Istantanea e ripristino di VM CPAR

Sommario

Introduzione

In questo documento viene descritta una procedura dettagliata per eseguire il backup (snapshot) delle istanze di autenticazione, autorizzazione e accounting (AAA).

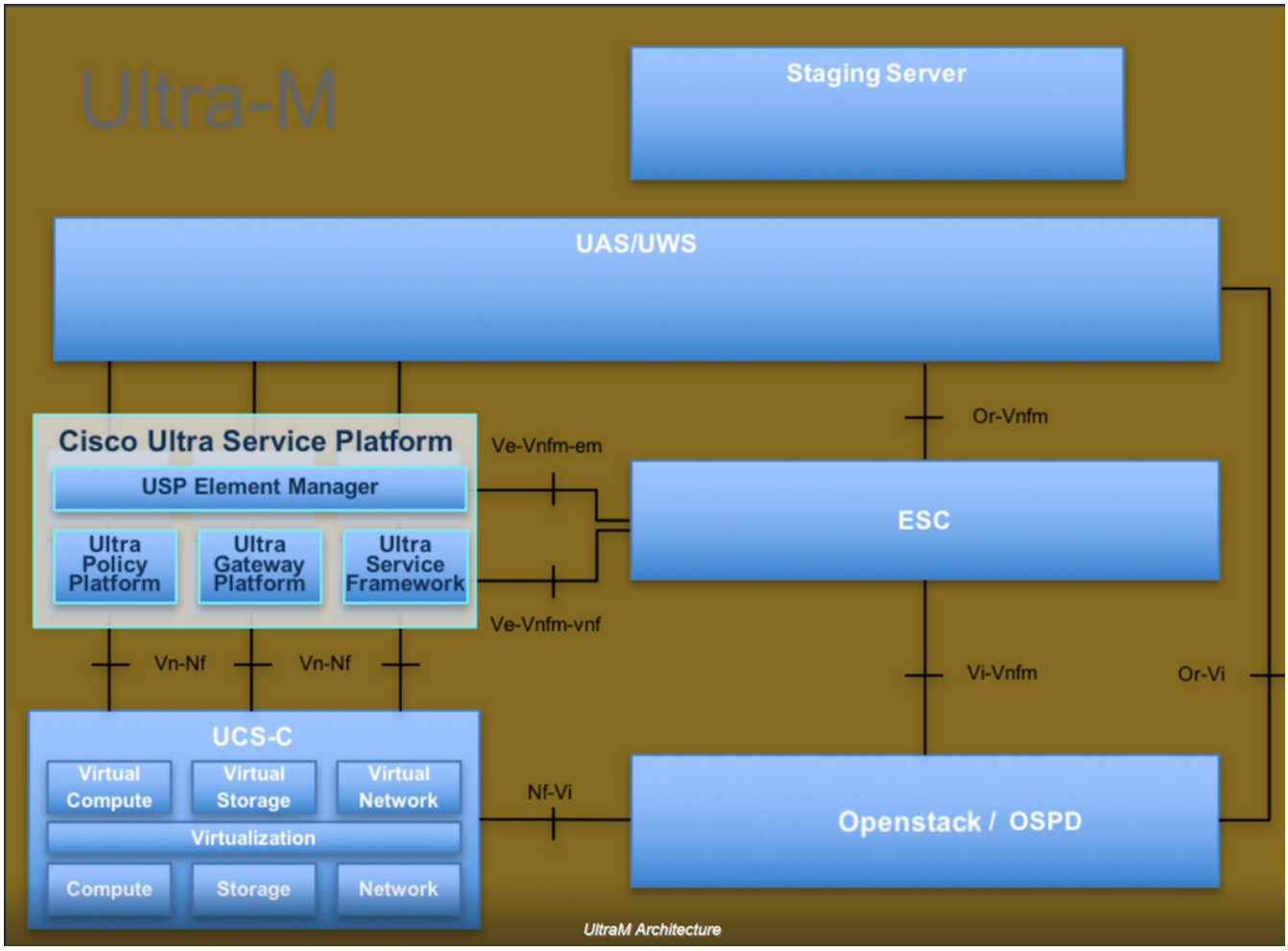
Premesse

Èessenziale eseguire questa operazione su ciascun sito e un sito alla volta per ridurre al minimo l'impatto sul traffico dell'abbonato.

Questa procedura è valida per un ambiente Openstack con la versione NEWTON in cui Elastic Services Controller (ESC) non gestisce Cisco Prime Access Registrar (CPAR) e CPAR viene installato direttamente sulla macchina virtuale (VM) distribuita su Openstack.

Ultra-M è una soluzione di base di pacchetti mobili preconfezionata e convalidata, progettata per semplificare l'installazione delle funzioni di rete virtuale (VNF). OpenStack è il Virtual Infrastructure Manager (VIM) per Ultra-M ed è costituito dai seguenti tipi di nodi:

- Calcola
- Disco Object Storage - Compute (OSD - Compute)
- Controller
- Piattaforma OpenStack - Director (OSPD)
- L'architettura di alto livello di Ultra-M e i componenti coinvolti sono illustrati in questa immagine:



Questo documento è destinato al personale Cisco che ha familiarità con la piattaforma Cisco Ultra-M e descrive in dettaglio i passaggi richiesti per eseguire operazioni su OpenStack e Redhat OS.

> **Nota:** Per definire le procedure descritte in questo documento, viene presa in considerazione la release di Ultra M 5.1.x.

Impatto sulla rete

In generale, quando il processo di CPAR viene interrotto, si prevede un peggioramento degli indicatori KPI, in quanto quando si chiude l'applicazione, sono necessari fino a 5 minuti per l'invio della trap di riduzione del diametro. In questo momento, tutte le richieste instradate verso CPAR avranno esito negativo. Trascorso questo periodo, i collegamenti risultano inattivi e Diameter Routing Agent (DRA) interrompe il routing del traffico verso questo nodo.

Inoltre, per tutte le sessioni esistenti nell'AAA che vengono chiuse, se esiste una procedura di collegamento/scollegamento che coinvolge queste sessioni con un altro AAA attivo, tale procedura avrà esito negativo, in quanto l'HSS (Hosted Security as a Service) risponde che l'utente è registrato nell'AAA che viene chiusa e la procedura non potrà essere completata correttamente.

Le prestazioni STR dovrebbero essere inferiori al 90% della percentuale di successo circa 10 ore dopo il completamento dell'attività. Trascorso tale periodo, il valore normale del 90% deve essere raggiunto.

Allarmi

Gli allarmi SNMP (Simple Network Management Protocol) vengono generati ogni volta che il servizio CPAR viene arrestato e avviato, quindi si prevede che le trap SNMP vengano generate durante tutto il processo. Le trap previste includono:

- ARRESTO SERVER CPAR
- VM INATTIVA
- NODE DOWN - (allarme previsto non generato direttamente dall'istanza CPAR)
- DRA

Backup snapshot VM

Arresto applicazione CPAR

> **Nota:** Accertarsi di disporre dell'accesso Web a HORIZON per il sito e dell'accesso a OSPD.

Passaggio 1. Aprire un client Secure Shell (SSH) connesso alla rete di produzione Transformation Management Office (TMO) e connettersi all'istanza CPAR.

> **Nota:** È importante non arrestare tutte e 4 le istanze AAA all'interno di un sito contemporaneamente, farlo una alla volta.

Passaggio 2. Per arrestare l'applicazione CPAR, eseguire il comando:

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

Deve essere visualizzato il messaggio "Cisco Prime Access Registrar Server Agent shutdown complete".

> **Nota:** Se si lascia aperta la sessione CLI, il **comando arserver stop** non funziona e viene visualizzato questo messaggio di errore.

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

          CLI is being used.   Current list of running

          CLI with process id is:


2903 /opt/CSCOar/bin/aregcmd –s
```

In questo esempio, è necessario terminare il processo evidenziato con ID 2903 prima di poter arrestare CPAR. In questo caso, eseguire il comando e terminare il processo:

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

Ripetere quindi il passaggio 1.

Passaggio 3. Per verificare che l'applicazione CPAR sia stata effettivamente chiusa, eseguire il comando:

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

Devono essere visualizzati i seguenti messaggi:

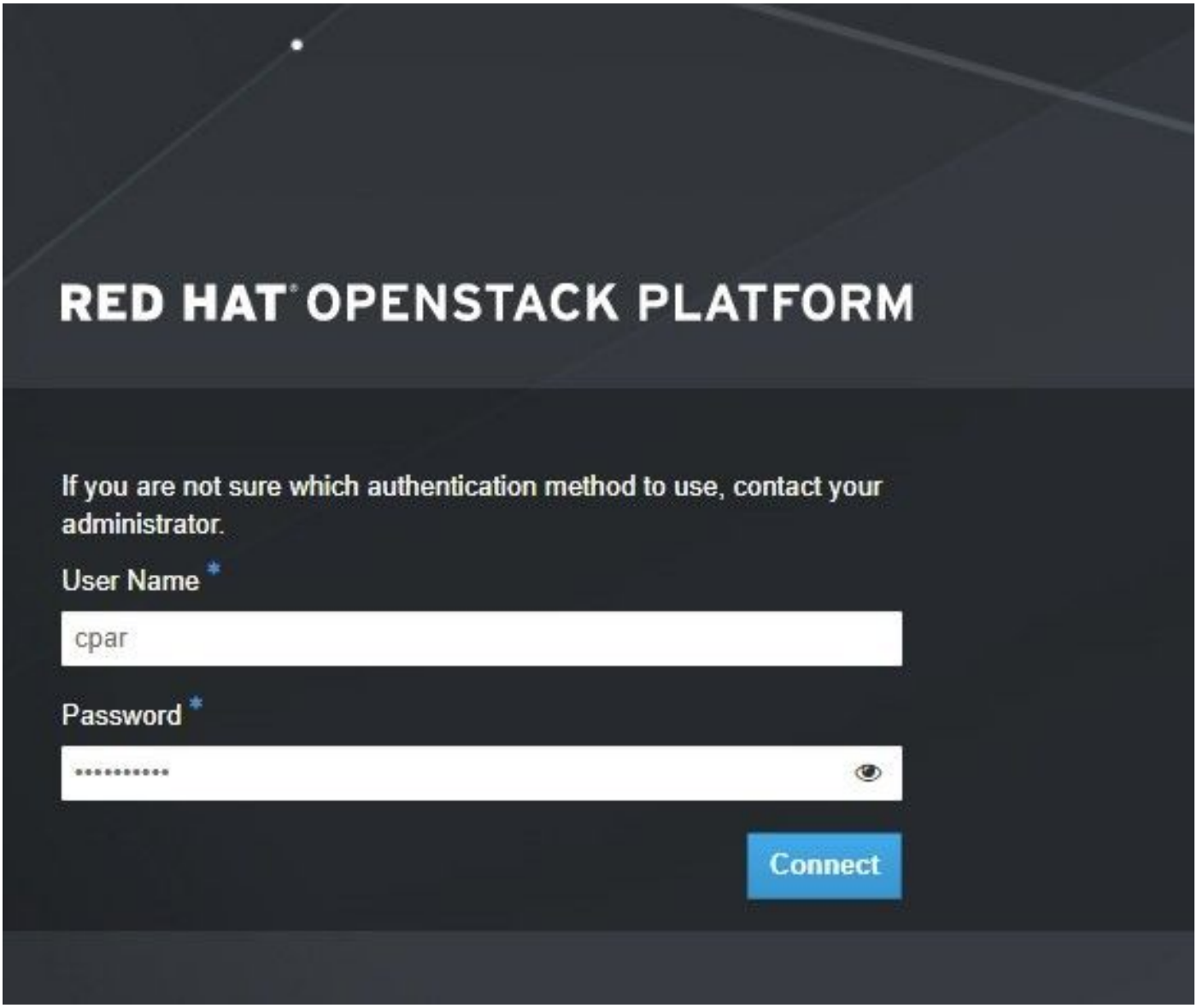
```
Cisco Prime Access Registrar Server Agent not running

Cisco Prime Access Registrar GUI not running
```

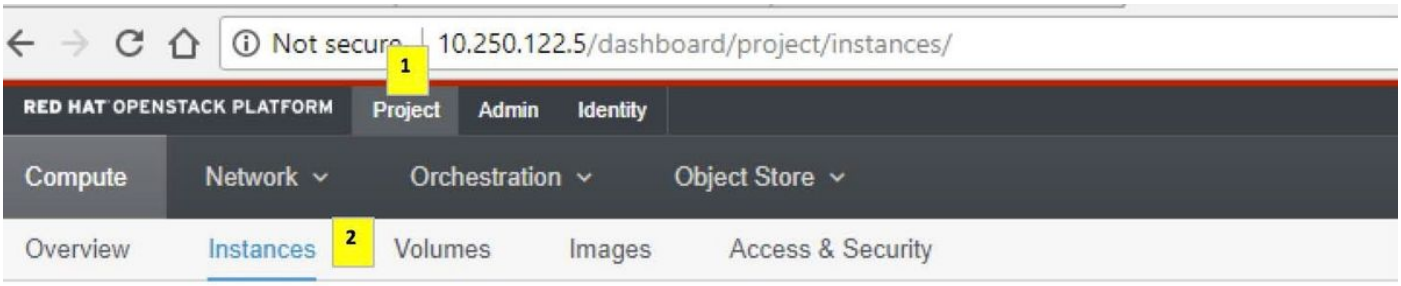
Attività snapshot backup VM

Passaggio 1. Accedere al sito Web dell'interfaccia utente di Horizon corrispondente al Sito (Città) attualmente utilizzato.

Quando si accede a Orizzonte, lo schermo osservato è come mostrato nell'immagine.



Passaggio 2. Passare a **Progetto > Istanze** come mostrato nell'immagine.



Se l'utente utilizzato era CPAR, in questo menu vengono visualizzate solo le 4 istanze AAA.

Passaggio 3. Chiudere una sola istanza alla volta e ripetere l'intero processo descritto in questo documento. Per arrestare la VM, passare a **Azioni > Arresta istanza** come mostrato nell'immagine e confermare la selezione.

Passaggio 4. Per verificare che l'istanza sia effettivamente chiusa, controllare le opzioni Status = **Shutoff** e Power State = **Shut Down**, come mostrato nell'immagine.

Questo passaggio termina il processo di chiusura CPAR.

Snapshot VM

Una volta disattivate le VM CPAR, le istantanee possono essere eseguite in parallelo, in quanto appartengono a computer indipendenti.

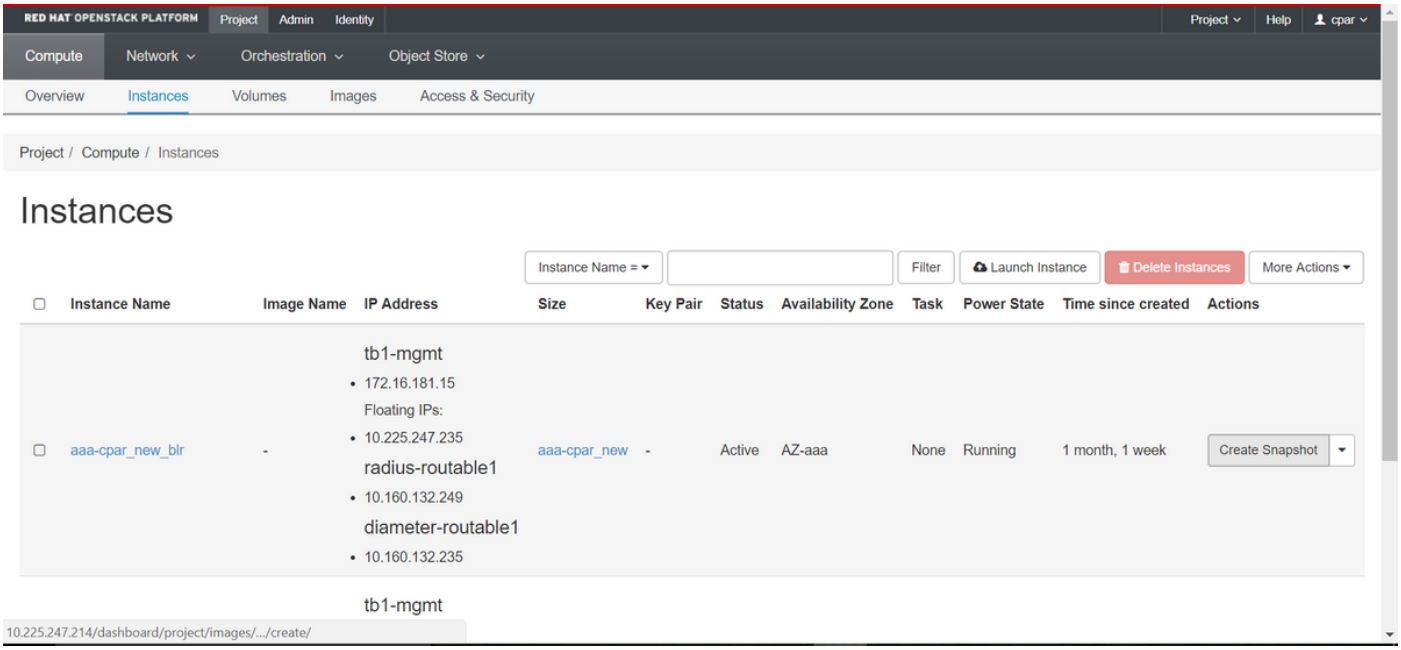
I quattro file QCOW2 vengono creati in parallelo.

Passaggio 1. Eseguire un'istantanea di ciascuna istanza AAA.

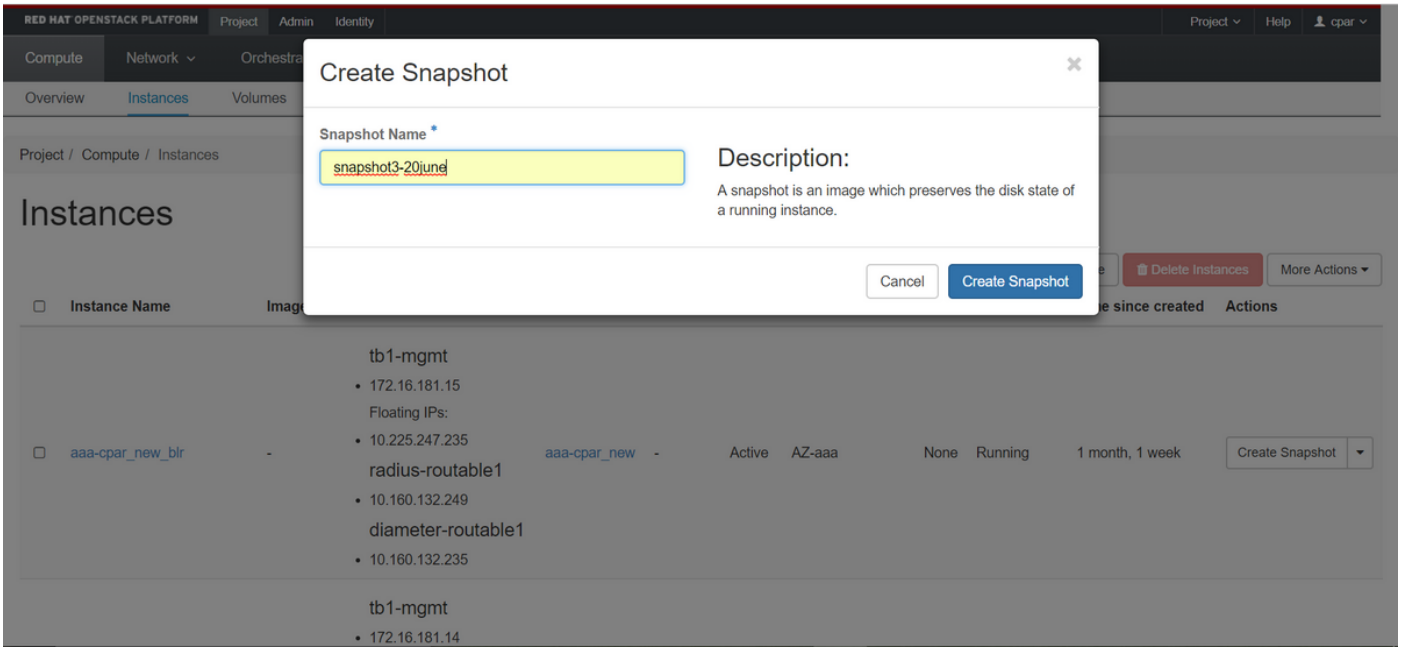
> **Nota:** 25 minuti per le istanze che utilizzano un'immagine QCOW come origine e 1 ora per le istanze che utilizzano un'immagine raw come origine.

Passaggio 2. Accesso alla **GUI** Horizon del POD Openstack.

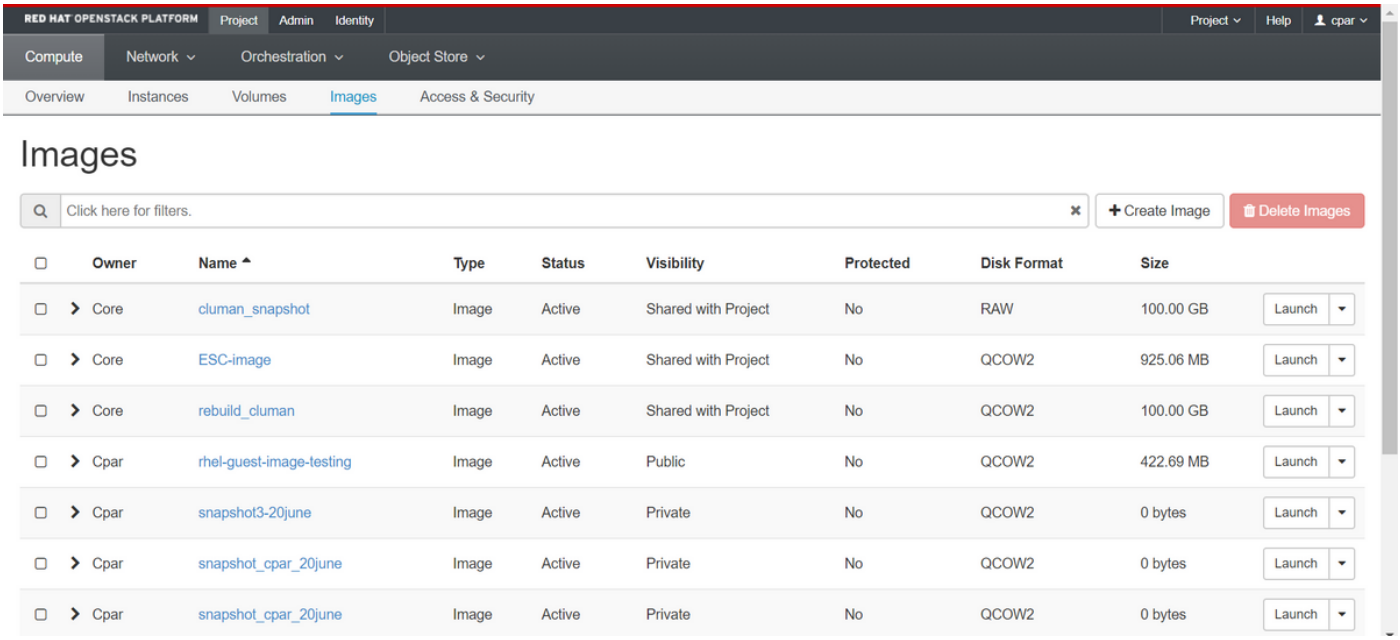
Passaggio 3. Una volta eseguito l'accesso, selezionare **Progetto > Calcola > Istanze** dal menu superiore e cercare le istanze AAA come mostrato nell'immagine.



Passaggio 3. Fare clic su **Crea snapshot** per procedere con la creazione dello snapshot come mostrato nell'immagine. Questa operazione deve essere eseguita sull'istanza AAA corrispondente.



Passaggio 4. Una volta eseguita l'istantanea, passare al menu **Immagini** e verificare che tutte le operazioni siano completate e che non vi siano problemi, come mostrato nell'immagine.



Passaggio 5. Il passaggio successivo consiste nel scaricare la copia istantanea in formato QCOW2 e trasferirla in un'entità remota, nel caso in cui l'OSPD venga perso in questo processo. A tale scopo, identificare la copia istantanea eseguendo il comando **glance image-list** a livello OSPD, come mostrato nell'immagine.

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

Passaggio 6. Dopo aver identificato lo snapshot da scaricare (in questo caso, quello contrassegnato in verde), è possibile scaricarlo in formato QCOW2 con il comando **glance image-download** come mostrato di seguito:

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

Il **&**processo viene inviato in background. Il completamento dell'azione richiede del tempo. Al termine, l'immagine può essere posizionata nella directory **/tmp**.

- Quando si invia il processo in background e la connettività viene interrotta, anche il processo viene interrotto.
- Eseguire il comando **diswn -h** in modo che, in caso di perdita della connessione SSH, il processo continui a essere in esecuzione e venga completato sull'host OSPD.

Passaggio 7. Al termine del processo di download, è necessario eseguire un processo di compressione poiché lo snapshot può essere riempito con ZEROES a causa di processi, task e file temporanei gestiti dal sistema operativo. Il comando da eseguire per la compressione dei file è

virtualizzato.

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

Questo processo può richiedere del tempo (circa 10-15 minuti). Al termine, il file risultante sarà quello da trasferire a un'entità esterna come specificato nel passaggio successivo.

Per ottenere questo risultato, è necessario verificare l'integrità del file, eseguire il comando successivo e cercare l'attributo "corrupt" alla fine dell'output.

```
[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
```

Passaggio 8. Per evitare un problema di perdita dell'OSPD, è necessario trasferire lo snapshot creato di recente nel formato QCOW2 a un'entità esterna. Prima di avviare il trasferimento di file, è necessario verificare se la destinazione dispone di spazio su disco sufficiente, eseguire il comando **df -kh** per verificare lo spazio di memoria.

Si consiglia di trasferirla temporaneamente nell'OSPD di un altro sito utilizzando SFTP **sftp** root@x.x.x.xdove **x.x.x.x** è l'IP di un OSPD remoto.

Passaggio 9. Per velocizzare il trasferimento, la destinazione può essere inviata a più OSPD. Allo stesso modo, è possibile eseguire il comando **scp *name_of_the_file*.qws2 root@ x.x.x.x:/tmp** (dove **x.x.x.x** è l'indirizzo IP di un OSPD remoto) per trasferire il file in un altro OSPD.

Ripristina istanza con snapshot

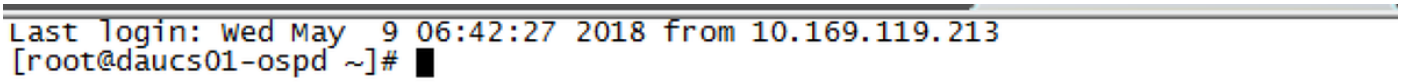
Processo di ripristino

Èpossibile ridistribuire l'istanza precedente con l'istantanea eseguita nei passaggi precedenti.

Passaggio 1. [FACOLTATIVO] Se non sono disponibili snapshot della macchina virtuale precedenti, connettersi al nodo OSPD in cui è stato inviato il backup e reindirizzare il backup al

nodo OSPD originale. Utilizzare **sftp** root@x.x.x.x, dove **x.x.x.x** è l'indirizzo IP dell'OSPD originale. Salvare il file snapshot nella directory **/tmp**.

Passaggio 2. Connettersi al nodo OSPD in cui l'istanza viene ridistribuita come mostrato nell'immagine.

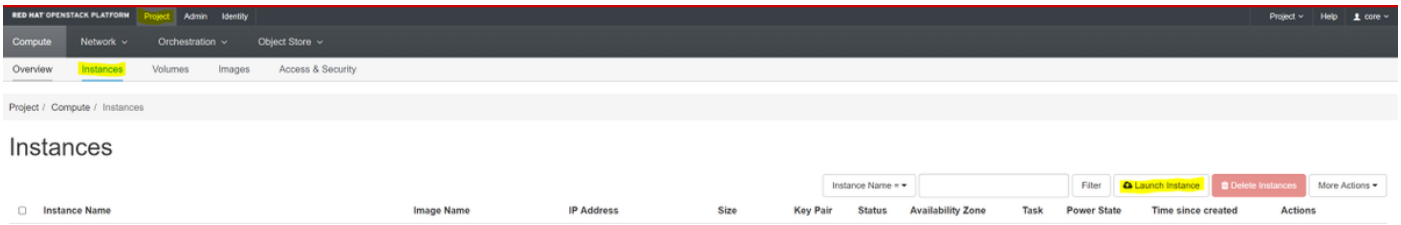


Passaggio 3. Per utilizzare l'istantanea come immagine, è necessario caricarla in Horizon come tale. A tale scopo, utilizzare il comando successivo.

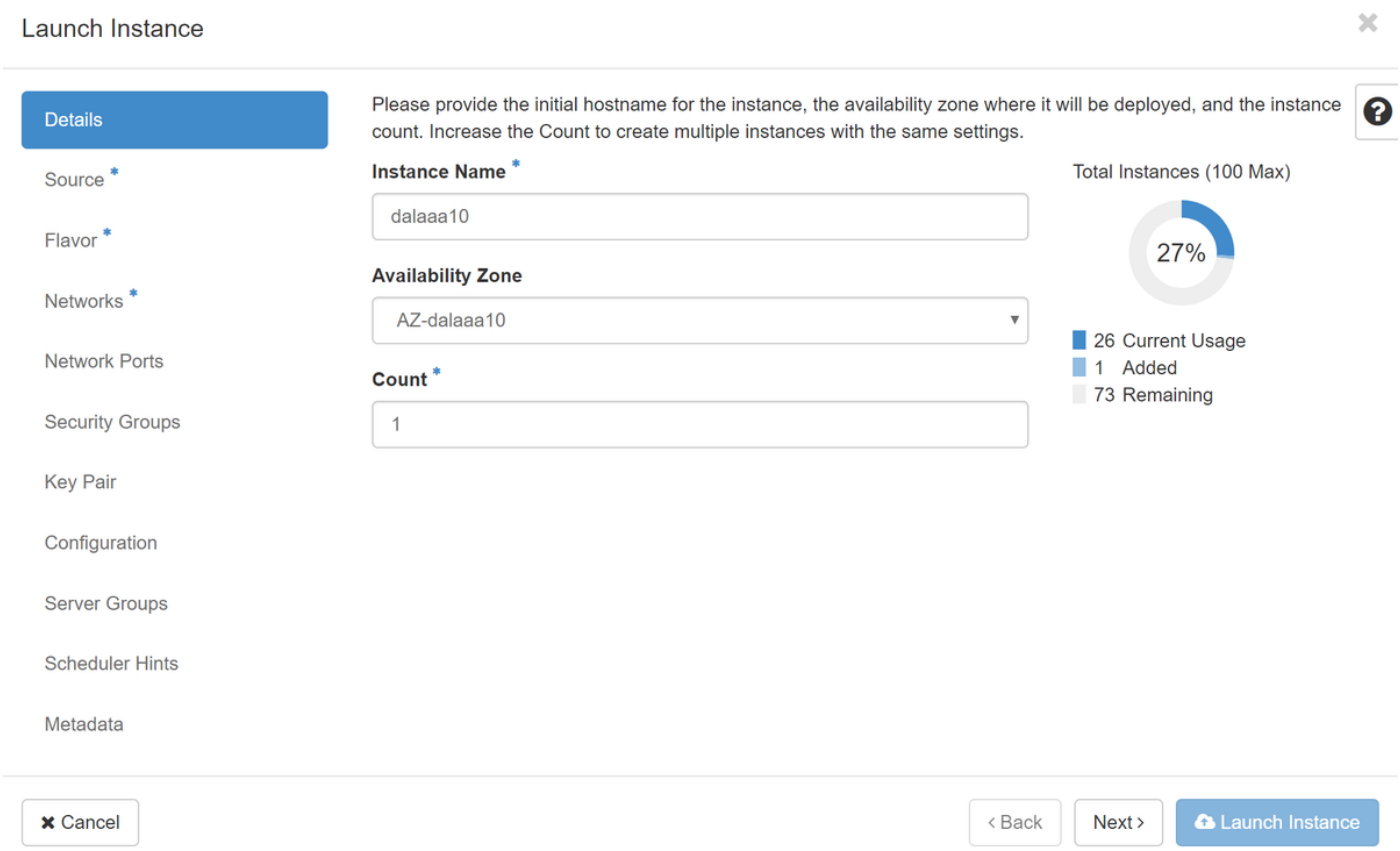
```
#glance image-create -- AAA-CPAR-Date-snapshot.qcow2 --container-format bare --disk-format qcow2 --name AAA-CPAR-Date-snapshot
```

Il processo può essere visto in orizzontale e come mostrato nell'immagine.

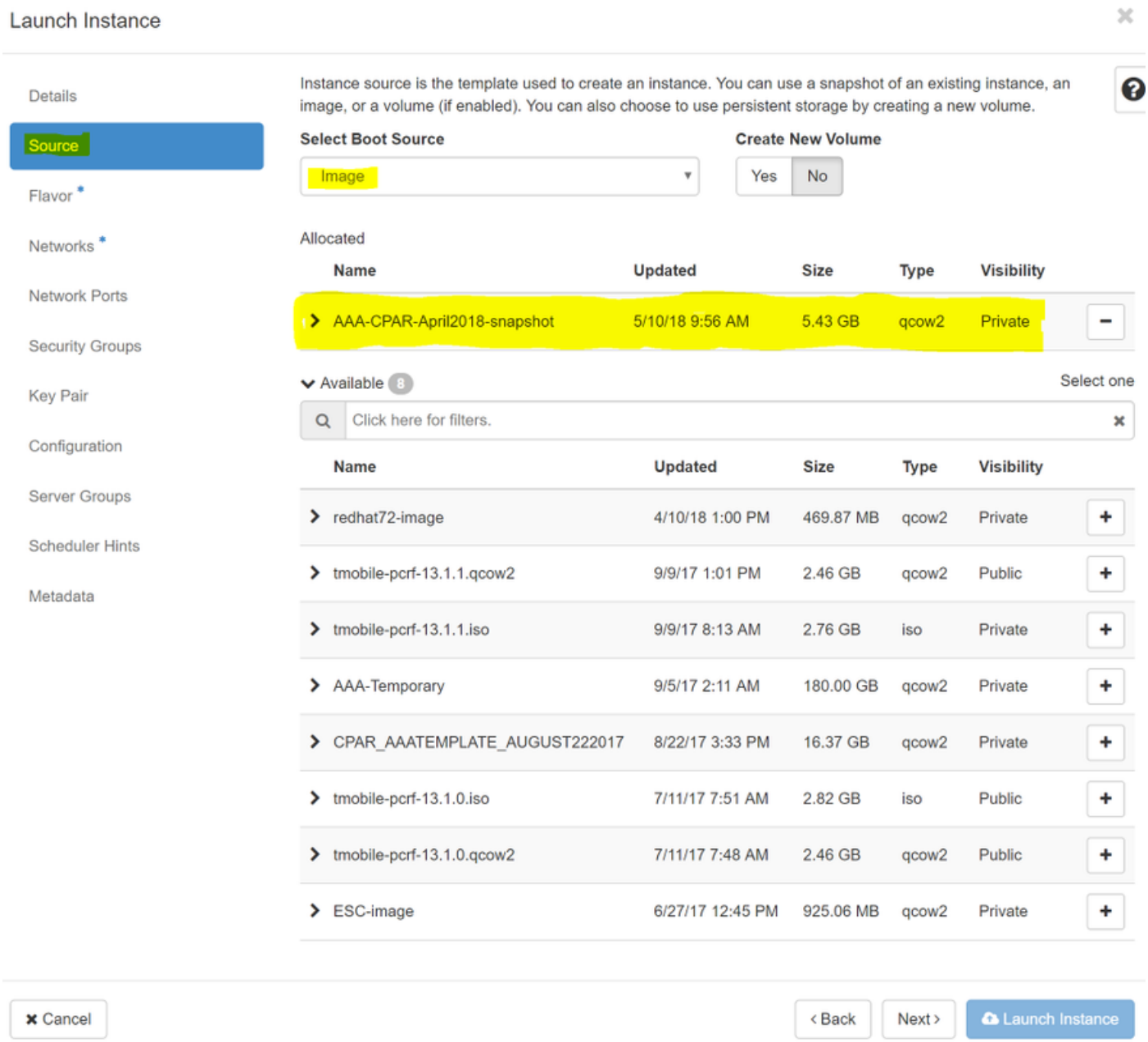
Passaggio 4. In Orizzonte, selezionare **Progetto > Istanze** e fare clic su **Avvia istanza**, come mostrato nell'immagine.



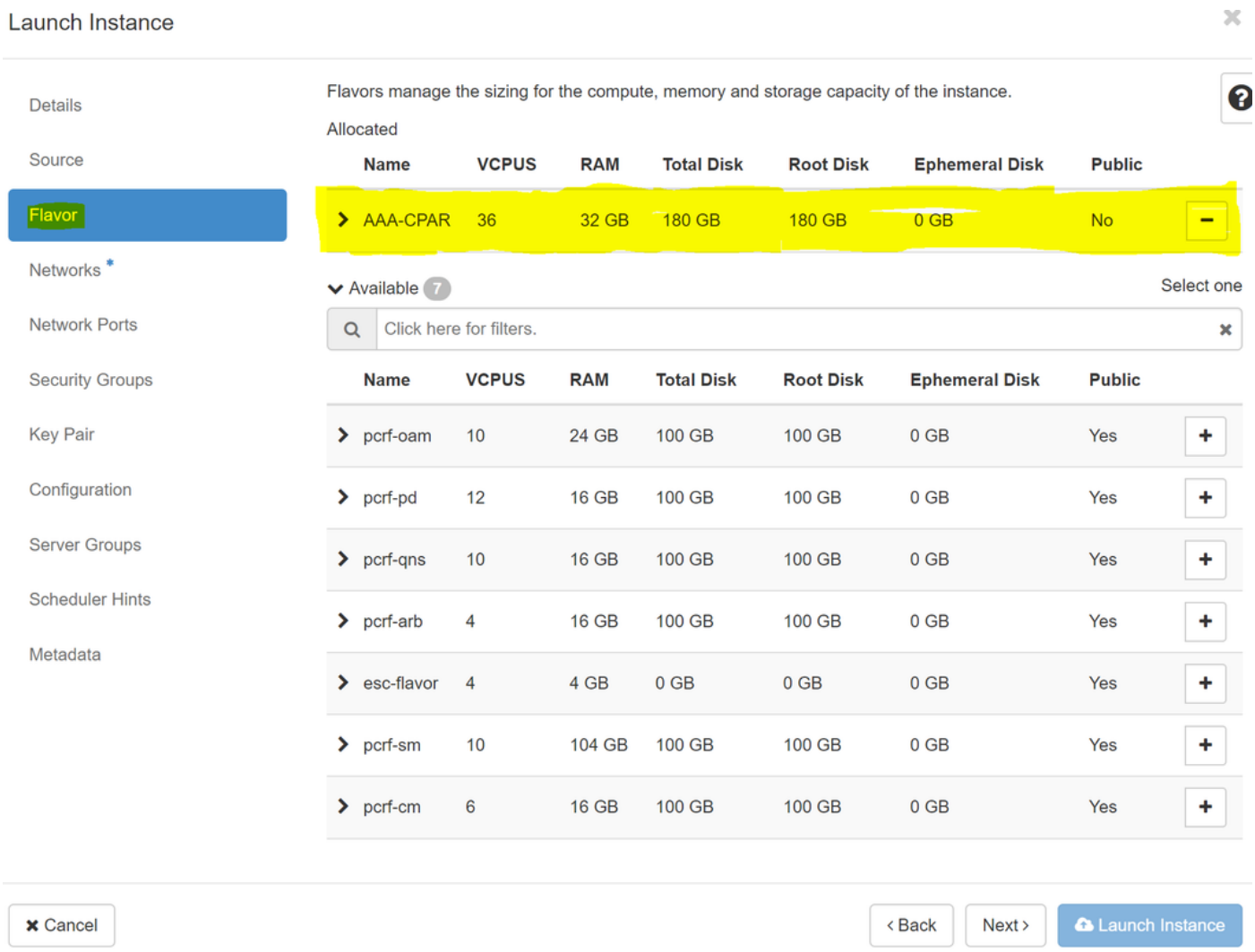
Passaggio 5. Inserire il **nome** dell'**istanza** e scegliere la **zona di disponibilità** come mostrato nell'immagine.



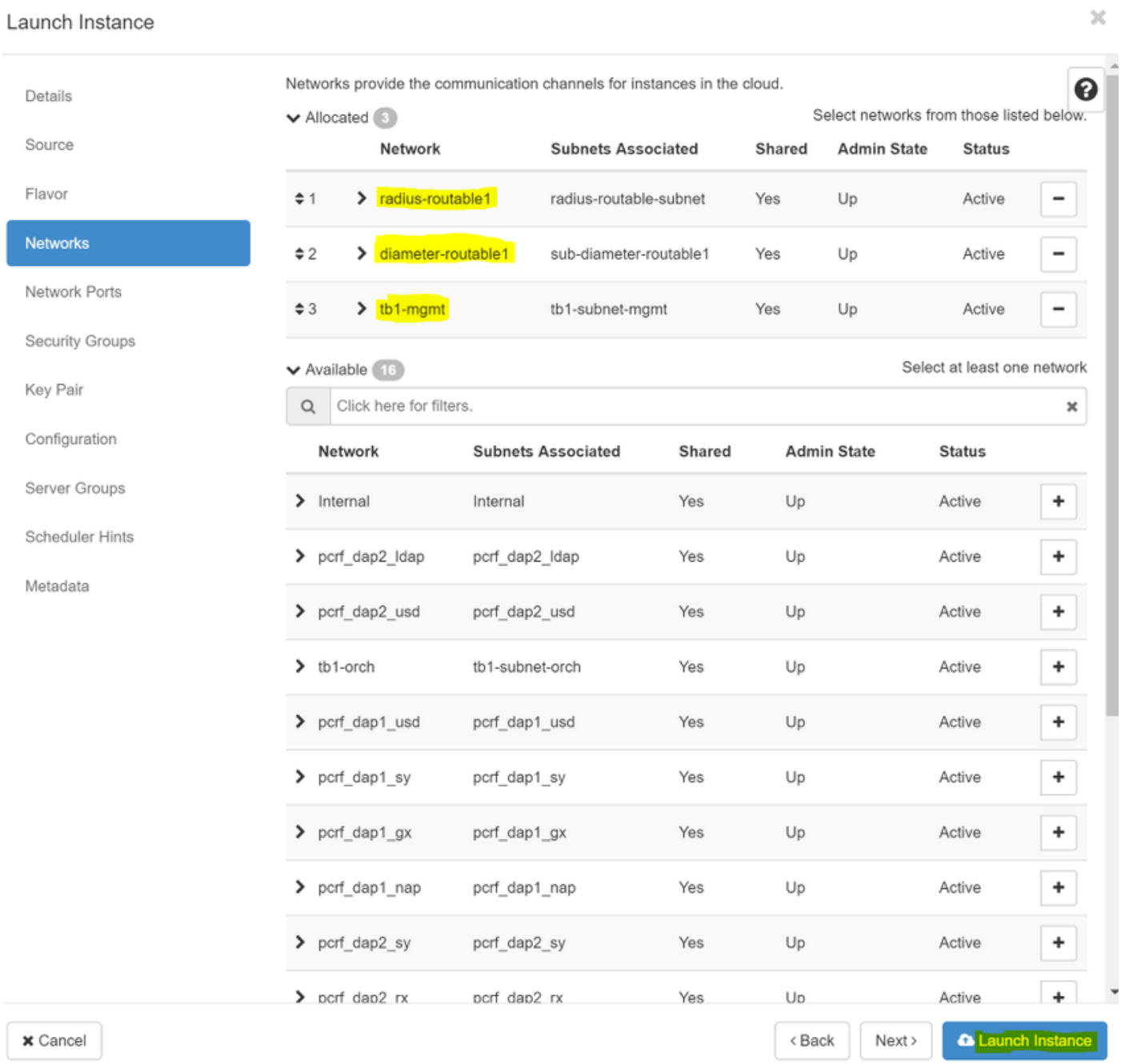
Passaggio 6. Nella scheda Origine, scegliere l'immagine per creare l'istanza. Nel menu Select Boot Source (Seleziona origine di avvio), selezionare **image** (Immagine). Di seguito è riportato un elenco di immagini. Scegliere quella caricata in precedenza facendo clic sul segno **+** come mostrato nell'immagine.



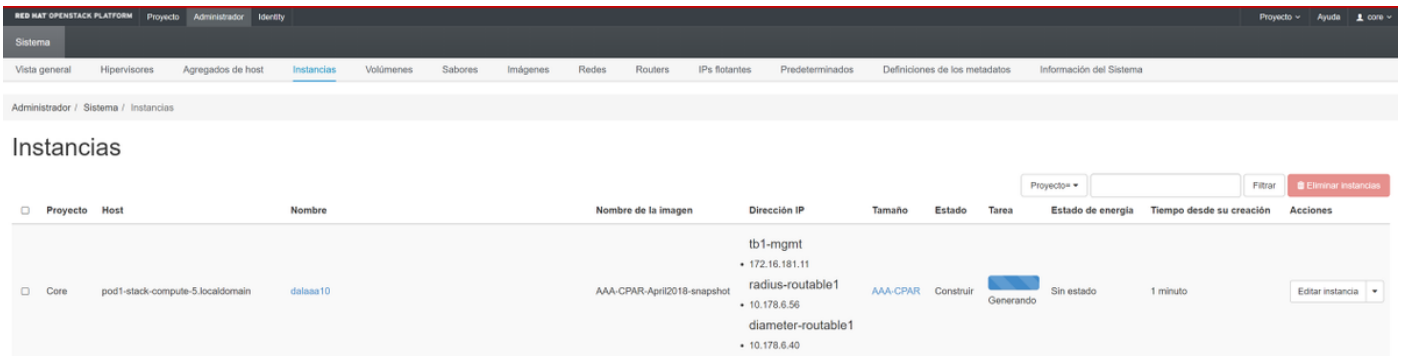
Passaggio 7. Nella scheda Gusto, scegliere il sapore AAA facendo clic sul segno **+** come mostrato nell'immagine.



Passaggio 8. Infine, passare alla scheda **Reti** e scegliere le reti necessarie per l'istanza facendo clic sul segno **+**. In questo caso, selezionare **diametralmente-definibile1**, **radius-routable1** e **tb1-mgmt**, come mostrato nell'immagine.



Passaggio 9. Per creare un'istanza, fare clic su **Avvia istanza**. L'avanzamento può essere monitorato in Orizzonte come mostrato nell'immagine.



Passaggio 10. Dopo alcuni minuti, l'istanza è completamente distribuita e pronta per l'uso, come mostrato nell'immagine.

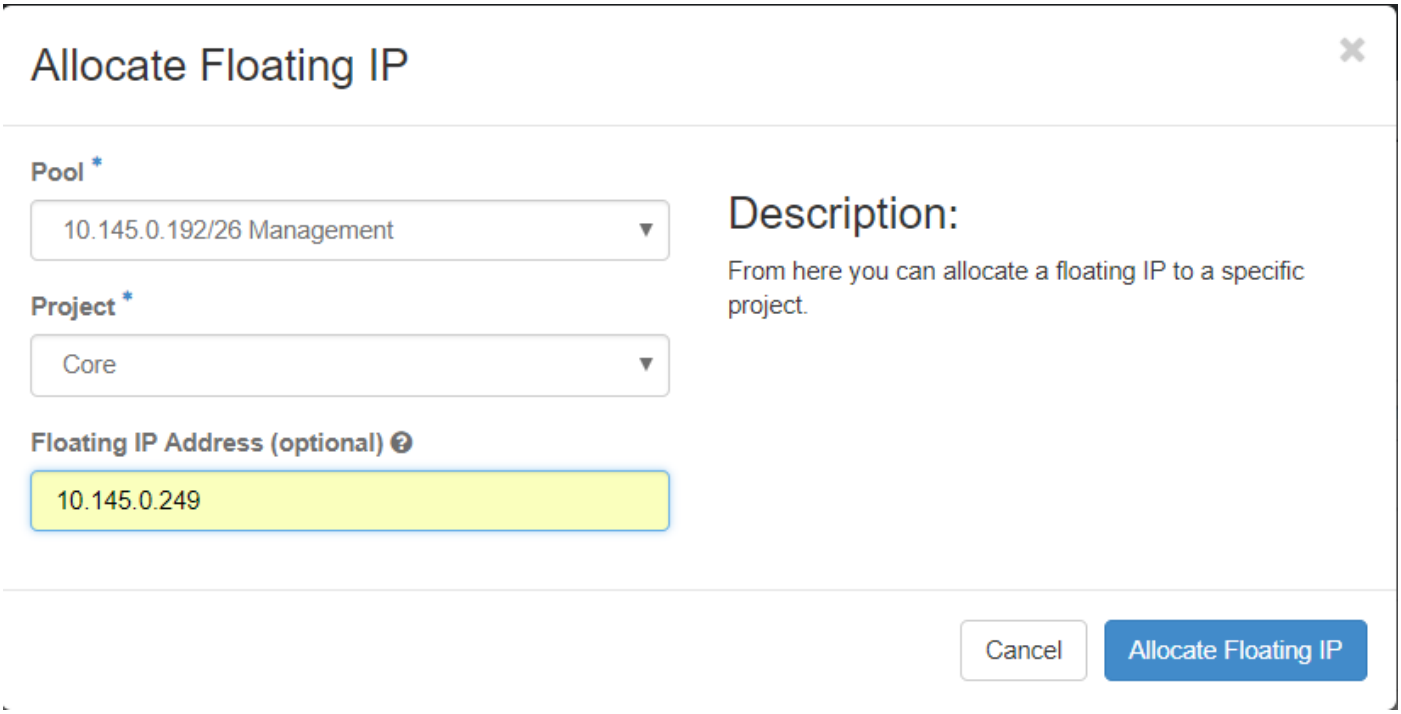
Crea e assegna indirizzo IP mobile

Un indirizzo IP mobile è un indirizzo instradabile, ossia è raggiungibile dall'esterno dell'architettura Ultra M/Openstack e può comunicare con altri nodi dalla rete.

Passaggio 1. Nel menu in alto Orizzonte, selezionare **Admin > Floating IPs** (Amministratore > IP mobili).

Passaggio 2. Fare clic su **Alloca IP al progetto**.

Passaggio 3. Nella finestra **Alloca IP mobile**, selezionare il **pool** dal quale appartiene il nuovo IP mobile, il **progetto** al quale verrà assegnato e lo **stesso indirizzo IP mobile**, come mostrato nell'immagine.

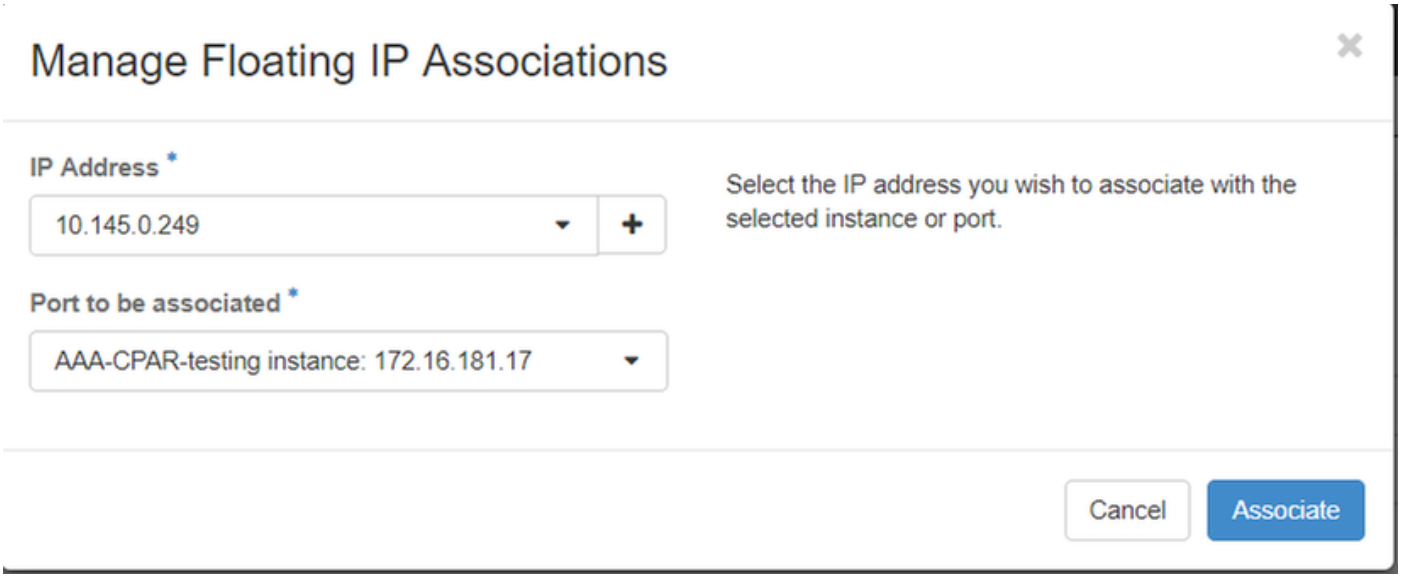


Passaggio 4. Fare clic su **Alloca IP mobile**.

Passaggio 5. Nel menu in alto Orizzonte, passare a **Progetto > Istanze**.

Passaggio 6. Nella colonna **Azione**, fare clic sulla freccia rivolta verso il basso nel pulsante **Crea snapshot** per visualizzare un menu. Fare clic sull'opzione **Associa IP mobile**.

Passaggio 7. Selezionare l'indirizzo IP mobile corrispondente da utilizzare nel campo **IP Address** (Indirizzo IP), quindi selezionare l'interfaccia di gestione corrispondente (eth0) dalla nuova istanza a cui verrà assegnato l'indirizzo IP mobile nella **porta da associare**, come mostrato nell'immagine.



Passaggio 8. Fare clic su **Associa**.

Abilitazione SSH

Passaggio 1. Nel menu in alto Orizzonte, passare a **Progetto > Istanze**.

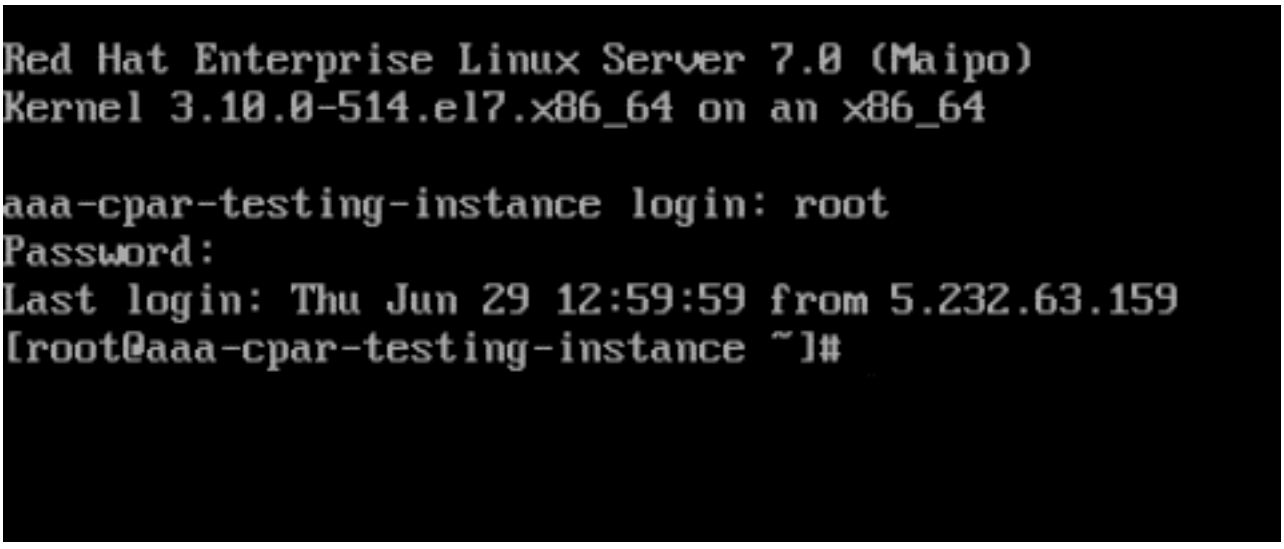
Passaggio 2. Fare clic sul nome dell'istanza o della macchina virtuale creata nella sezione **Avviare una nuova istanza**.

Passaggio 3. Fare clic su **Console**. Viene visualizzata la CLI della VM.

Passaggio 4. Una volta visualizzata la CLI, immettere le credenziali di accesso appropriate, come mostrato nell'immagine:

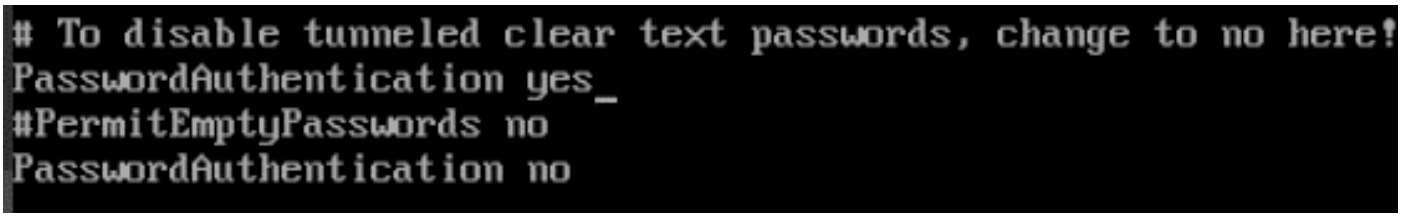
Username: **radice**

Password: **<cisco123>**



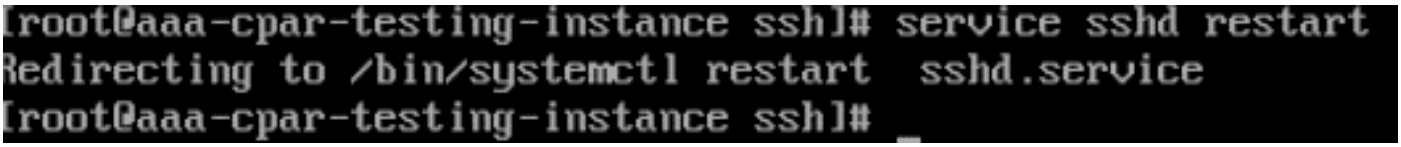
Passaggio 5. Nella CLI, eseguire il comando **vi /etc/ssh/sshd_config** per modificare la configurazione SSH.

Passaggio 6. Una volta aperto il file di configurazione SSH, premere **I** per modificare il file. Modificare quindi la prima riga da **PasswordAuthentication no** a **PasswordAuthentication yes** , come mostrato nell'immagine.

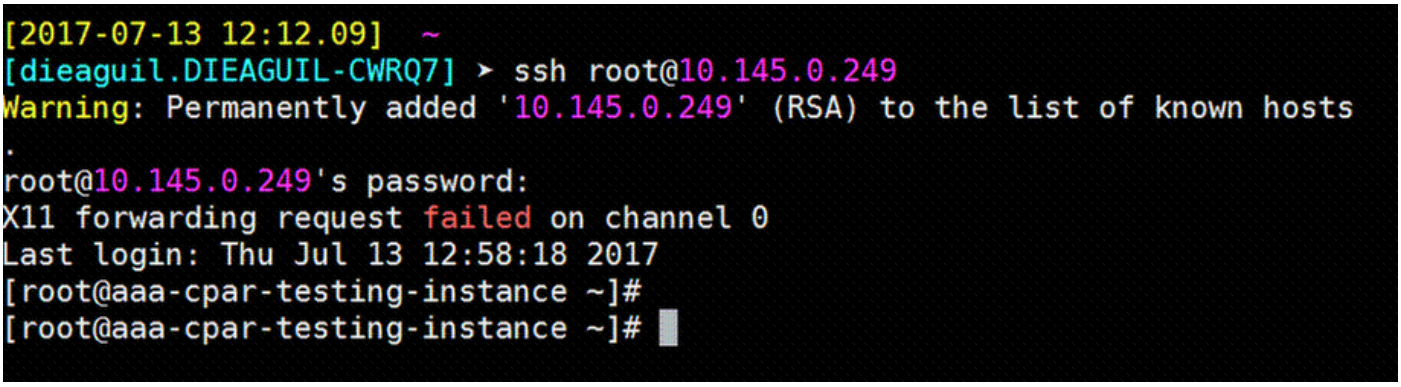


Passaggio 7. Premere **ESC** e immettere **:wq!** per salvare le modifiche al file **sshd_config**.

Passaggio 8. Eseguire il comando **service sshd restart** come mostrato nell'immagine.

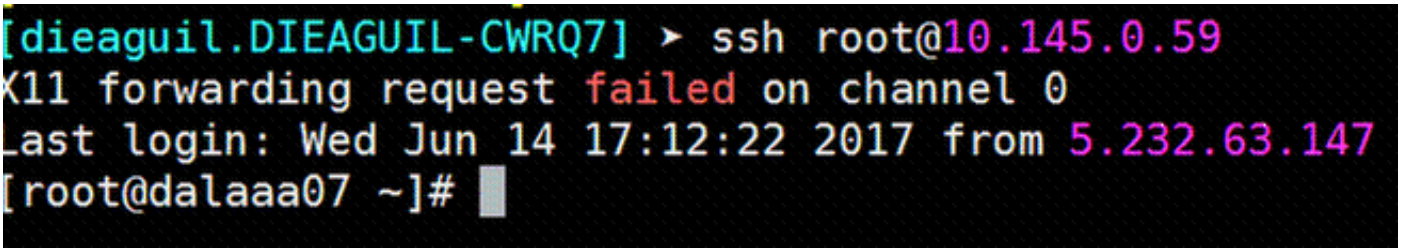


Passaggio 9. Per verificare la corretta applicazione delle modifiche alla configurazione SSH, aprire un client SSH e provare a stabilire una connessione remota sicura con l'IP mobile assegnato all'istanza (ad esempio **10.145.0.249**) e la **radice** dell'utente, come mostrato nell'immagine.



Definizione sessione SSH

Passaggio 1. Aprire una sessione SSH con l'indirizzo IP della macchina virtuale/server corrispondente in cui è installata l'applicazione, come mostrato nell'immagine.



Avvio istanza CPAR

Seguire questi passaggi una volta che l'attività è stata completata e i servizi CPAR possono essere ristabiliti nel Sito che è stato chiuso.

Passaggio 1. Accedere nuovamente a Orizzonte, selezionare **progetto > istanza > avvia istanza**.

Passaggio 2. Verificare che lo stato dell'istanza sia **Attivo** e che lo stato di alimentazione sia **In esecuzione**, come mostrato nell'immagine.

Controllo dello stato post-attività

Passaggio 1. Eseguire il comando **/opt/CSCOar/bin/arstatus** a livello di sistema operativo:

```
[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 ~]#
```

Passaggio 2. Eseguire il comando **/opt/CSCOar/bin/aregcmd** a livello di sistema operativo e immettere le credenziali dell'amministratore. Verificare che CPAR Health sia 10 su 10 e che l'uscita da CPAR CLI sia corretta.

```
[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
```

Passaggio 3. Eseguire il comando **netstat | diametro grep** e verificare che tutte le connessioni DRA siano stabilite.

L'output qui menzionato è relativo a un ambiente in cui sono previsti collegamenti con diametro. Se vengono visualizzati meno collegamenti, si tratta di una disconnessione da DRA che deve essere analizzata.

```
[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
```

Passaggio 4. Verificare che nel log di TelePresence Server (TPS) siano visualizzate le richieste elaborate da CPAR. I valori evidenziati rappresentano i TPS e quelli a cui è necessario prestare attenzione.

Il valore di TPS non deve superare 1500.

```
[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
```

Passaggio 5. Cercare eventuali messaggi "error" o "alarm" in name_radius_1_log:

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

Passaggio 6. Per verificare la quantità di memoria utilizzata dal processo CPAR, eseguire il comando:

```
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
```

Questo valore evidenziato deve essere inferiore a 7 Gb, ovvero il valore massimo consentito a livello di applicazione.