètre. À ce stade, toutes les demandes acheminées vers le CPAR échoueront. Après cette période, les liaisons sont arrêtées et l'agent de routage de diamètre (DRA) arrête le routage du trafic vers ce noeud.

En outre, pour toutes les sessions existantes de l'AAA qui sont arrêtées, s'il existe une procédure d'attachement/détachement qui implique ces sessions avec une autre AAA active, cette procédure échouera, car la sécurité hébergée en tant que service (HSS) répond que l'utilisateur est inscrit sur l'AAA qui est arrêté et que la procédure ne pourra pas être terminée correctement.

Les performances du STR devraient être inférieures à 90 % environ 10 heures après la fin de l'activité. Après ce délai, la valeur normale de 90 % doit être atteinte.

Alarmes

Les alarmes SNMP (Simple Network Management Protocol) sont générées chaque fois que le service CPAR est arrêté et démarré, de sorte que les déroutements SNMP doivent être générés tout au long du processus. Les pièges attendus sont les suivants :

- ARRÊT DU SERVEUR CPAR
- VM BAS
- NODE DOWN (alarme attendue qui n'est pas directement générée par l'instance CPAR)
- DRA

Sauvegarde instantanée de VM

Arrêt de l'application CPAR

> **Note**: Assurez-vous que vous avez accès à HORIZON pour le site en place et à OSPD.

Étape 1. Ouvrez tout client Secure Shell (SSH) connecté au réseau Production Transformation Management Office (TMO) et connectez-vous à l'instance CPAR.

> **Note**: Il est important de ne pas arrêter les 4 instances AAA d'un site en même temps, le faire une par une.

Étape 2. Pour arrêter l'application CPAR, exécutez la commande suivante :

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

Un message indiquant que l'agent Cisco Prime Access Registrar Server est arrêté doit s'afficher.

> **Note**: Si vous laissez la session CLI ouverte, la **commande arserver stop** ne fonctionne pas et ce message d'erreur s'affiche.

```
ERROR:    You can not shut down Cisco Prime Access Registrar while the

          CLI is being used.   Current list of running

          CLI with process id is:


2903 /opt/CSCOar/bin/aregcmd -s
```

Dans cet exemple, l'ID de processus mis en surbrillance 2903 doit être terminé avant que CPAR puisse être arrêté. Si c'est le cas, exécutez la commande et terminez ce processus :

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

Répétez ensuite l'étape 1.

Étape 3. Afin de vérifier que l'application CPAR a bien été arrêtée, exécutez la commande :

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

Ces messages doivent apparaître :

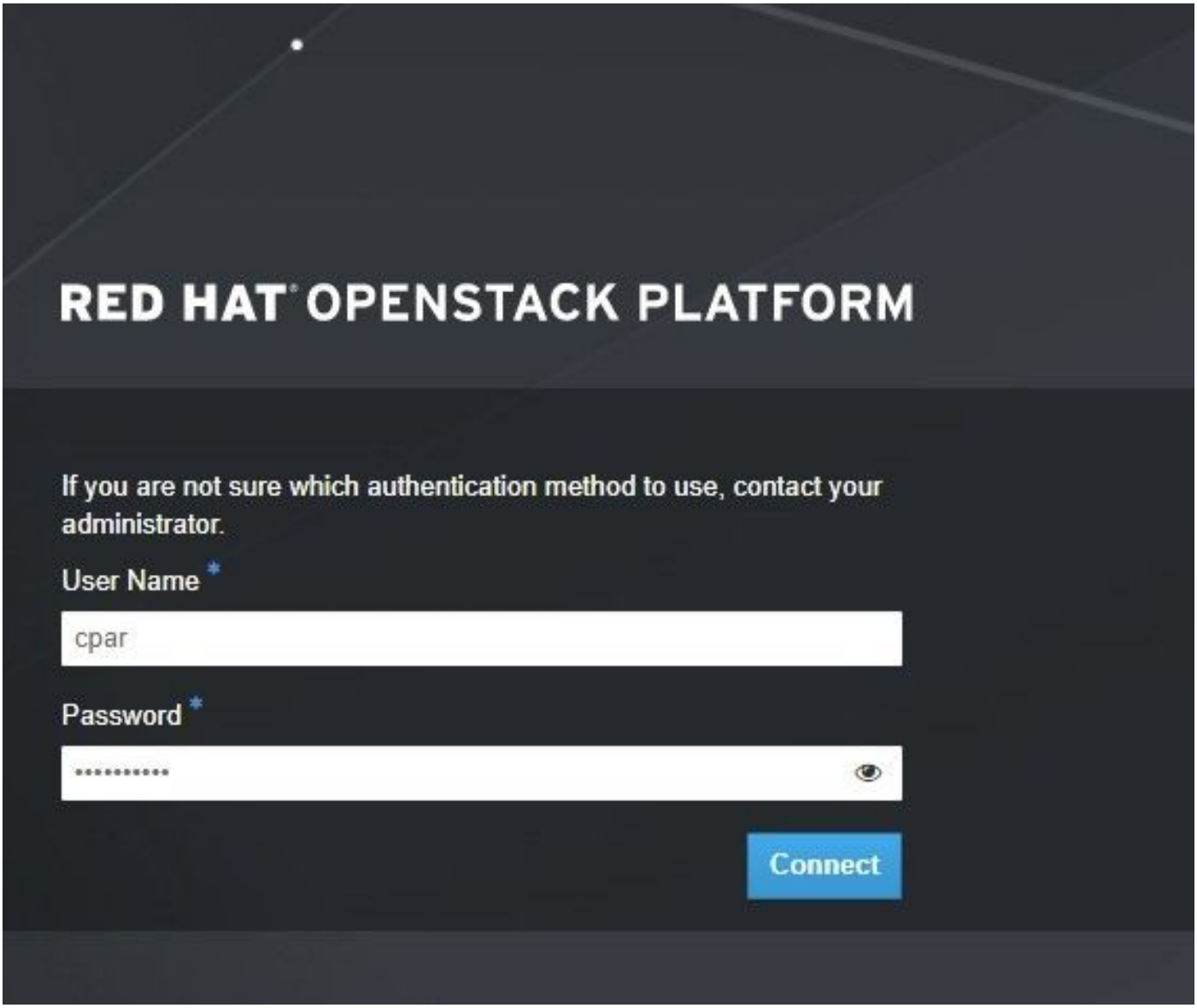
```
Cisco Prime Access Registrar Server Agent not running

Cisco Prime Access Registrar GUI not running
```

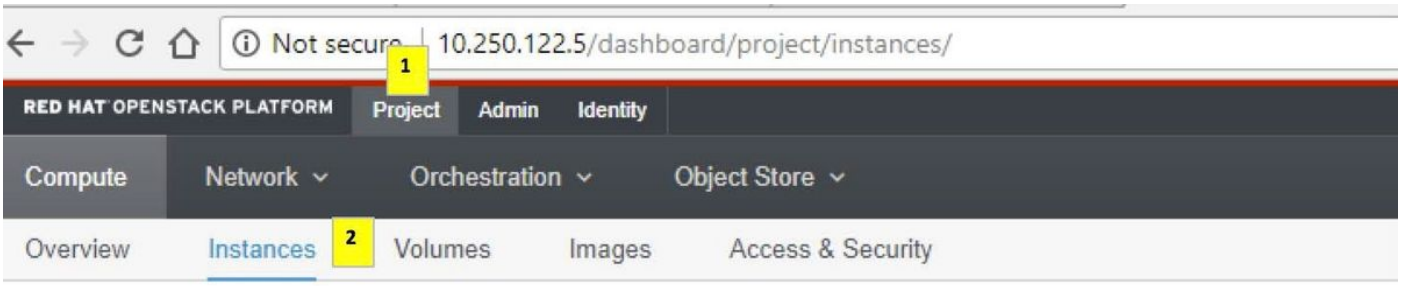
Tâche de capture instantanée de sauvegarde de VM

Étape 1. Saisissez le site Web de l'interface graphique d'Horizon correspondant au site (ville) sur lequel vous travaillez actuellement.

Lorsque vous accédez à Horizon, l'écran observé est tel qu'illustré dans l'image.

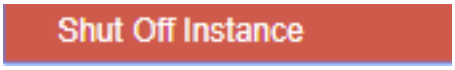


Étape 2. Accédez à **Project > Instances** comme indiqué dans l'image.



Si l'utilisateur utilisé était CPAR, seules les 4 instances AAA apparaissent dans ce menu.

Étape 3. Arrêtez une seule instance à la fois, répétez l'ensemble du processus de ce document. Afin d'arrêter la machine virtuelle, accédez à **Actions > Arrêter l'instance** comme indiqué dans l'image et confirmez votre sélection.



Étape 4. Afin de valider que l'instance est effectivement arrêtée, cochez la case Status = **Shutoff** and Power State = **Shut Down**, comme le montre l'image.

Cette étape met fin au processus d'arrêt CPAR.

Instantané VM

Une fois les machines virtuelles CPAR hors service, les snapshots peuvent être pris en parallèle, car ils appartiennent à des ordinateurs indépendants.

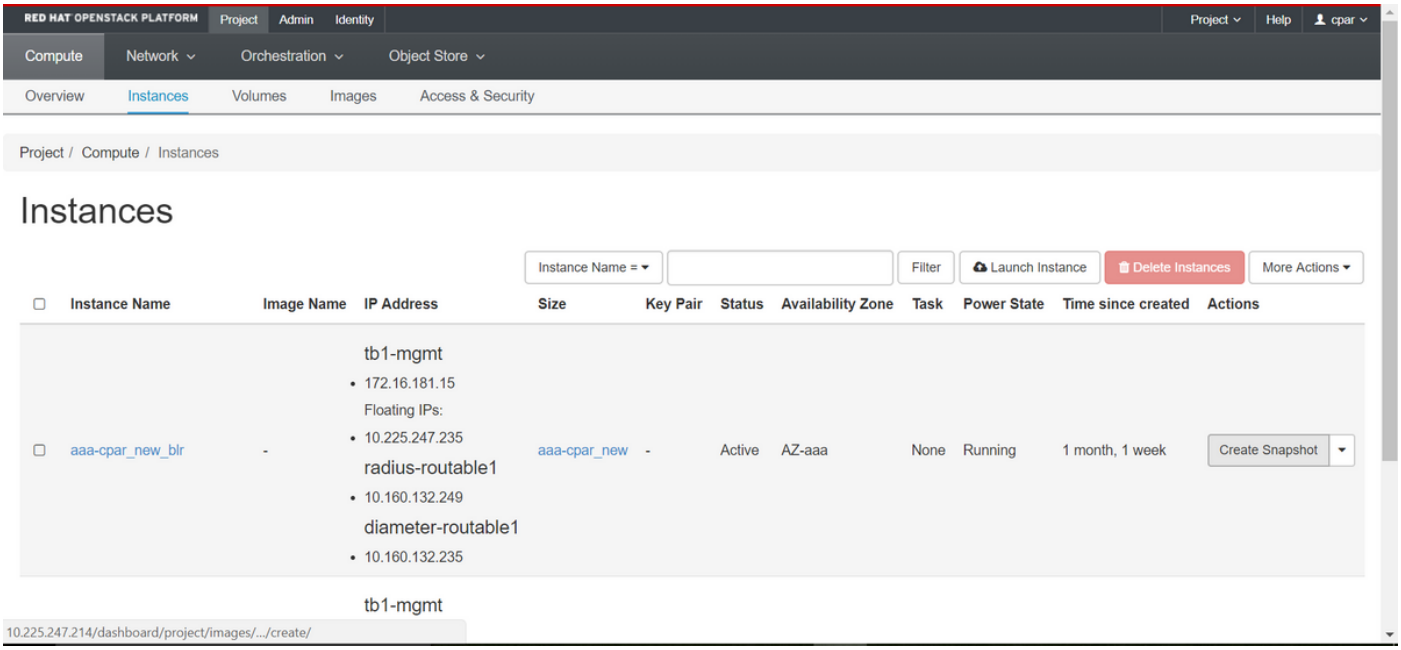
Les quatre fichiers QCOW2 sont créés en parallèle.

Étape 1. Prenez un instantané de chaque instance AAA.

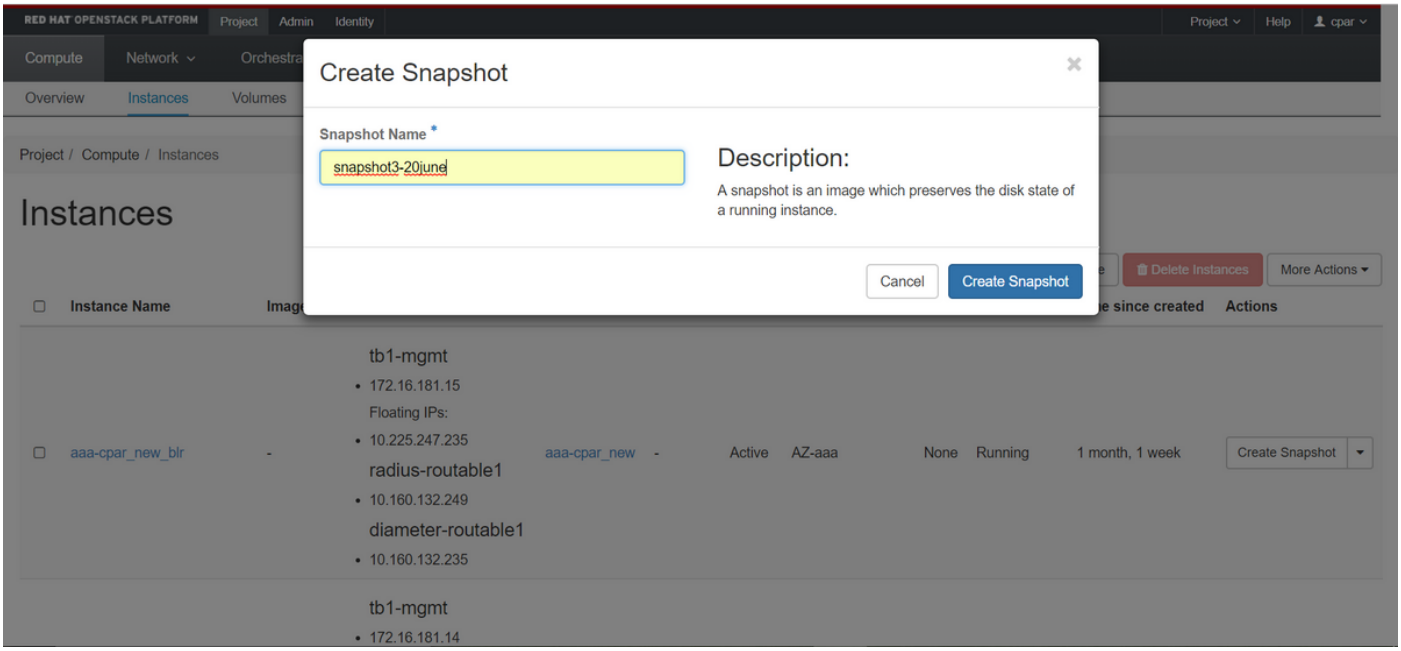
> **Note**: 25 minutes pour les instances qui utilisent une image QCOW comme source et 1 heure pour les instances qui utilisent une image brute comme source.

Étape 2. Connectez-vous à l'**interface graphique** Horizon d'Openstack de POD.

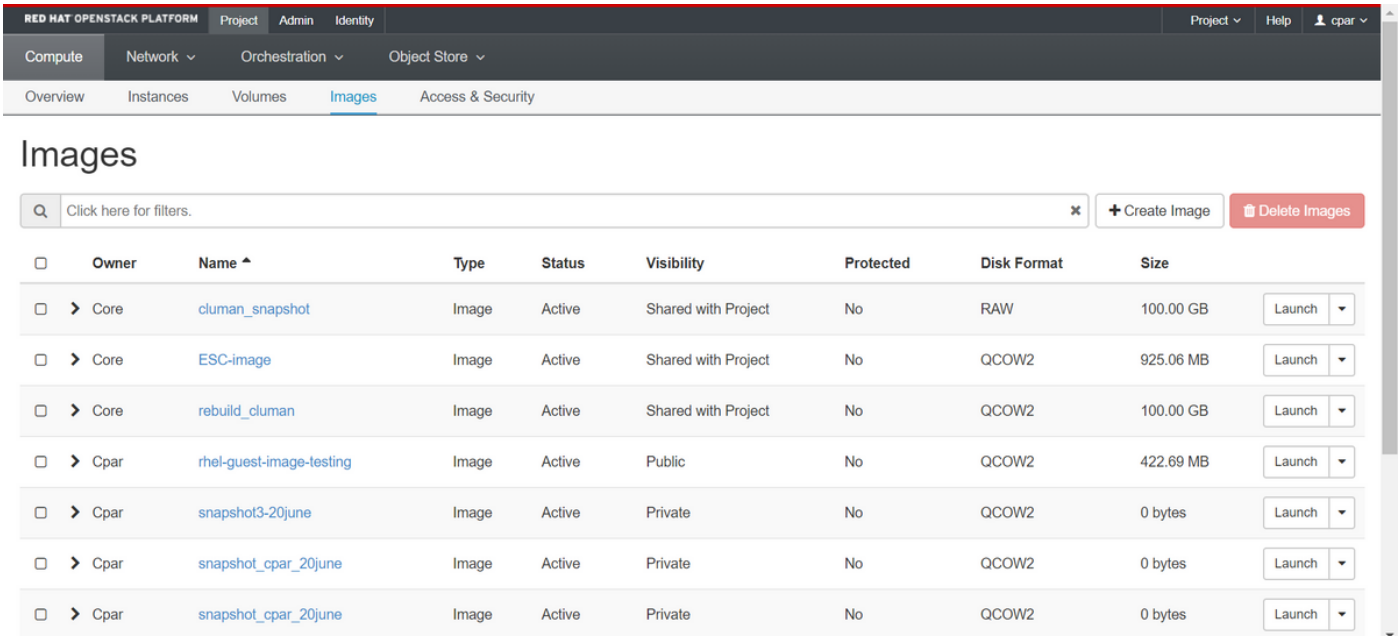
Étape 3. Une fois connecté, accédez à **Project > Compute > Instances** dans le menu supérieur et recherchez les instances AAA comme indiqué dans l'image.



Étape 3. Cliquez sur **Create Snapshot** afin de poursuivre la création de clichés comme indiqué dans l'image. Ceci doit être exécuté sur l'instance AAA correspondante.



Étape 4. Une fois l'instantané exécuté, accédez au menu **Images** et vérifiez que tout se termine et ne signale aucun problème comme indiqué dans l'image.



Étape 5. L'étape suivante consiste à télécharger l'instantané au format QCOW2 et à le transférer à une entité distante, au cas où l'OSPD serait perdu dans ce processus. Pour ce faire, identifiez l'instantané en exécutant la commande **glance image-list** au niveau OSPD, comme illustré dans l'image.

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

Étape 6. Une fois que vous avez identifié le snapshot à télécharger (dans ce cas, c'est celui marqué en vert), vous pouvez le télécharger au format QCOW2 avec la commande **glance image-download** comme illustré ici :

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

Le **&** envoie le processus en arrière-plan. Il faut un certain temps pour terminer l'action. Une fois cette opération terminée, l'image peut être localisée dans le répertoire **/tmp**.

- Lorsque vous envoyez le processus en arrière-plan et que la connectivité est perdue, le processus est également arrêté.
- Exécutez la commande **disown -h** afin que, en cas de perte de connexion SSH, le processus continue à s'exécuter et se termine sur l'OSPD.

Étape 7. Une fois le processus de téléchargement terminé, un processus de compression doit être exécuté car ce snapshot peut être rempli de ZEROES en raison de processus, de tâches et de fichiers temporaires gérés par le système d'exploitation (OS). La commande à exécuter pour la

compression de fichiers est **virt-sparsify**.

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

Ce processus peut prendre un certain temps (environ 10 à 15 minutes). Une fois terminé, le fichier qui en résulte est celui qui doit être transféré à une entité externe comme spécifié à l'étape suivante.

Pour ce faire, vous devez vérifier l'intégrité du fichier. Exécutez la commande suivante et recherchez l'attribut ” corrompu “ à la fin de sa sortie.

```
[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
```

Étape 8. Afin d'éviter un problème de perte de l'OSPD, l'instantané récemment créé au format QCOW2 doit être transféré à une entité externe. Avant de commencer le transfert de fichiers, vous devez vérifier si la destination a suffisamment d'espace disque disponible, exécutez la commande **df -kh** afin de vérifier l'espace mémoire.

Il est conseillé de le transférer temporairement à l'OSPD d'un autre site avec l'utilisation de SFTP **sftp** root@x.x.x.xwhere **x.x.x.x** est l'adresse IP d'un OSPD distant.

Étape 9. Afin d'accélérer le transfert, la destination peut être envoyée à plusieurs OSPD. De la même manière, vous pouvez exécuter la commande **scp *name_of_the_file*.qcow2 root@ x.x.x.x:/tmp** (où **x.x.x.x** est l'adresse IP d'un OSPD distant) afin de transférer le fichier vers un autre OSPD.

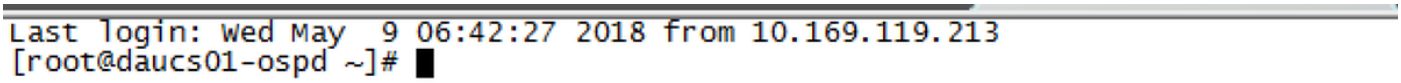
Récupérer une instance avec un snapshot

Processus de récupération

Il est possible de redéployer l'instance précédente avec l'instantané effectué lors des étapes précédentes.

Étape 1. [FACULTATIF] S'il n'y a pas de capture instantanée de machine virtuelle précédente disponible, connectez-vous au noeud OSPD où la sauvegarde a été envoyée et redirigez la sauvegarde vers son noeud OSPD d'origine. Utilisez **sftp** root@x.x.x.x, où **x.x.x.x** est l'adresse IP d'un OSPD d'origine. Enregistrez le fichier d'instantané dans le répertoire **/tmp**.

Étape 2. Connectez-vous au noeud OSPD où l'instance est redéployée, comme illustré dans l'image.

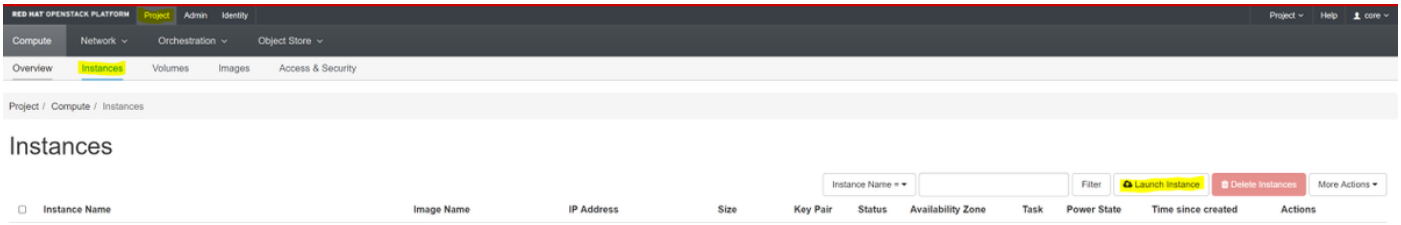


Étape 3. Pour utiliser l'instantané comme image, il est nécessaire de le télécharger sur horizon en tant que tel. Utilisez la commande suivante pour cela.

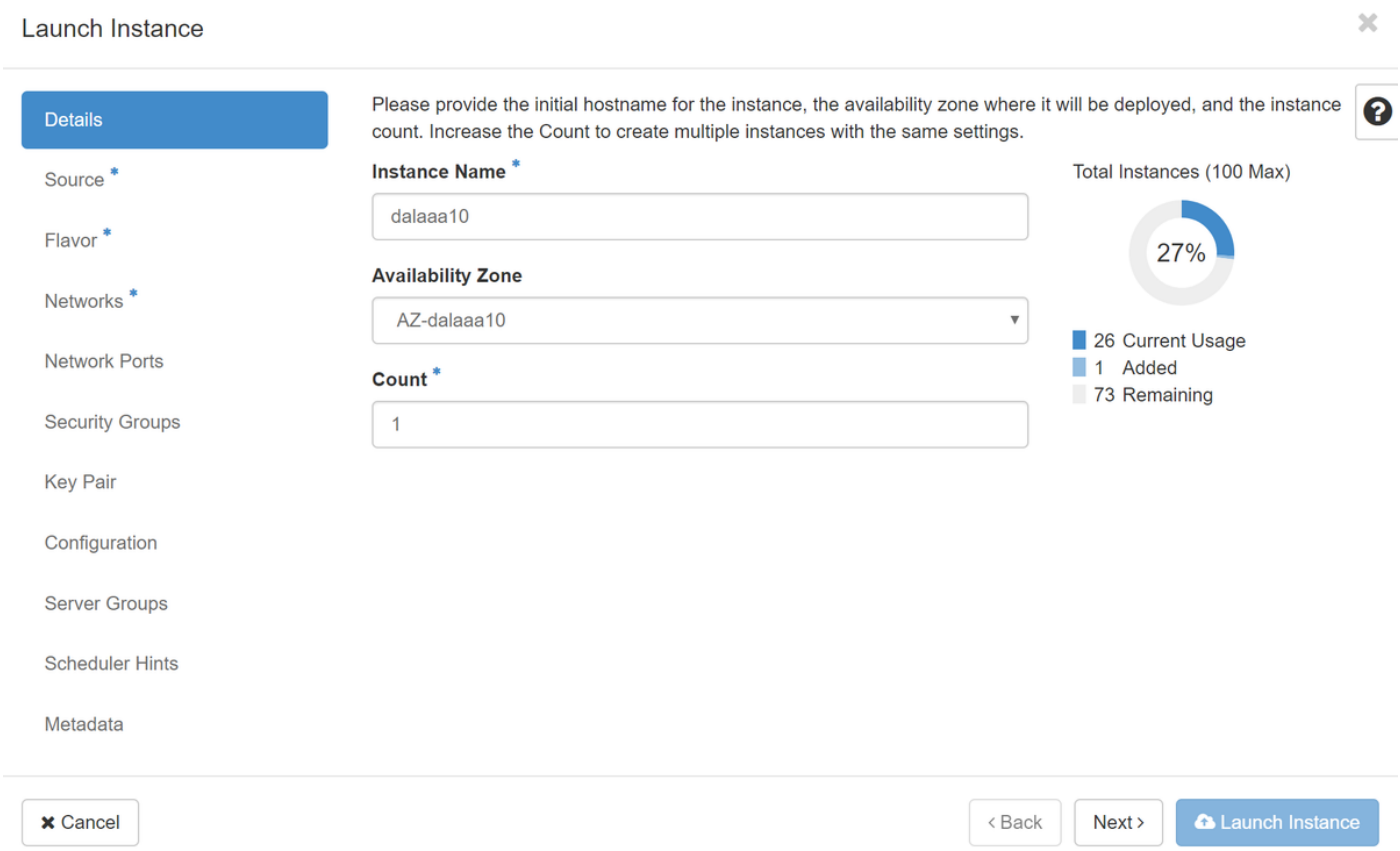
```
#glance image-create -- AAA-CPAR-Date-snapshot.qcow2 --container-format bare --disk-format qcow2
--name AAA-CPAR-Date-snapshot
```

Le processus peut être vu à l'horizon et comme le montre l'image.

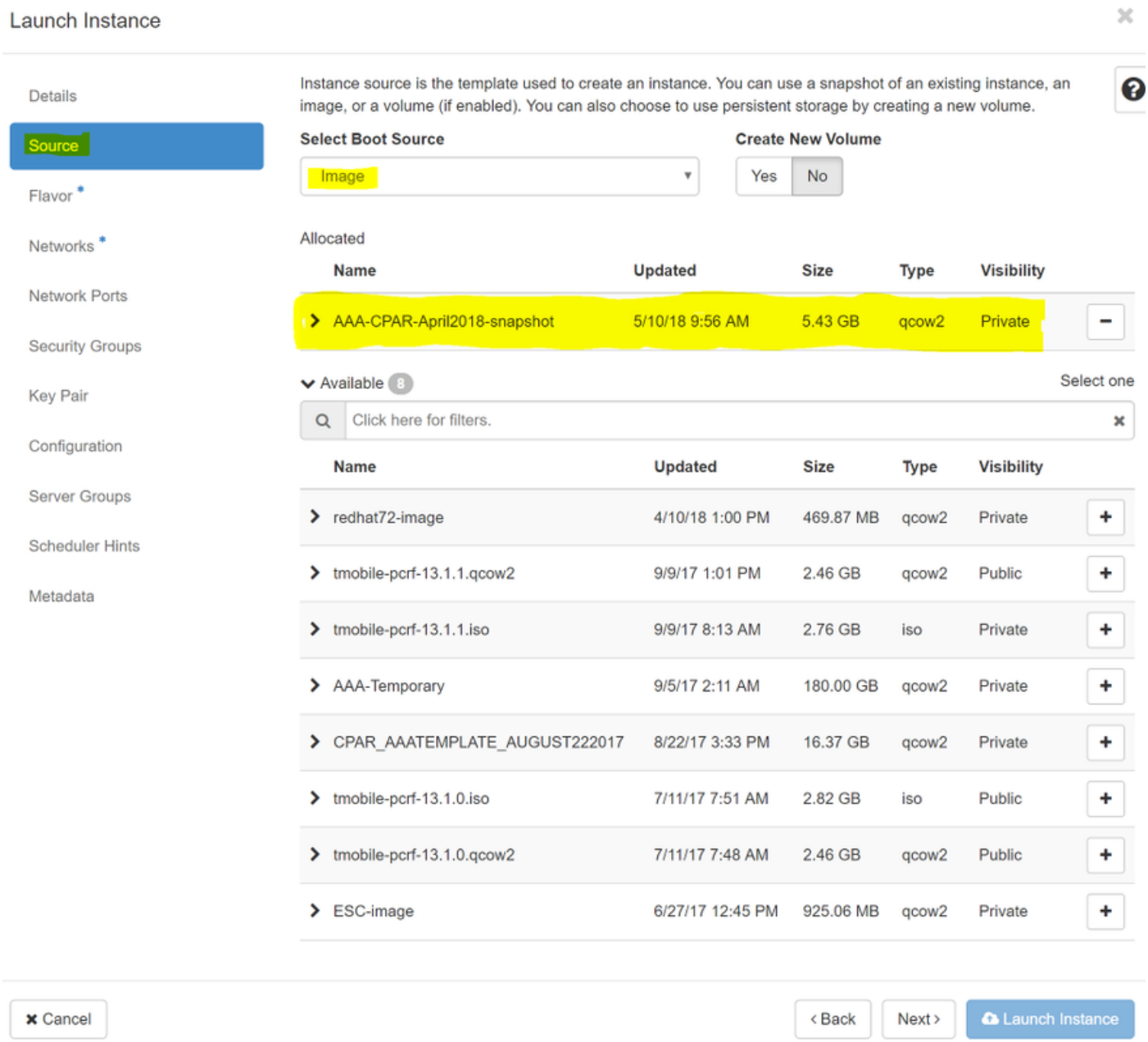
Étape 4. Dans Horizon, accédez à **Project > Instances** et cliquez sur **Lancer l'instance** comme indiqué dans l'image.



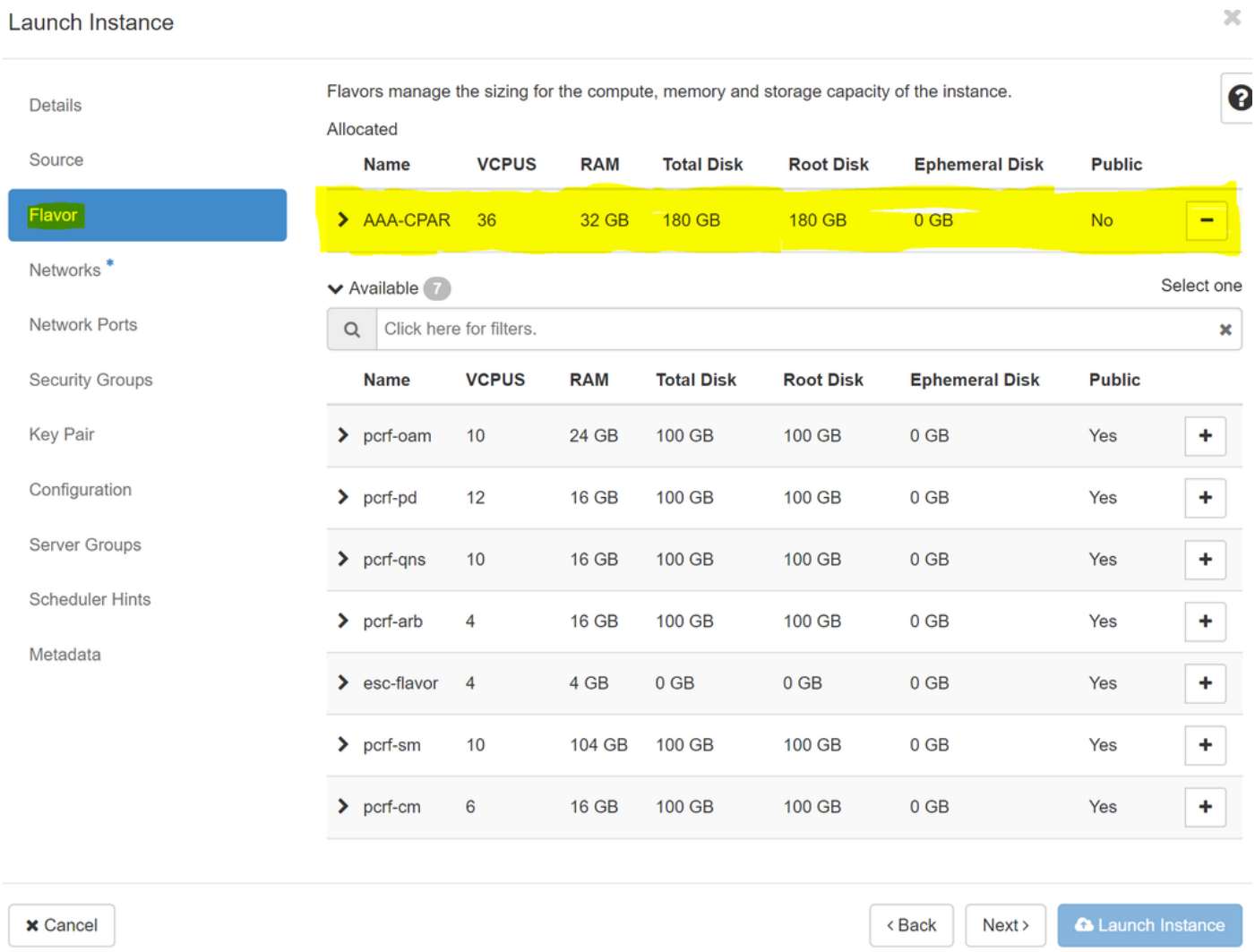
Étape 5. Entrez le **nom de l'instance** et choisissez la **zone de disponibilité** comme indiqué dans l'image.



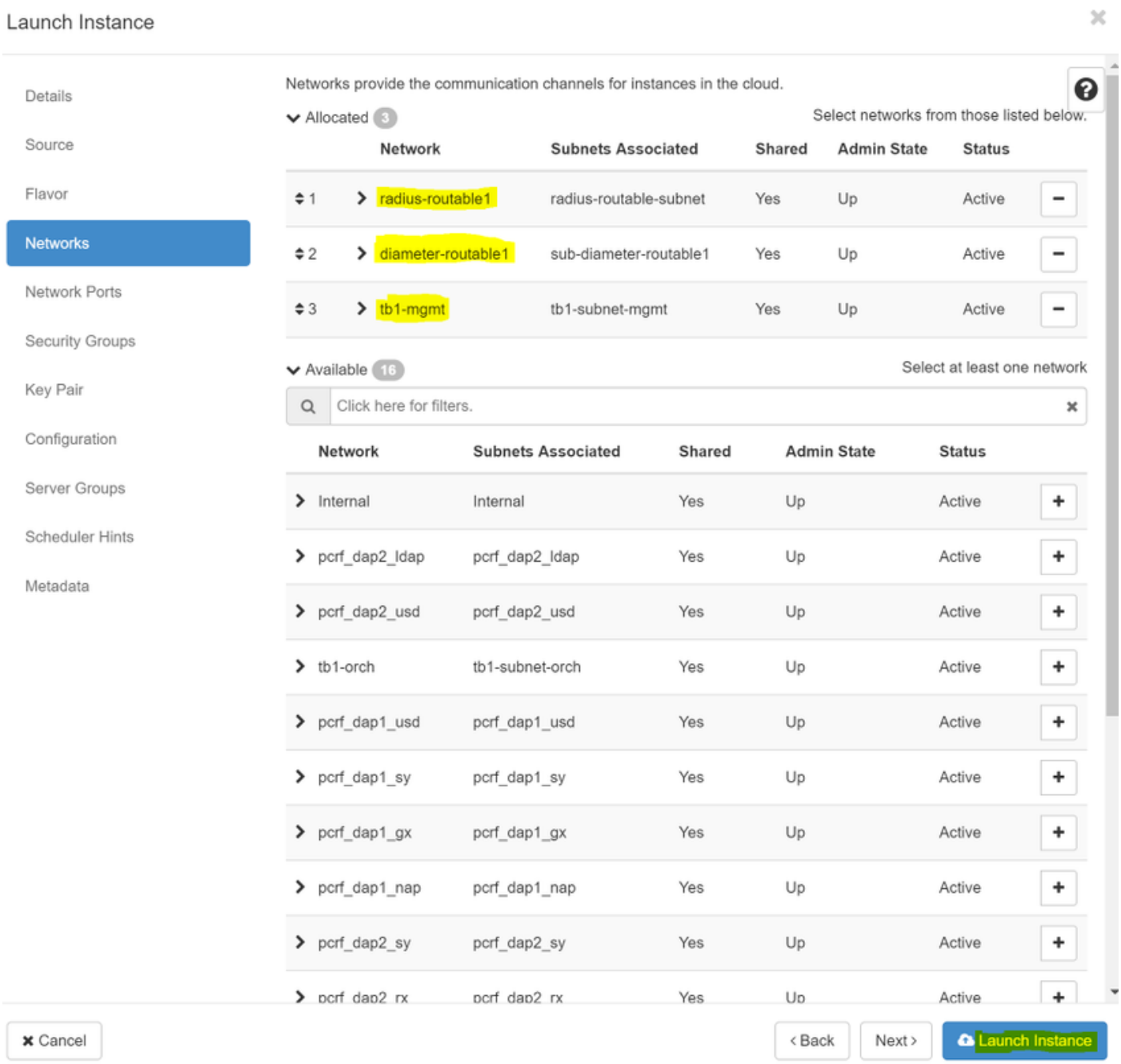
Étape 6. Dans l'onglet Source, sélectionnez l'image afin de créer l'instance. Dans le menu Sélectionner la source de démarrage, sélectionnez **image** et une liste d'images s'affiche ici. Choisissez celui qui a été précédemment téléchargé en cliquant sur son **+** signe comme indiqué dans l'image.



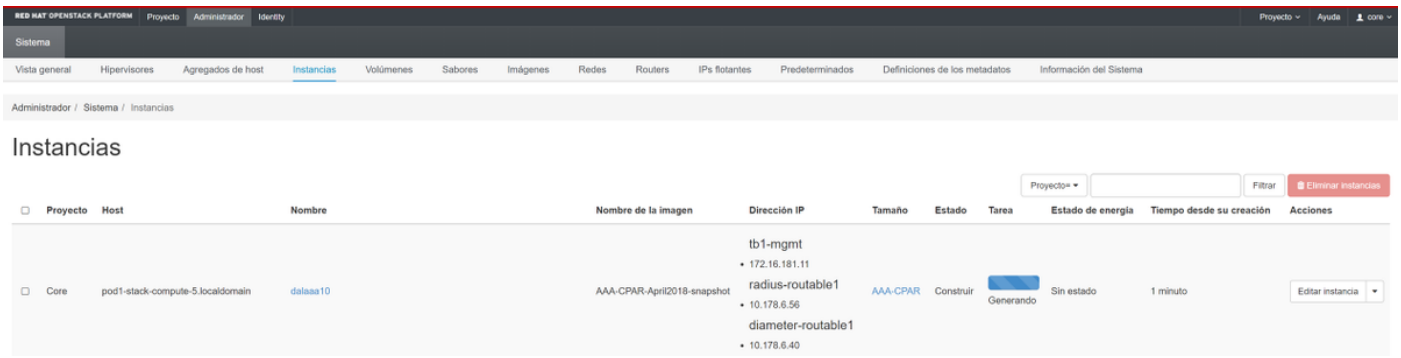
Étape 7. Dans l'onglet Saveur, choisissez la saveur AAA en cliquant sur le signe **+** comme indiqué dans l'image.



Étape 8. Enfin, accédez à l'onglet **Réseaux** et choisissez les réseaux dont l'instance aura besoin en cliquant sur le signe **+**. Dans ce cas, sélectionnez **diamètre-soutable1**, **radius-routable1** et **tb1-mgmt** comme indiqué dans l'image.



Étape 9. Cliquez sur **Lancer l'instance** afin de la créer. La progression peut être surveillée dans Horizon comme l'illustre l'image.



Étape 10. Au bout de quelques minutes, l'instance est entièrement déployée et prête à être utilisée, comme l'illustre l'image.

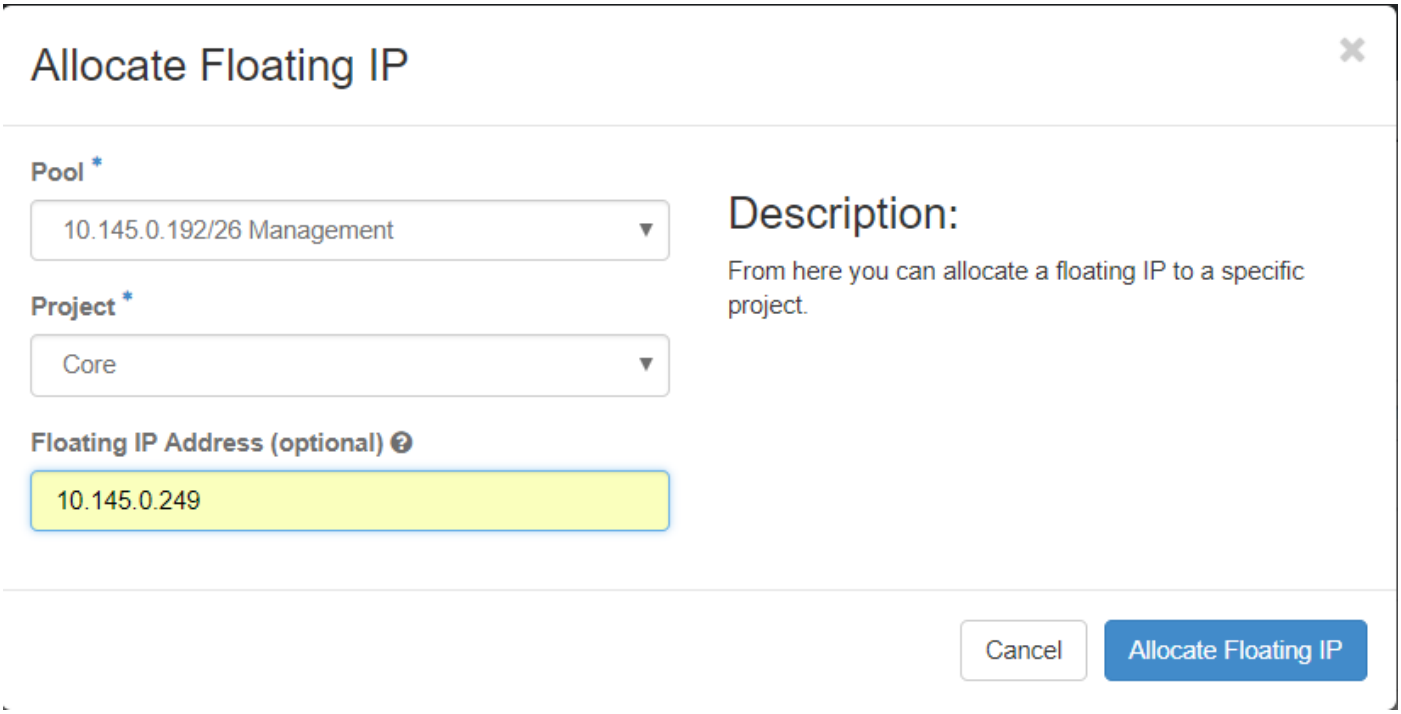
Créer et attribuer une adresse IP flottante

Une adresse IP flottante est une adresse routable, ce qui signifie qu'elle est accessible depuis l'extérieur de l'architecture Ultra M/Openstack et qu'elle peut communiquer avec d'autres noeuds du réseau.

Étape 1. Dans le menu supérieur Horizon, accédez à **Admin > Floating IPs**.

Étape 2. Cliquez sur **Allouer IP au projet**.

Étape 3. Dans la fenêtre **Allouer une adresse IP flottante**, sélectionnez le **pool** auquel appartient la nouvelle adresse IP flottante, le **projet** où elle sera affectée et la nouvelle **adresse IP flottante** elle-même comme indiqué dans l'image.

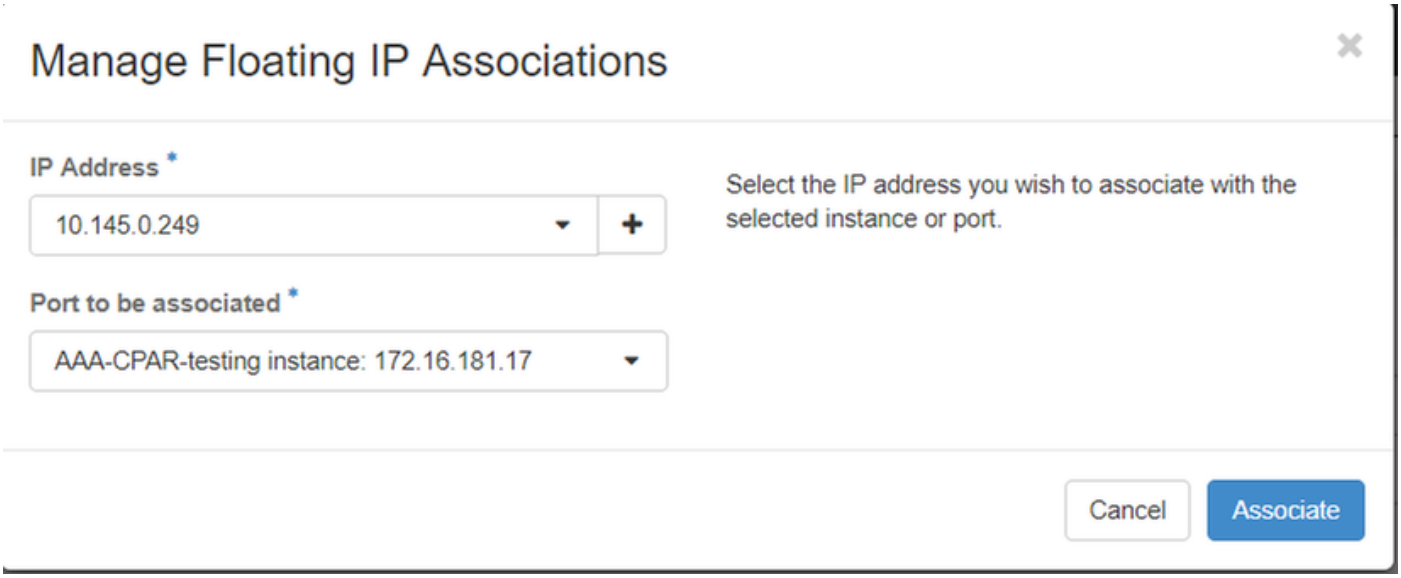


Étape 4. Cliquez sur **Allouer IP flottante**.

Étape 5. Dans le menu supérieur Horizon, accédez à **Project > Instances**.

Étape 6. Dans la colonne **Action**, cliquez sur la flèche pointant vers le bas dans le bouton **Créer un instantané**, un menu s'affiche. Cliquez sur **Associer une** option **IP flottante**.

Étape 7. Sélectionnez l'adresse IP flottante correspondante à utiliser dans le champ **Adresse IP**, puis choisissez l'interface de gestion correspondante (eth0) dans la nouvelle instance où cette adresse IP flottante sera attribuée dans le **port à associer** comme indiqué dans l'image.



Étape 8. Cliquez sur **Associer**.

Activer SSH

Étape 1. Dans le menu supérieur Horizon, accédez à **Project > Instances**.

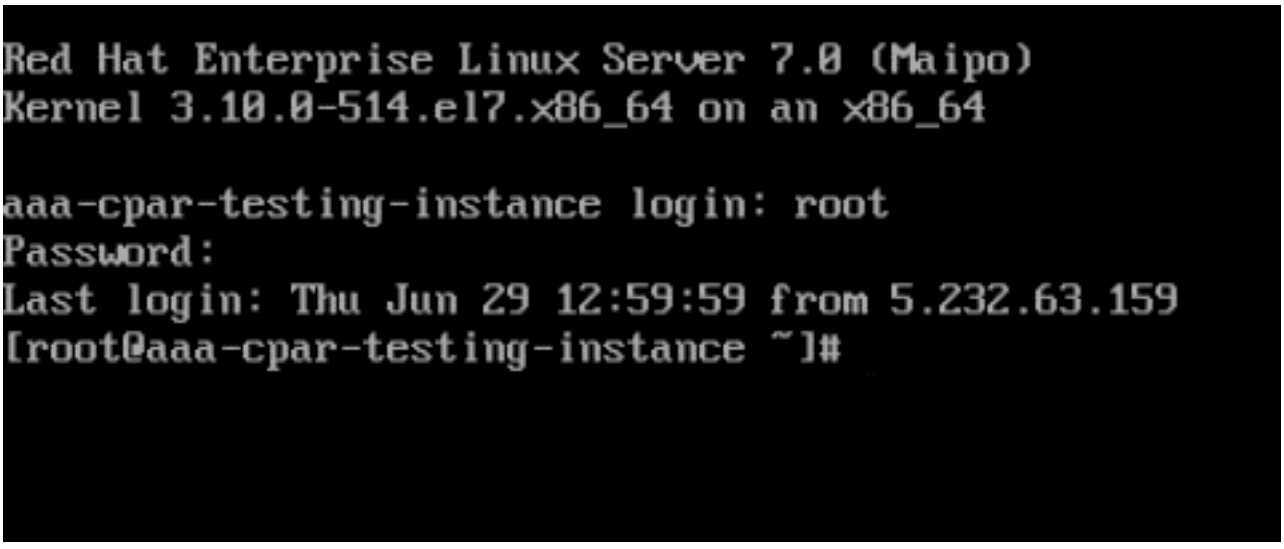
Étape 2. Cliquez sur le nom de l'instance/de la machine virtuelle créée dans la section **Lancer une nouvelle instance**.

Étape 3. Cliquez sur **Console**. Affiche l'interface de ligne de commande de la machine virtuelle.

Étape 4. Une fois l'interface de ligne de commande affichée, saisissez les informations d'identification de connexion appropriées, comme indiqué dans l'image :

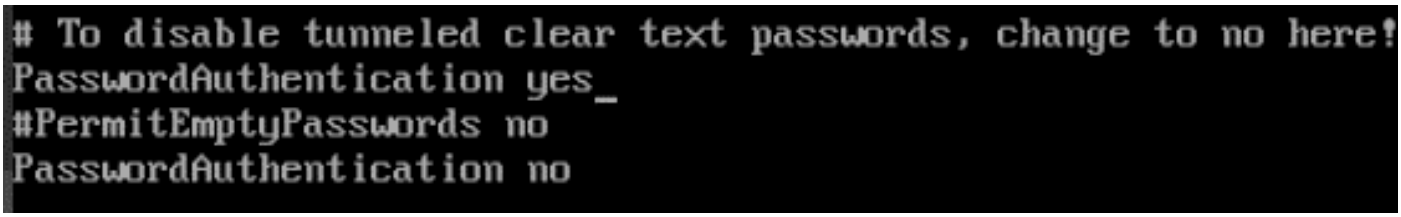
username (nom d'utilisateur) : **racine**

Mot de passe : **<cisco123>**



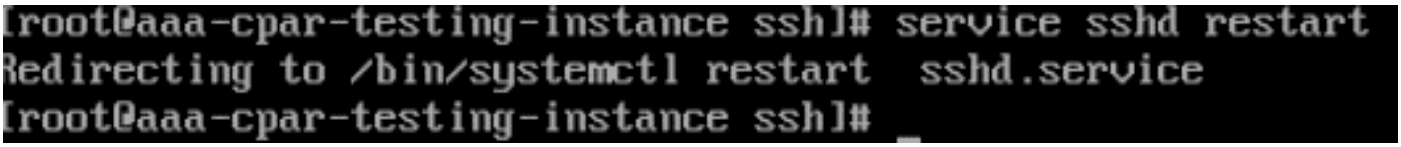
Étape 5. Dans l'interface de ligne de commande, exécutez la commande **vi /etc/ssh/sshd_config** afin de modifier la configuration SSH.

Étape 6. Une fois le fichier de configuration SSH ouvert, appuyez sur **I** afin de modifier le fichier. Ensuite, changez la première ligne de **PasswordAuthentication no** à **PasswordAuthentication yes** comme indiqué dans l'image.

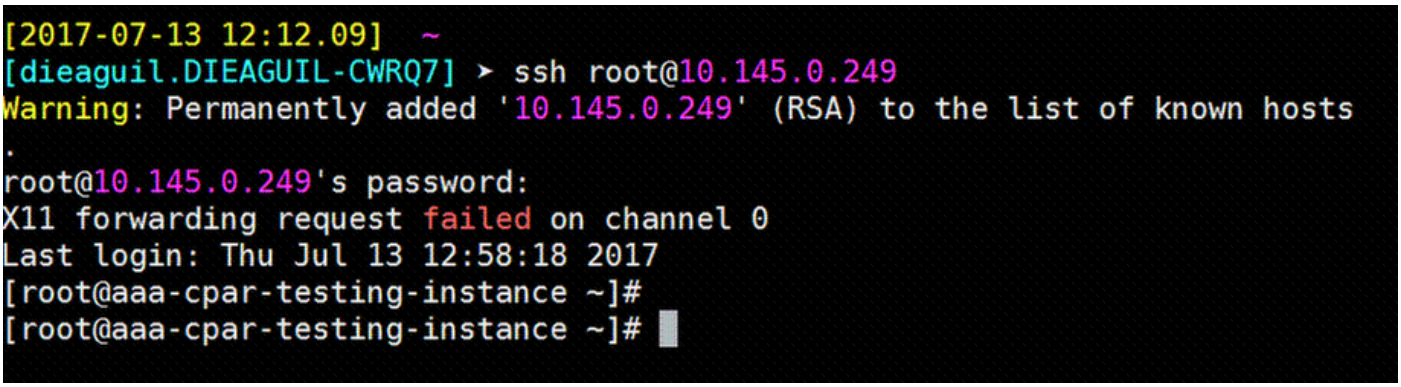


Étape 7. Appuyez sur **Échap** et saisissez **:wq!** afin d'enregistrer les modifications de fichier **sshd_config**.

Étape 8. Exécutez la commande **service sshd restart comme indiqué dans l'image.**

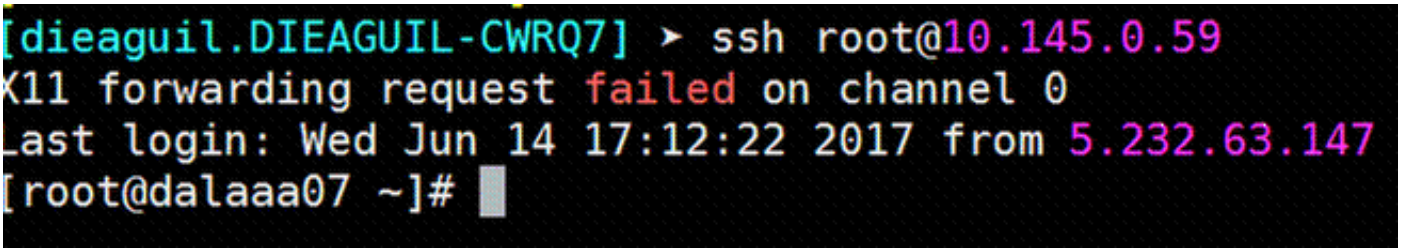


Étape 9. Afin de tester si les modifications de configuration SSH ont été correctement appliquées, ouvrez n'importe quel client SSH et essayez d'établir une connexion sécurisée à distance avec l'adresse IP flottante attribuée à l'instance (c'est-à-dire **10.145.0.249**) et la **racine** utilisateur comme indiqué dans l'image.



Établir une session SSH

Étape 1. Ouvrez une session SSH avec l'adresse IP de la machine virtuelle/serveur correspondante sur laquelle l'application est installée, comme illustré dans l'image.



Début de l'instance CPAR

Suivez ces étapes une fois l'activité terminée et les services CPAR peuvent être rétablis sur le site

qui a été arrêté.

Étape 1. Reconnectez-vous à Horizon, accédez à **project > instance > start instance**.

Étape 2. Vérifiez que l'état de l'instance est **Actif** et que l'état d'alimentation est **En cours d'exécution** comme indiqué dans l'image.

Vérification de l'intégrité après activité

Étape 1. Exécutez la commande **/opt/CSCOar/bin/arstatus** au niveau du système d'exploitation :

```
[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 ~]#
```

Étape 2. Exécutez la commande **/opt/CSCOar/bin/aregcmd** au niveau du système d'exploitation et saisissez les informations d'identification de l'administrateur. Vérifiez que l'intégrité CPAR est 10 sur 10 et quittez l'interface CLI CPAR.

```
[root@aaa02 logs]# /opt/CSCOar/bin/aregcmd

Cisco Prime Access Registrar 7.3.0.1 Configuration Utility

Copyright (C) 1995-2017 by Cisco Systems, Inc.  All rights reserved.

Cluster:

User: admin

Passphrase:

Logging in to localhost
```

```
[ //localhost ]

    LicenseInfo = PAR-NG-TPS 7.3(100TPS:)

                  PAR-ADD-TPS 7.3(2000TPS:)

                  PAR-RDDR-TRX 7.3()

                  PAR-HSS 7.3()

    Radius/

    Administrators/


Server 'Radius' is Running, its health is 10 out of 10


--> exit
```

Étape 3. Exécutez la commande **netstat | grand diamètre** et vérifiez que toutes les connexions DRA sont établies.

Le résultat mentionné ici est pour un environnement où des liaisons de diamètre sont attendues. Si moins de liens sont affichés, cela représente une déconnexion du DRA qui doit être analysée.

```
[root@aa02 logs]# netstat | grep diameter

tcp         0            0 aaa02.aaa.epc.:77 mp1.dra01.d:diameter ESTABLISHED

tcp         0            0 aaa02.aaa.epc.:36 tsa6.dra01:diameter ESTABLISHED

tcp         0            0 aaa02.aaa.epc.:47 mp2.dra01.d:diameter ESTABLISHED

tcp         0            0 aaa02.aaa.epc.:07 tsa5.dra01:diameter ESTABLISHED

tcp         0            0 aaa02.aaa.epc.:08 np2.dra01.d:diameter ESTABLISHED
```

Étape 4. Vérifiez que le journal TelePresence Server (TPS) affiche les demandes traitées par CPAR. Les valeurs mises en évidence représentent le TPS et celles-ci sont celles auxquelles vous devez prêter attention.

La valeur de TPS ne doit pas dépasser 1 500.

```
[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
```

Étape 5. Recherchez tous les messages de ” d'erreur “ ou “ dans name_radius_1_log :

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

Étape 6. Afin de vérifier la quantité de mémoire utilisée par le processus CPAR, exécutez la commande :

```
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
```

Cette valeur mise en surbrillance doit être inférieure à 7 Go, ce qui correspond au maximum autorisé au niveau de l'application.