CPAR VM Snapshot and Recovery

Contents

Introduction

This document describes a step by step procedure on how to backup(snapshot) the Authentication, Authorization, and Accounting (AAA) instances.

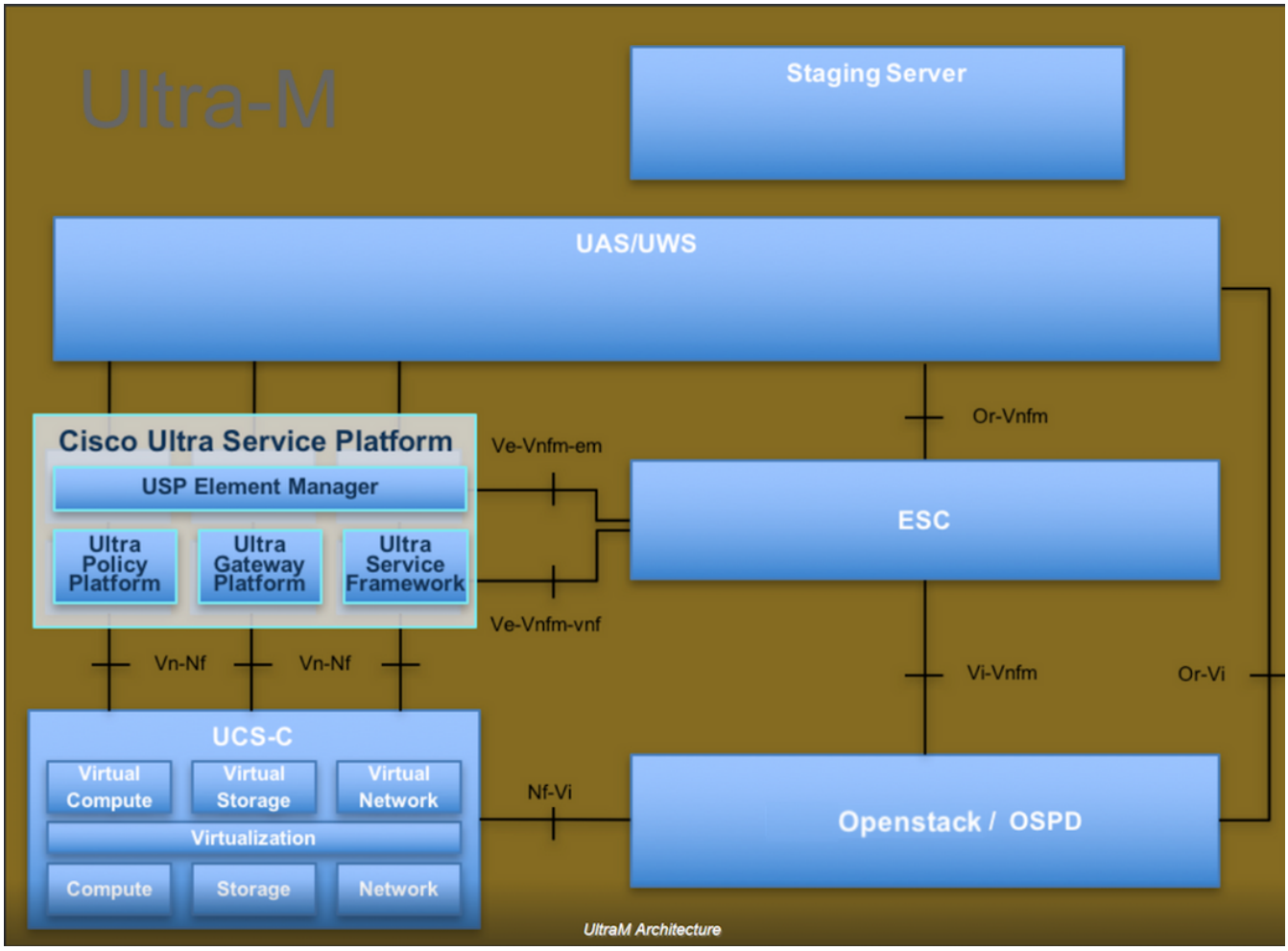
Background Information

It is imperative to execute this per site and one site at a time in order to minimize the impact on the subscriber's traffic.

This procedure applies for an Openstack environment with the use of NEWTON version where Elastic Services Controller (ESC) does not manage Cisco Prime Access Registrar (CPAR) and CPAR is installed directly on the Virtual Machine (VM) deployed on Openstack.

Ultra-M is a pre-packaged and validated virtualized mobile packet core solution that is designed in order to simplify the deployment of Virtual Network Functions (VNFs). OpenStack is the Virtualized Infrastructure Manager (VIM) for Ultra-M and consists of these node types:

- Compute
- Object Storage Disk - Compute (OSD - Compute)
- Controller
- OpenStack Platform - Director (OSPD)
- The high-level architecture of Ultra-M and the components involved are depicted in this image:



This document is intended for Cisco personnel who are familiar with Cisco Ultra-M platform and it details the steps required in order to carry out at OpenStack and Redhat OS.

Note: Ultra M 5.1.x release is considered in order to define the procedures in this document.

Network Impact

In general when the process of CPAR goes down, KPI degradation is expected as when you shut down the application, it takes up to 5 minutes for the diameter peer down trap to be sent. At this time, all the requests routed towards the CPAR will fail. After that time, the links are determined to be down and Diameter Routing Agent (DRA) stops routing traffic towards this node.

Furthermore, for all the existing sessions in the AAA that are shut down, if there is an attach/detach procedure that involves these sessions with another active AAA, that procedure will fail, as the Hosted Security as a Service (HSS) replies that the user is registered on the AAA that is shut down and the procedure won't be able to complete successfully.

STR performance is expected to be under 90% success rate around 10 hours after the activity is completed. After that time, the normal value of 90% must be reached.

Alarms

Simple Network Management Protocol (SNMP) Alarms are generated whenever the CPAR service

is stopped and started, so SNMP traps are expected to be generated throughout the process. Traps expected include:

- CPAR SERVER STOP
- VM DOWN
- NODE DOWN – (Expected alarm that is not directly generated by the CPAR instance)
- DRA

VM Snapshot Backup

CPAR Application Shutdown

> **Note**: Ensure that you have web access to HORIZON for the site in place and access to OSPD.

Step 1. Open any Secure Shell (SSH) client connected to the Transformation Management Office (TMO) Production network and connect to the CPAR instance.

> **Note**: It is important not to shutdown all 4 AAA instances within one site at the same time, do it one at a time.

Step 2. In order to Shut Down CPAR application, run the command:

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

A message "Cisco Prime Access Registrar Server Agent shutdown complete" must show up.

> **Note**: If you leave the CLI session open, the **arserver stop command** won't work and this error message is displayed.

```
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 this example, the highlighted process id 2903 needs to be terminated before CPAR can be stopped. If this is the case, run the command and terminate this process:

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

Then, repeat Step 1.

Step 3. In order to verify that the CPAR application was indeed shutdown, run the command:

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

These messages must appear:

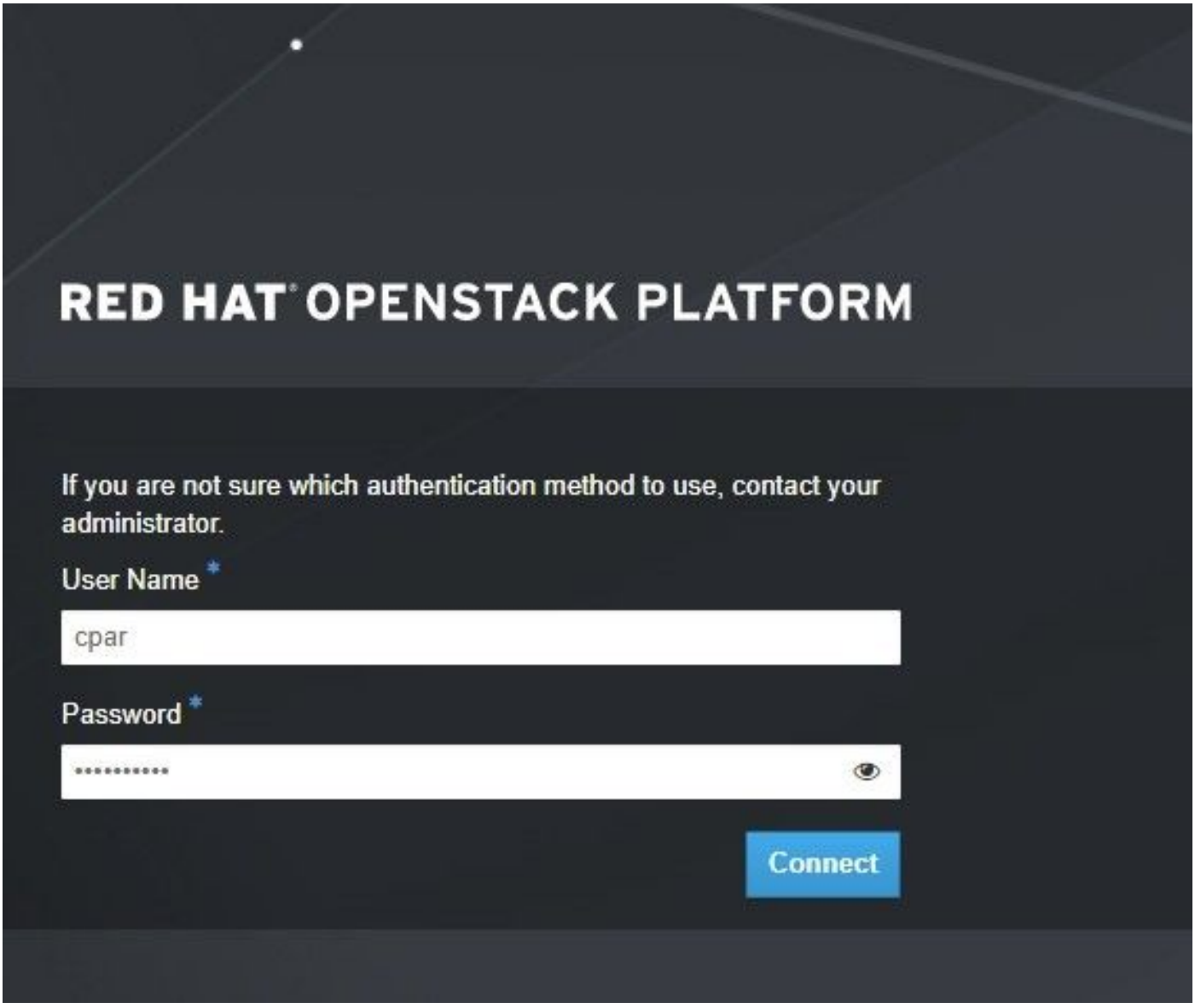
```
Cisco Prime Access Registrar Server Agent not running

Cisco Prime Access Registrar GUI not running
```

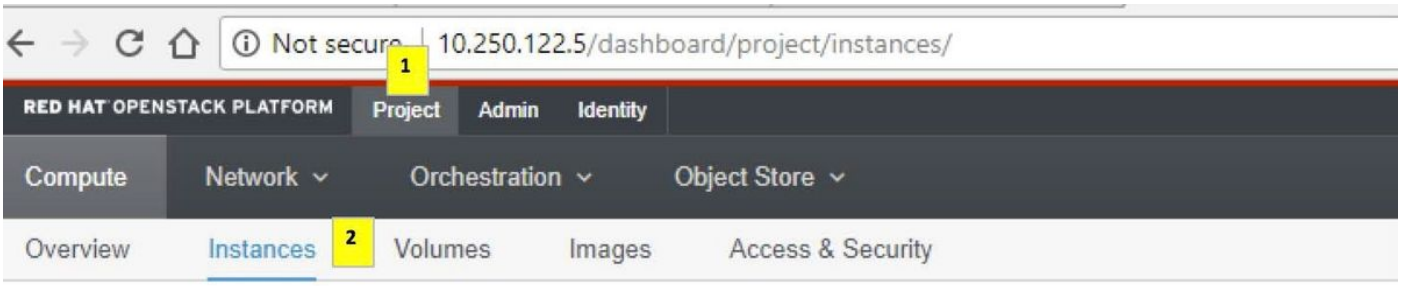
VM Backup Snapshot Task

Step 1. Enter the Horizon GUI website that corresponds to the Site (City) currently worked on.

When you access Horizon, the screen observed is as shown in the image.

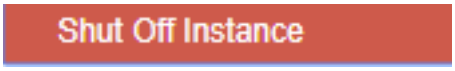


Step 2. Navigate to **Project > Instances** as shown in the image.



If the user used was CPAR, then only the 4 AAA instances appear in this menu.

Step 3. Shut down only one instance at a time, repeat the whole process in this document. In order to shutdown the VM, navigate to **Actions > Shut Off Instance** as shown in the image and confirm your selection..



Step 4. In order to validate that the instance is indeed shut down check the Status = **Shutoff** and Power State = **Shut Down**, as shown in the image.

This step ends the CPAR shutdown process.

VM Snapshot

Once the CPAR VMs are down, the snapshots can be taken in parallel, as they belong to independent computes.

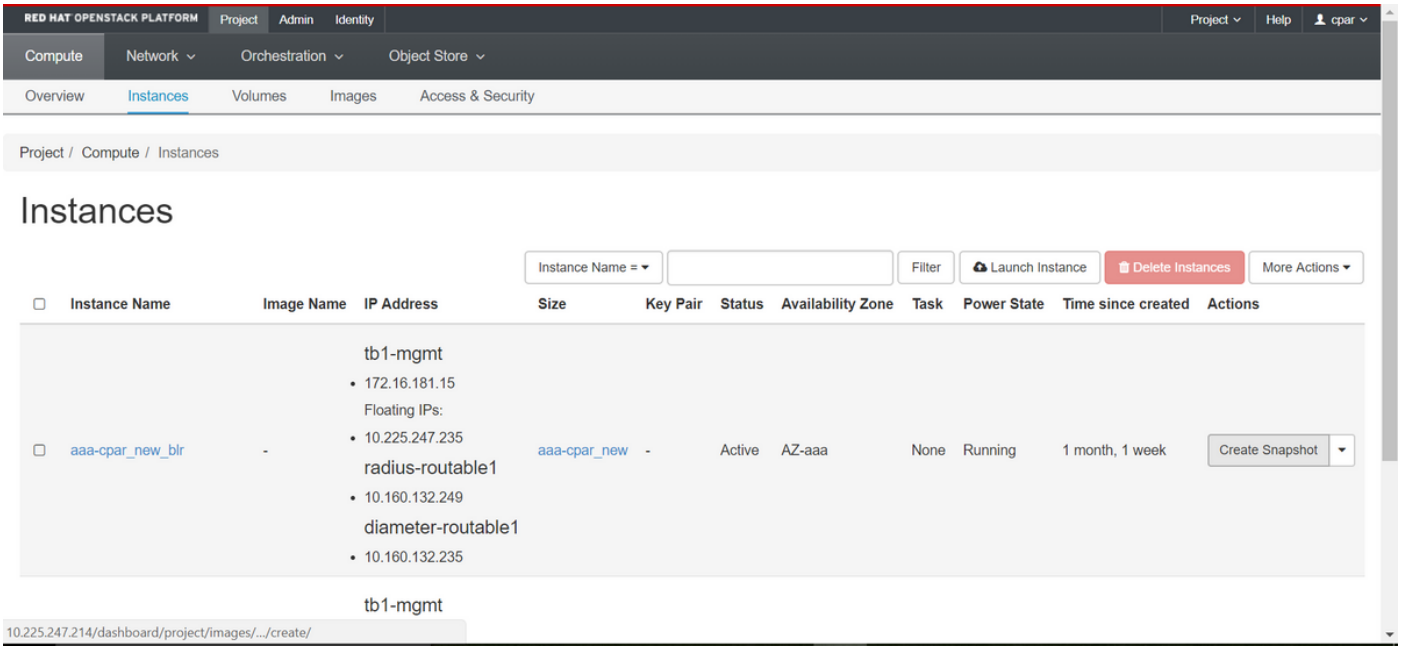
The four QCOW2 files are created in parallel.

Step 1. Take a snapshot of each AAA instance.

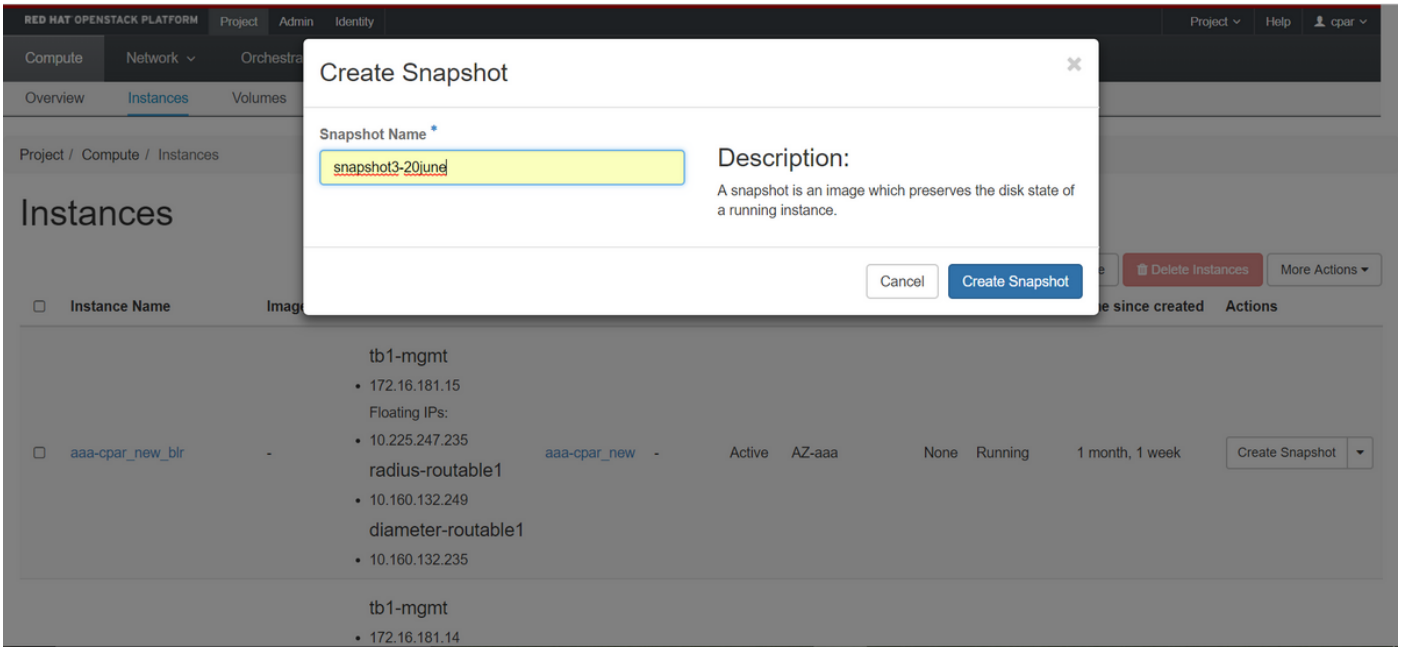
> **Note**: 25 minutes for instances that uses a QCOW image as a source and 1 hour for instances that uses a raw image as a source.

Step 2. Login to POD's Openstack's Horizon **GUI**.

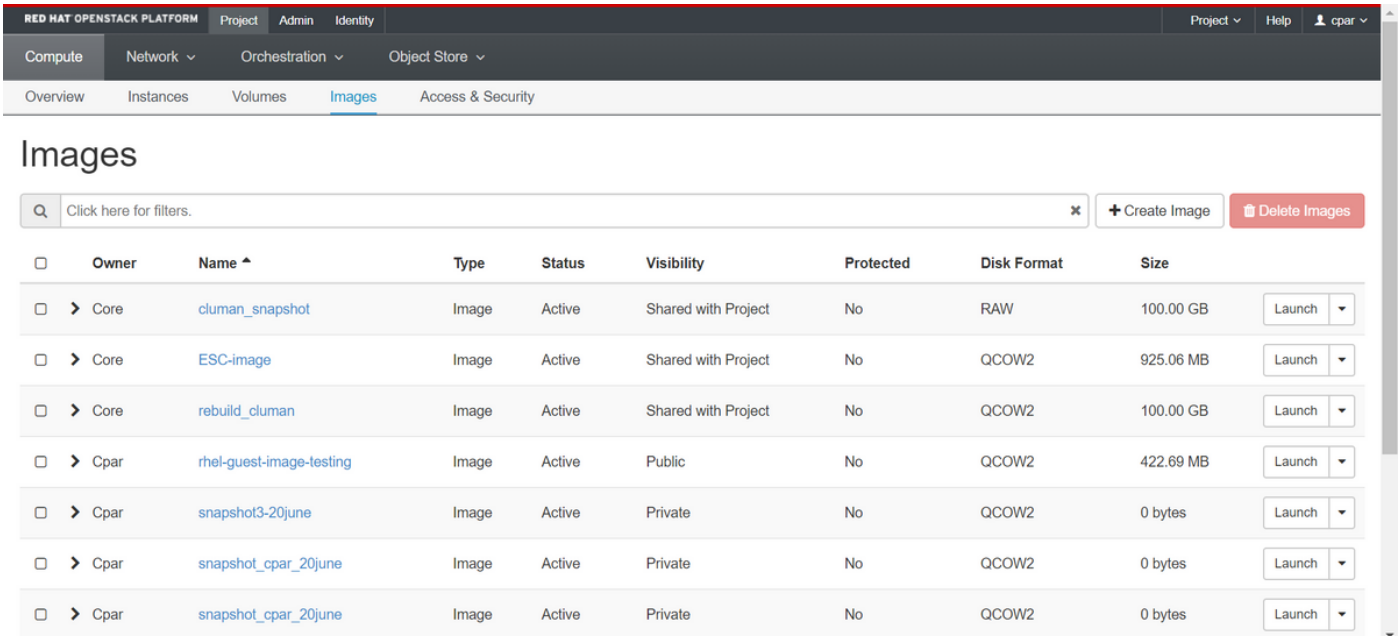
Step 3. Once you log in, navigate to **Project > Compute > Instances** on the top menu and look for the AAA instances as shown in the image.



Step 3. Click **Create Snapshot** in order to proceed with snapshot creation as shown in the image. This needs to be executed on the corresponding AAA instance.



Step 4. Once the snapshot is executed, navigate to **Images** menu and verify that all finish and report no problem as shown in the image.



Step 5. The next step is to download the snapshot on a QCOW2 format and transfer it to a remote entity, in case the OSPD is lost in this process. In order to achieve this, identify the snapshot by running the command **glance image-list** at OSPD level as shown in the 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  |
+--------------------------------------+----------------------------+
```

Step 6. Once you identify the snapshot to be downloaded (in this case, it's the one marked in green), you can download it on a QCOW2 format with the command **glance image-download** as depicted here:

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

The **&** sends the process to background. It takes some time to complete the action. Once it is done, the image can be located at **/tmp** directory.

- When you send the process to the background and if the connectivity is lost, then the process is also stopped.
- Run the command **disown -h** so that in case SSH connection is lost, the process still runs and finishes on the OSPD.

Step 7. Once the download process finishes, a compression process needs to be executed as that snapshot can be filled with ZEROES because of processes, tasks and temporary files handled by the Operating System (OS). The command to run for file compression is **virt-sparsify**.

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

This process can take some time (around 10-15 minutes). Once finished, the file that results is the one that needs to be transferred to an external entity as specified on next step.

Verification of the file integrity is required, in order to achieve this, run the next command and look for the “corrupt” attribute at the end of its 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
```

Step 8. In order to avoid a problem where the OSPD is lost, the recently created snapshot on QCOW2 format needs to be transferred to an external entity. Before you start the file transfer, you have to check if the destination have enough available disk space, run the command **df –kh** in order to verify the memory space.

An advice is to transfer it to another site’s OSPD temporarily with the use of SFTP **sftp root@x.x.x.x**where **x.x.x.x** is the IP of a remote OSPD.

Step 9. In order to speed up the transfer, the destination can be sent to multiple OSPDs. In the same way, you can run the command **scp *name_of_the_file*.qcow2 root@ x.x.x.x:/tmp** (where **x.x.x.x** is the IP of a remote OSPD) in order to transfer the file to another OSPD.

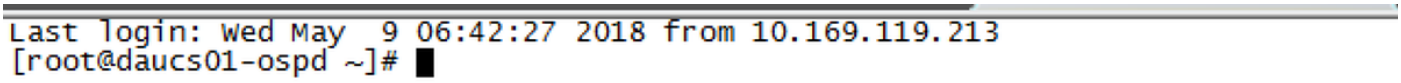
Recover Instance with Snapshot

Recovery Process

It is possible to redeploy the previous instance with the snapshot taken in previous steps.

Step 1. [OPTIONAL] If there is no previous VM snapshot available then connect to the OSPD node where the backup was sent and sftp the backup back to its original OSPD node. Use **sftp root@x.x.x.x**, where **x.x.x.x** is the IP of a the original OSPD. Save the snapshot file in **/tmp** directory.

Step 2. Connect to the OSPD node where the instance re-deploy as shown in the image.

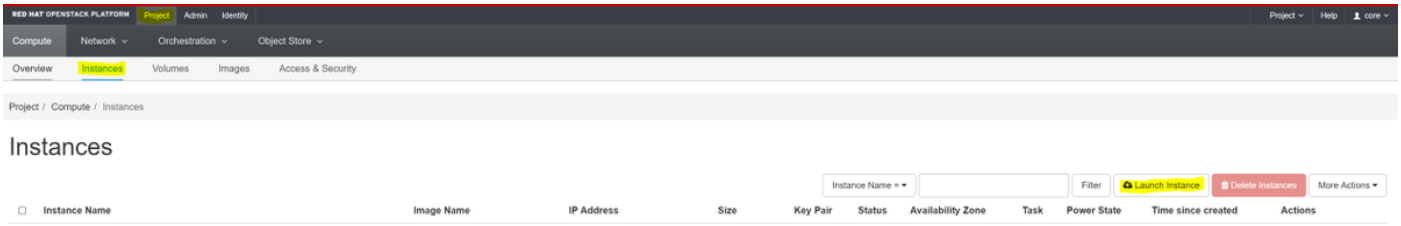


Step 3. In order to use the snapshot as an image it is necessary to upload it to horizon as such. Use the next command to do so.

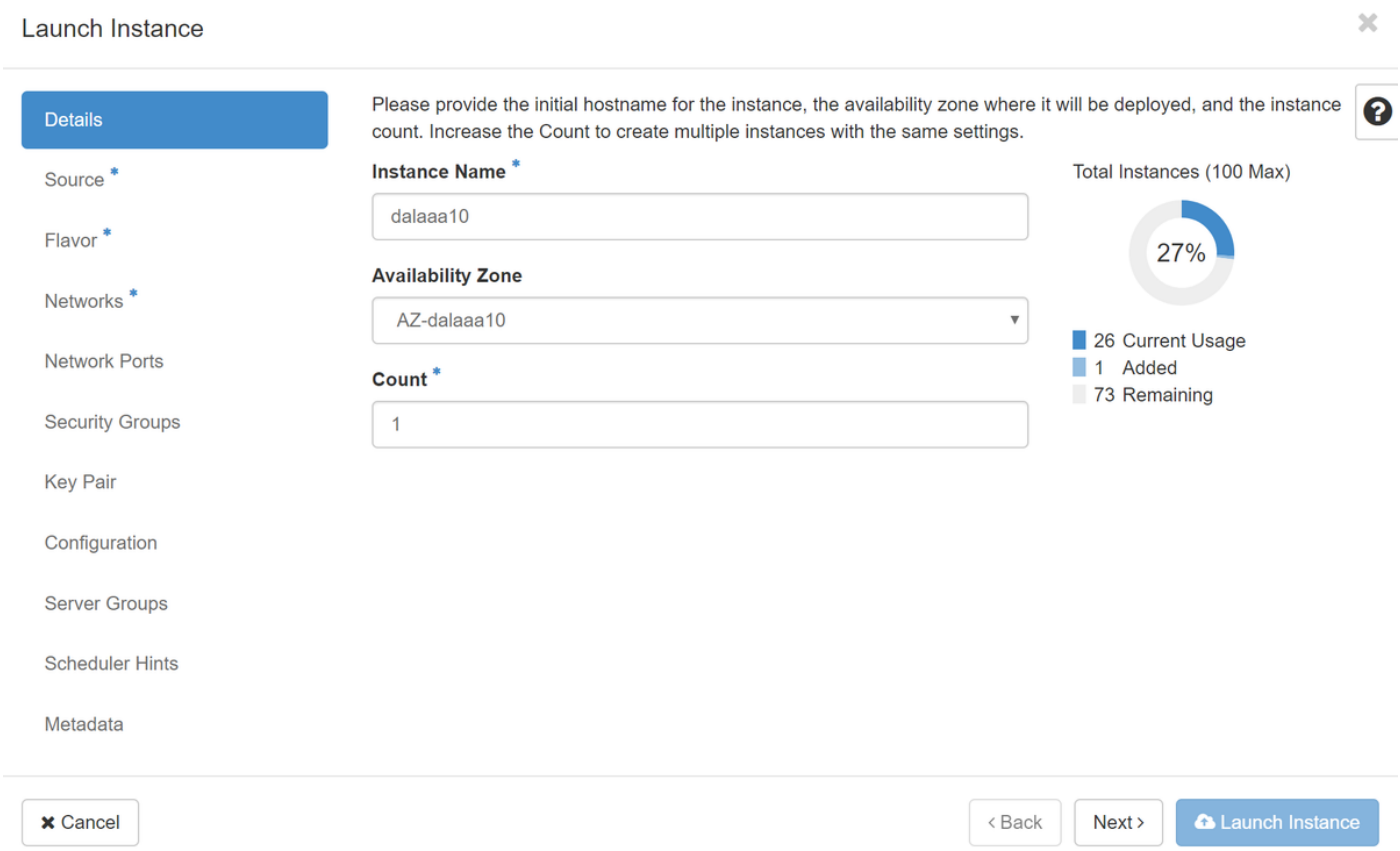
```
#glance image-create -- AAA-CPAR-Date-snapshot.qcow2 --container-format bare --disk-format qcow2 --name AAA-CPAR-Date-snapshot
```

The process can be seen in horizon and as shown in the image.

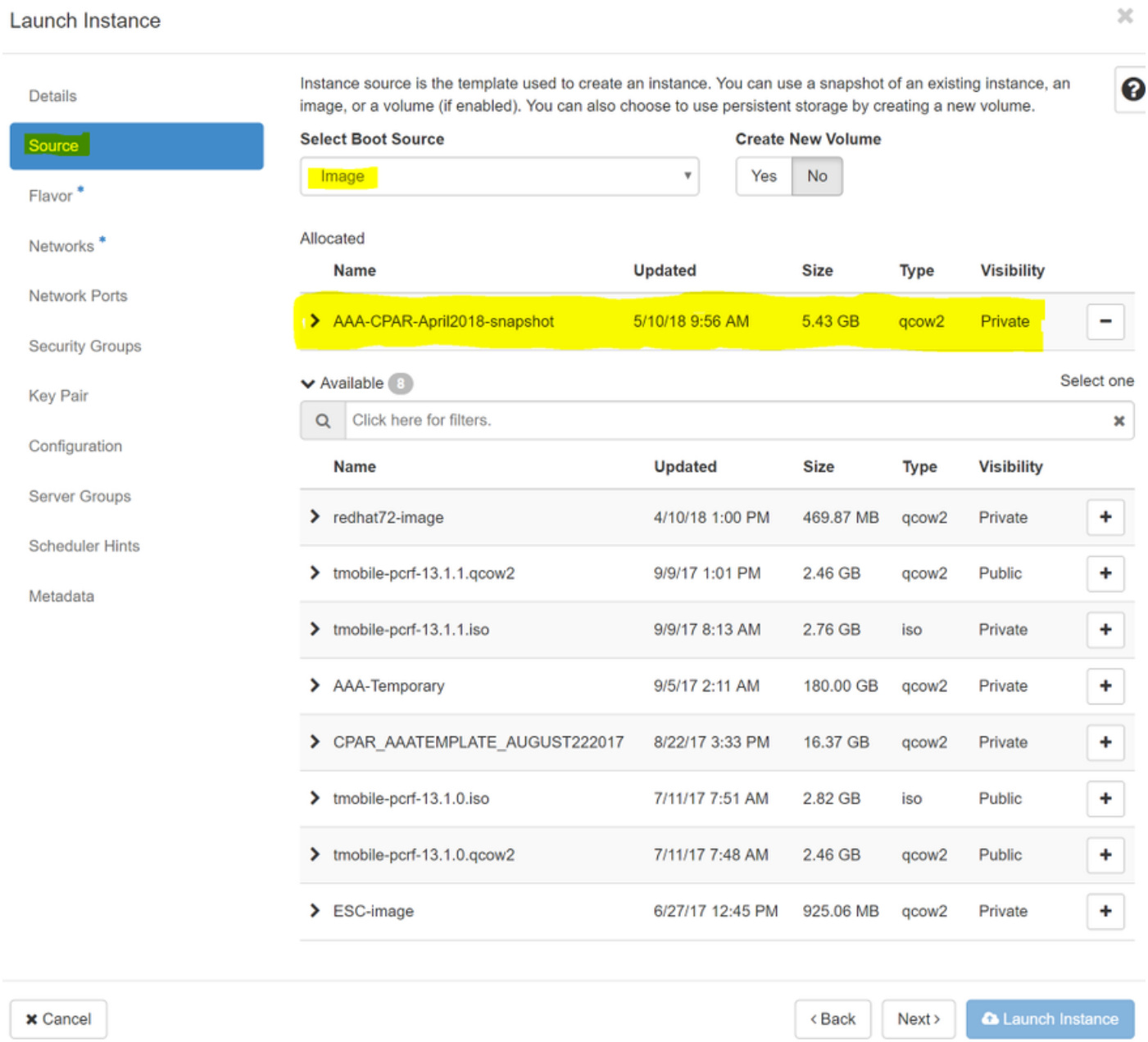
Step 4. In Horizon, navigate to **Project > Instances** and click **Launch Instance** as shown in the image.



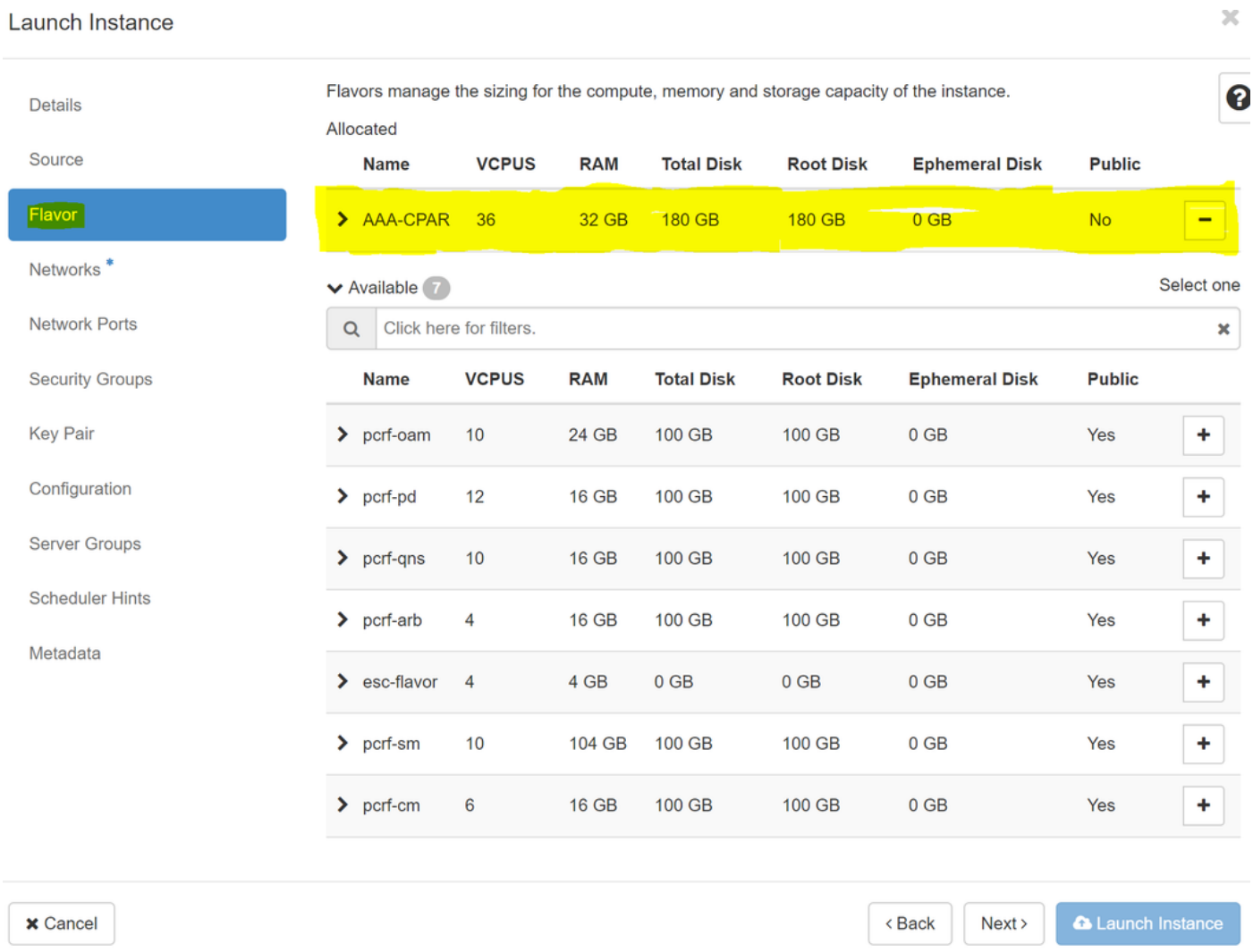
Step 5. Enter the **Instance Name** and choose the **Availability Zone** as shown in the image.



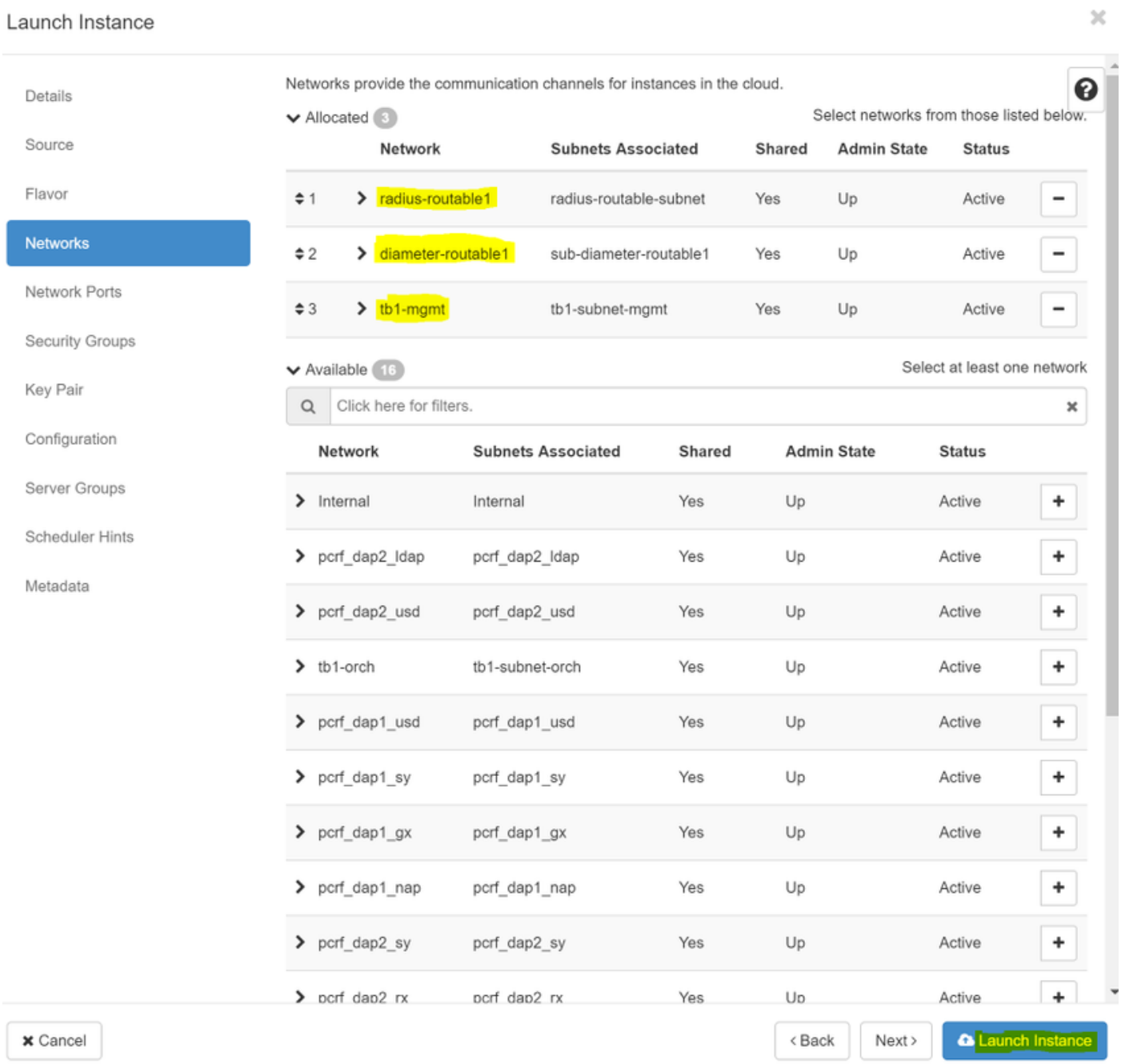
Step 6. In the Source tab, choose the image in order to create the instance. In the Select Boot Source menu, select **image** and a list of images is shown here. Choose the one that was previously uploaded by clicking on its **+** sign as shown in the image.



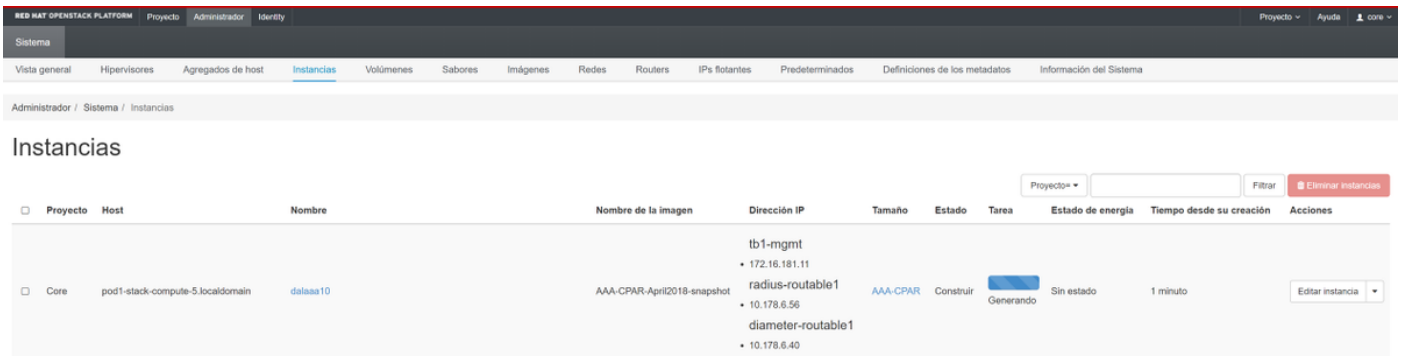
Step 7. In the Flavor tab, choose the AAA Flavor by clicking on the **+** sign as shown in the image.



Step 8. Finally, navigate to the **Networks** tab and choose the networks that the instance will need by clicking on the **+** sign. For this case, select **diameter-soutable1**, **radius-routable1** and **tb1-mgmt** as shown in the image.



Step 9. Click **Launch Instance** in order to create it. The progress can be monitored in Horizon as shown in the image.



Step 10. After a few minutes, the instance is completely deployed and ready for use as shown in the image.

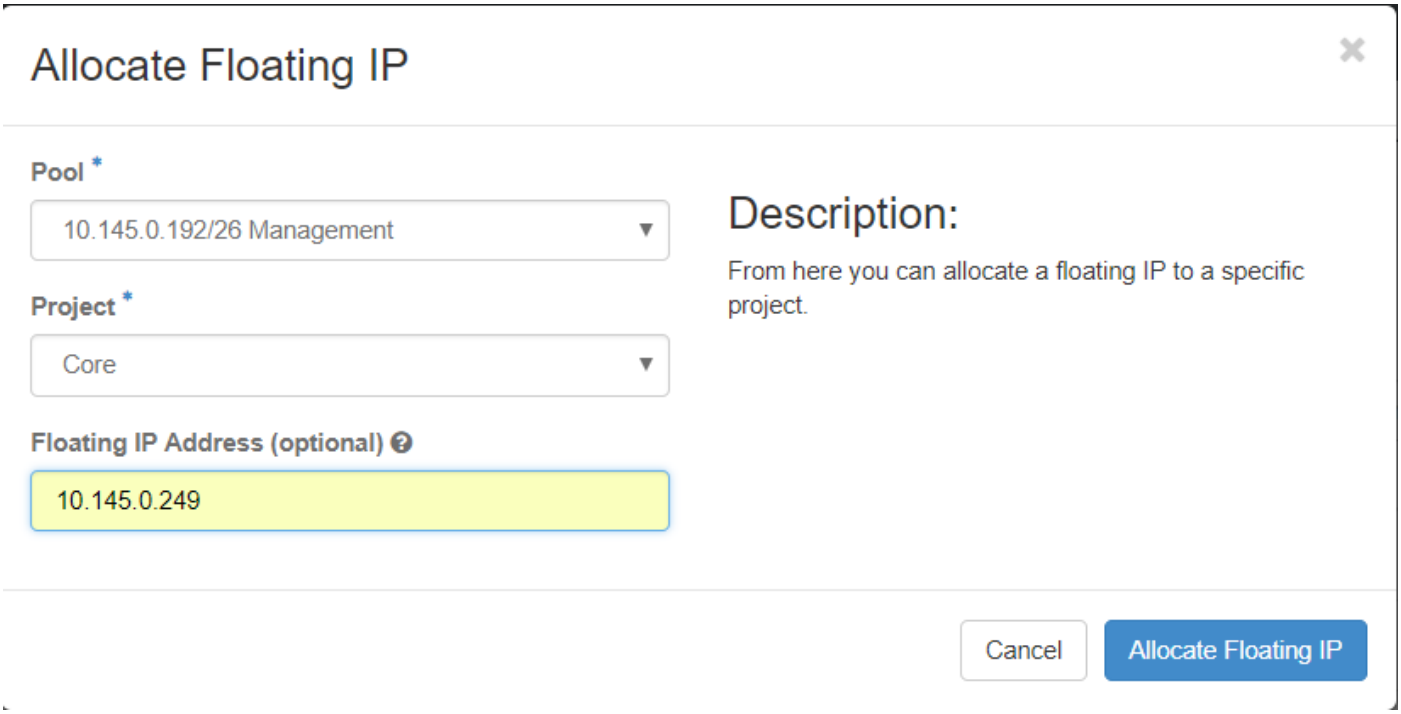
Create and Assign Floating IP Address

A floating IP address is a routable address, which means that it's reachable from the outside of Ultra M/Openstack architecture, and it's able to communicate with other nodes from the network.

Step 1. In the Horizon top menu, navigate to **Admin > Floating IPs**.

Step 2. Click **Allocate IP to Project**.

Step 3. In the **Allocate Floating IP** window, select the **Pool** from which the new floating IP belongs, the **Project** where it is going to be assigned, and the new **Floating IP Address** itself as shown in the image.

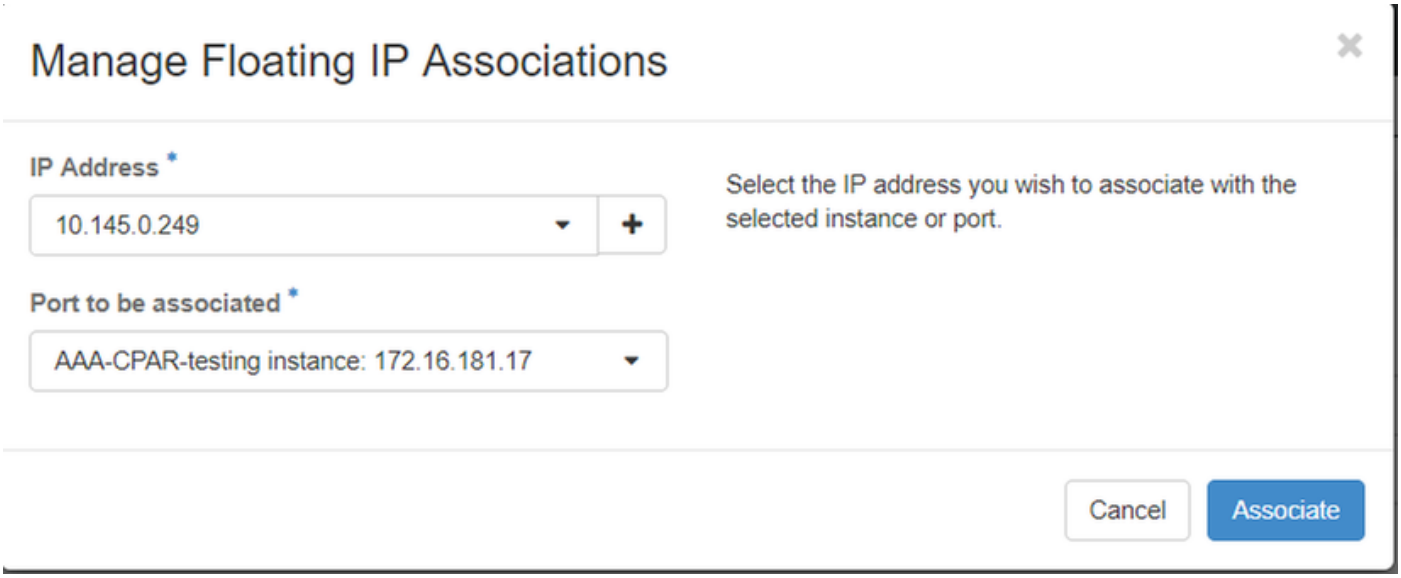


Step 4. Click **Allocate Floating IP**.

Step 5. In the Horizon top menu, navigate to **Project > Instances**.

Step 6. In the **Action** column, click on the arrow that points down in the **Create Snapshot** button, a menu is displayed. Click **Associate Floating IP** option.

Step 7. Select the corresponding floating IP address intended to be used in the **IP Address** field, and choose the corresponding management interface (eth0) from the new instance where this floating IP is going to be assigned in the **Port to be associated** as shown in the image.



Step 8. Click **Associate**.

Enable SSH

Step 1. In the Horizon top menu, navigate to **Project > Instances**.

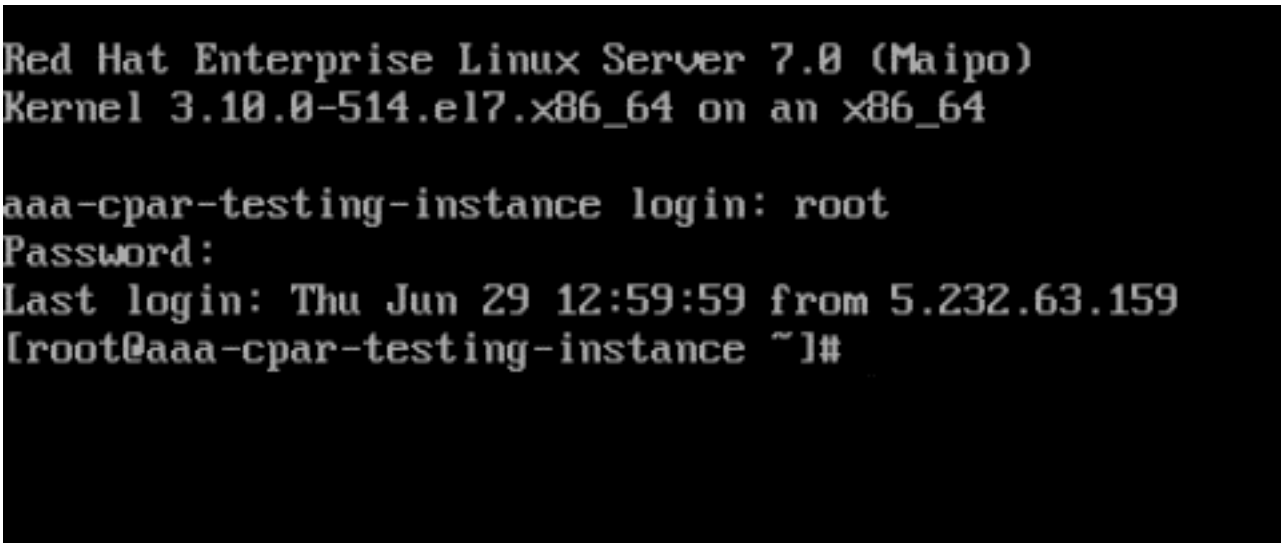
Step 2. Click on the name of the instance/VM that was created in section **Launch a new instance**.

Step 3. Click **Console**. This displays the CLI of the VM.

Step 4. Once the CLI is displayed, enter the proper login credentials as shown in the image:

Username: **root**

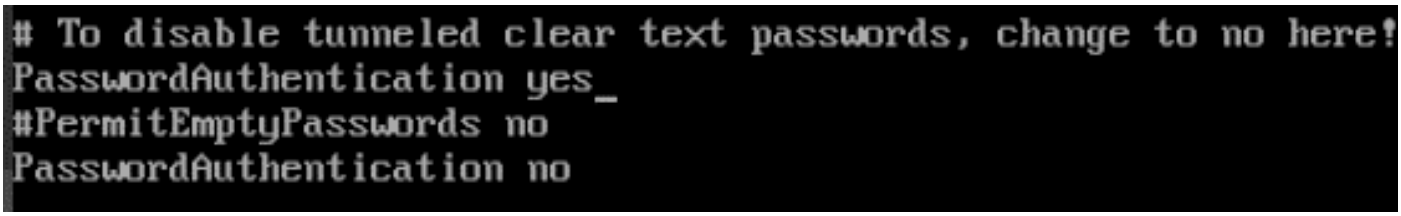
Password: <**cisco123**>



Step 5. In the CLI, run the command **vi /etc/ssh/sshd_config** in order to edit SSH configuration.

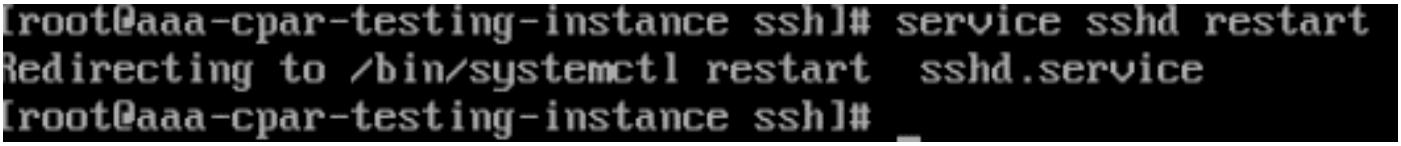
Step 6. Once the SSH configuration file is open, press **I** in order to edit the file. Then change the first line from **PasswordAuthentication no** to **PasswordAuthentication yes** as shown in the

image.

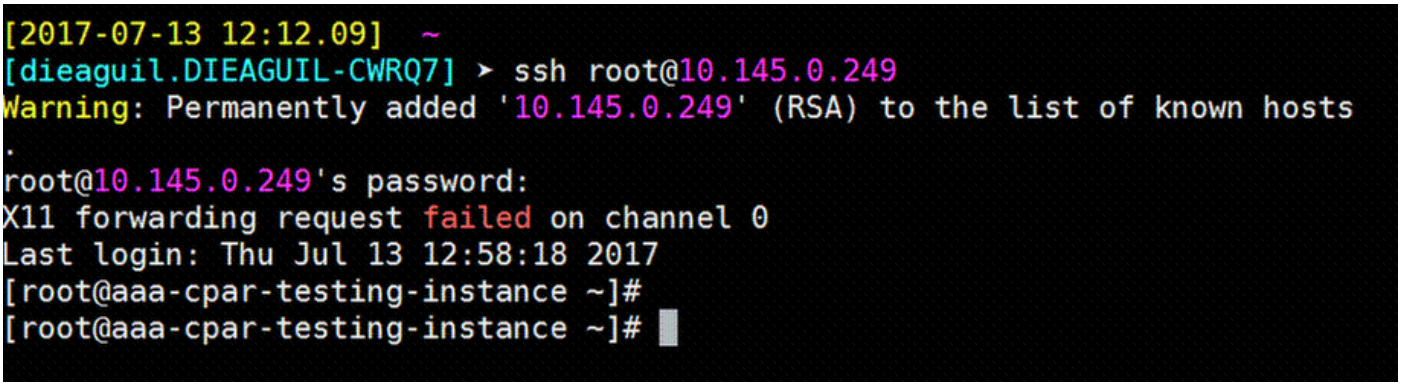


Step 7. Press **ESC** and enter **:wq!** in order to save **sshd_config** file changes.

Step 8. Run the command **service sshd restart as shown in the image.**

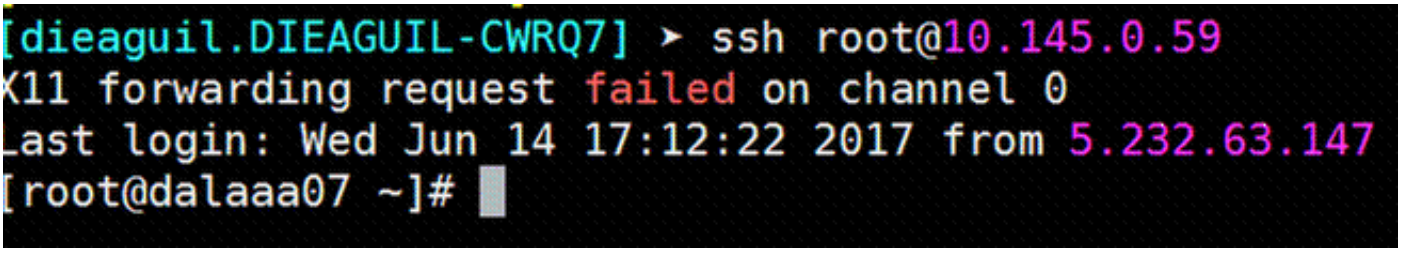


Step 9. In order to test if the SSH configuration changes have been correctly applied, open any SSH client and try to establish a remote secure connection with the floating IP assigned to the instance (i.e. **10.145.0.249**) and the user **root** as shown in the image.



Establish SSH Session

Step 1. Open a SSH session with the IP address of the corresponding VM/server where the application is installed as shown in the image.



CPAR Instance Start

Follow these steps once the activity has been completed and CPAR services can be re-established in the Site that was shut down.

Step 1. Login back to Horizon, navigate to **project > instance > start instance**.

Step 2. Verify that the Status of the instance is **Active** and the Power State is **Running** as shown in the image.

Post-activity Health Check

Step 1. Run the command **/opt/CSCOar/bin/arstatus** at OS level:

```
[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 ~]#
```

Step 2. Run the command **/opt/CSCOar/bin/aregcmd** at OS level and enter the admin credentials. Verify that CPAR Health is 10 out of 10 and the exit CPAR CLI.

```
[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
```

Step 3. Run the command **netstat | grep diameter** and verify that all DRA connections are established.

The output mentioned here is for an environment where Diameter links are expected. If fewer links are displayed, this represents a disconnection from the DRA that needs to be analyzed.

```
[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
```

Step 4. Check that the TelePresence Server (TPS) log shows the requests that are processed by CPAR. The values highlighted represent the TPS and those are the ones you need to pay attention to.

The value of TPS must not exceed 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
```

Step 5. Look for any “error” or “alarm” messages in name_radius_1_log:

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

Step 6. In order to verify the amount of memory that the CPAR process uses, run the command:

```
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
```

This highlighted value must be lower than 7Gb, which is the maximum allowed at application level.