

Instantánea y recuperación de VM CPAR

Contenido

[Introducción](#)

[Antecedentes](#)

[Impacto en la red](#)

[Alarmas](#)

[Copia de seguridad de instantánea de VM](#)

[Cierre de la aplicación CPAR](#)

[Tarea de instantánea de copia de seguridad de VM](#)

[Instantánea de VM](#)

[Recuperación de instancias con Snapshot](#)

[Proceso de recuperación](#)

[Creación y asignación de direcciones IP flotantes](#)

[Habilitar SSH](#)

[Establecer sesión SSH](#)

[Inicio de instancia de CPAR](#)

[Comprobación de estado posterior a la actividad](#)

Introducción

Este documento describe un procedimiento paso a paso sobre cómo realizar una copia de seguridad (instantánea) de las instancias de autenticación, autorización y contabilidad (AAA).

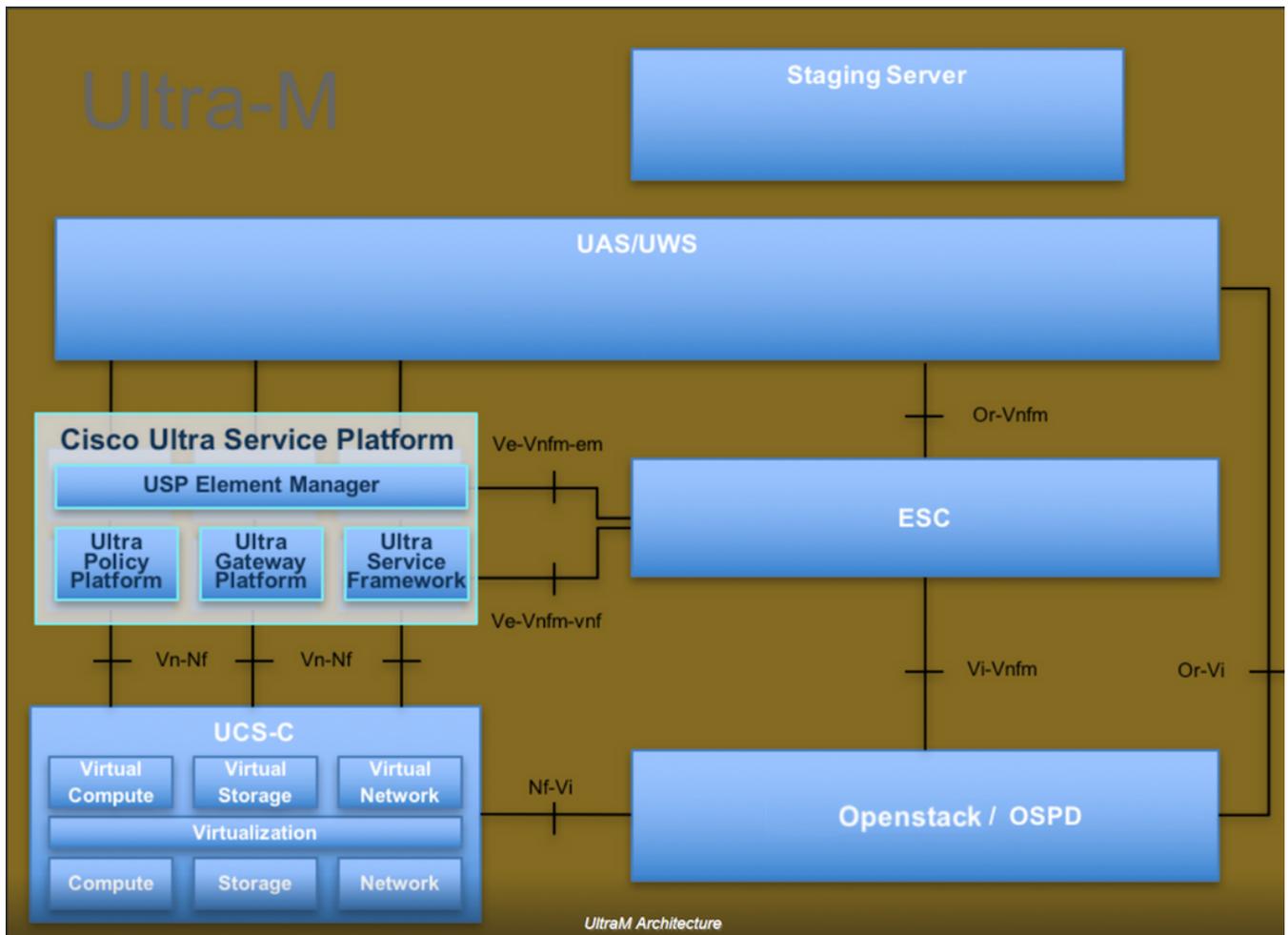
Antecedentes

Es imprescindible ejecutar esto por sitio y por sitio a la vez para minimizar el impacto en el tráfico del suscriptor.

Este procedimiento se aplica a un entorno Openstack con el uso de la versión NEWTON donde Elastic Services Controller (ESC) no administra Cisco Prime Access Registrar (CPAR) y CPAR se instala directamente en la Máquina virtual (VM) implementada en Openstack.

Ultra-M es una solución de núcleo de paquetes móviles virtualizada validada y empaquetada previamente diseñada para simplificar la implementación de funciones de red virtual (VNF). OpenStack es el Virtualized Infrastructure Manager (VIM) para Ultra-M y consta de estos tipos de nodos:

- Informática
- Disco de almacenamiento de objetos - Compute (OSD - Compute)
- Controlador
- Plataforma OpenStack: Director (OSPD)
- La arquitectura de alto nivel de Ultra-M y los componentes involucrados se ilustran en esta imagen:



Este documento está dirigido al personal de Cisco que está familiarizado con la plataforma Cisco Ultra-M y detalla los pasos necesarios para llevar a cabo en OpenStack y Redhat OS.

Nota: Se considera la versión Ultra M 5.1.x para definir los procedimientos en este documento.

Impacto en la red

En general, cuando el proceso del CPAR se interrumpe, se espera que la degradación del KPI se produzca como cuando cierra la aplicación, tarda hasta 5 minutos en enviar la trampa descendente del par de diámetro. En este momento, todas las solicitudes dirigidas al CPAR fracasarán. Después de ese tiempo, se determina que los enlaces están inactivos y el agente de routing de diámetro (DRA) detiene el enrutamiento del tráfico hacia este nodo.

Además, para todas las sesiones existentes en la AAA que se cierran, si hay un procedimiento de adjuntar/desasociar que involucra estas sesiones con otra AAA activa, ese procedimiento fallará, ya que la seguridad alojada como servicio (HSS) responde que el usuario está registrado en la AAA que se cierra y que el procedimiento no podrá completarse satisfactoriamente.

Se espera que el rendimiento de STR sea inferior al 90% aproximadamente 10 horas después de completar la actividad. Después de ese tiempo, se debe alcanzar el valor normal del 90%.

Alarmas

Las alarmas SNMP se generan cada vez que se detiene y se inicia el servicio CPAR, por lo que se espera que se generen trampas SNMP a lo largo del proceso. Las trampas esperadas incluyen:

- DETENCIÓN DEL SERVIDOR CPAR
- VM DOWN
- NODO ABAJO: (alarma esperada que no ha sido generada directamente por la instancia CPAR)
- DRA

Copia de seguridad de instantánea de VM

Cierre de la aplicación CPAR

Nota: Asegúrese de que tiene acceso a HORIZON para el sitio y acceso a OSPD.

Paso 1. Abra cualquier cliente de Secure Shell (SSH) conectado a la red de producción de Transformation Management Office (TMO) y conéctese a la instancia de CPAR.

Nota: Es importante no cerrar las 4 instancias AAA dentro de un sitio al mismo tiempo, hágalo de uno en uno.

Paso 2. Para apagar la aplicación CPAR, ejecute el comando:

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

Debe aparecer un mensaje "Cisco Prime Access Registrar Server shutdown complete".

Nota: Si deja la sesión CLI abierta, el comando **arserver stop** no funcionará y se mostrará este mensaje de error.

```
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
```

En este ejemplo, la ID de proceso resaltada 2903 debe terminar antes de que el CPAR pueda ser detenido. Si este es el caso, ejecute el comando y termine este proceso:

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

A continuación, repita el paso 1.

Paso 3. Para verificar que la aplicación CPAR fue efectivamente cerrada, ejecute el comando:

/opt/CSCOar/bin/arstatus

Estos mensajes deben aparecer:

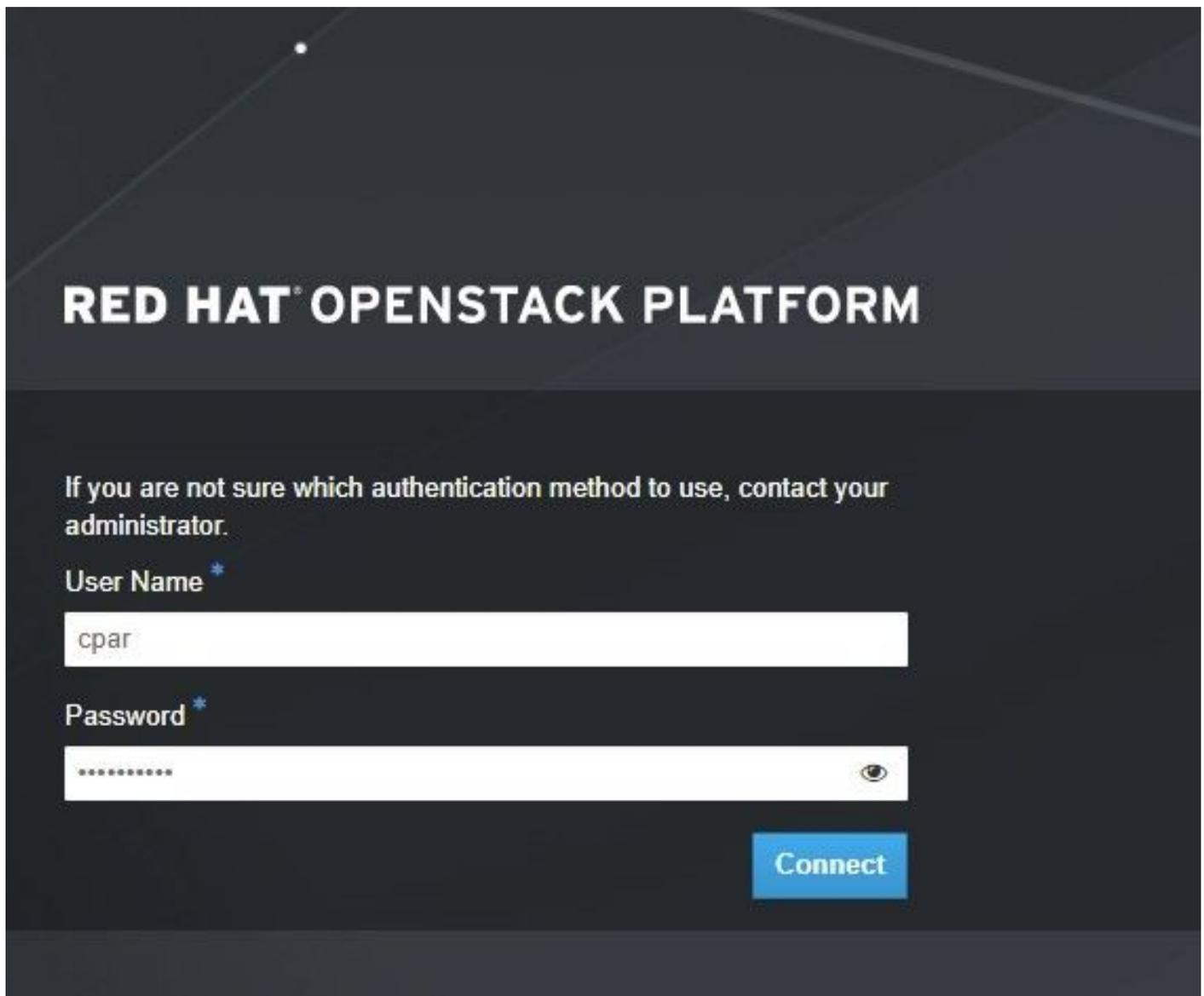
Cisco Prime Access Registrar Server Agent not running

Cisco Prime Access Registrar GUI not running

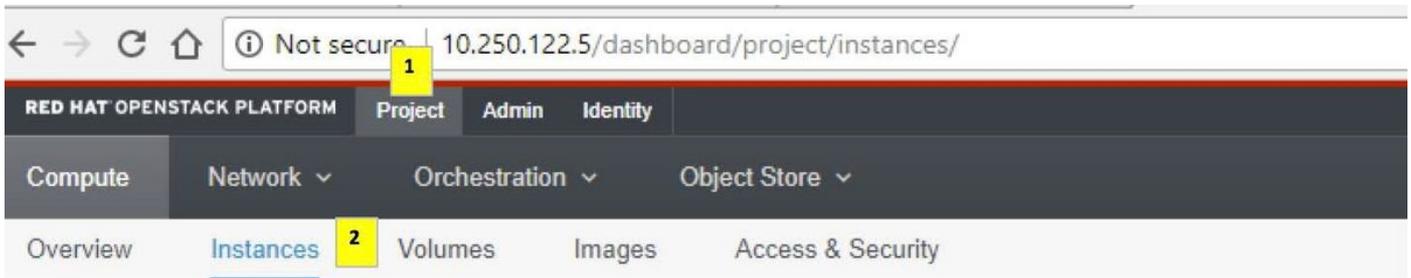
Tarea de instantánea de copia de seguridad de VM

Paso 1. Introduzca el sitio web de la interfaz gráfica de usuario de Horizonte correspondiente al sitio (ciudad) en el que se ha trabajado actualmente.

Cuando accede a Horizonte, la pantalla observada es la que se muestra en la imagen.



Paso 2. Vaya a **Project > Instancias** como se muestra en la imagen.



Si el usuario utilizado fue CPAR, en este menú solo aparecen las 4 instancias AAA.

Paso 3. Cierre sólo una instancia a la vez, repita todo el proceso en este documento. Para apagar la máquina virtual, navegue hasta **Acciones > Cerrar instancia** como se muestra en la imagen y confirme su selección.



Paso 4. Para validar que la instancia se apague, verifique el estado = **Apagar** y el estado de energía = **Apagar**, como se muestra en la imagen.

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

Este paso finaliza el proceso de cierre del CPAR.

Instantánea de VM

Una vez que las máquinas virtuales CPAR están inactivas, las instantáneas pueden tomarse en paralelo, ya que pertenecen a equipos independientes.

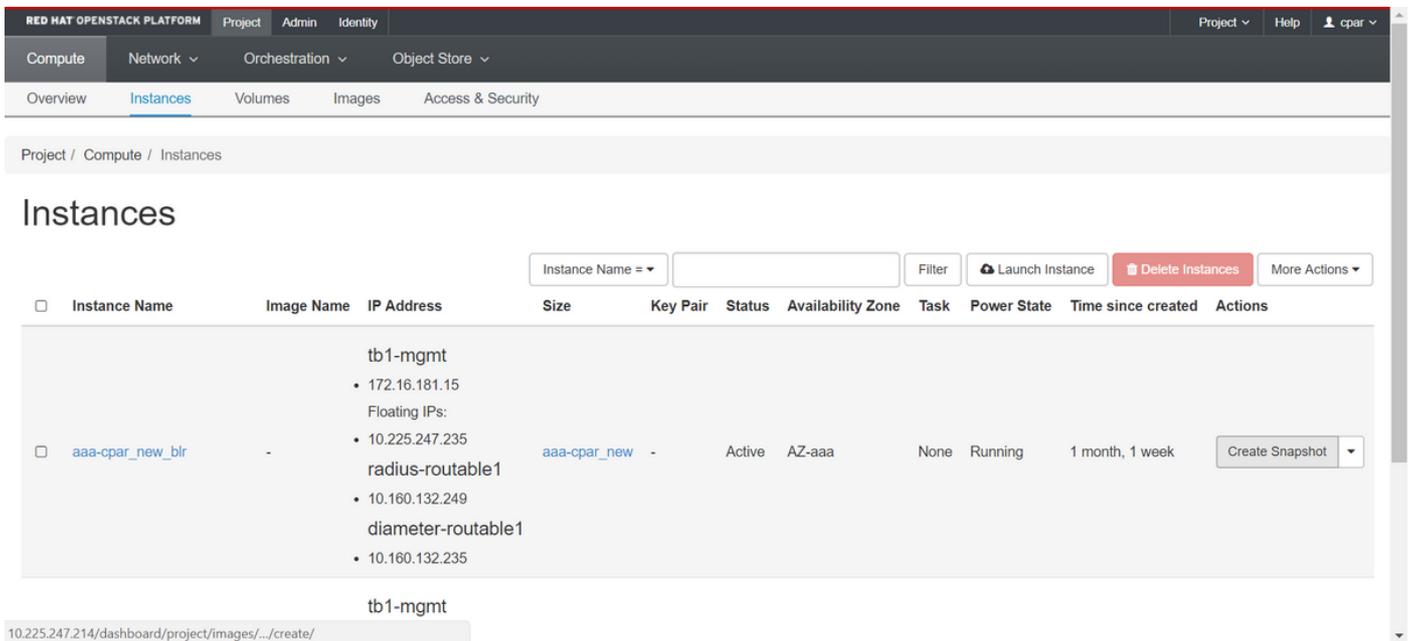
Los cuatro archivos QCOW2 se crean en paralelo.

Paso 1. Tome una instantánea de cada instancia de AAA.

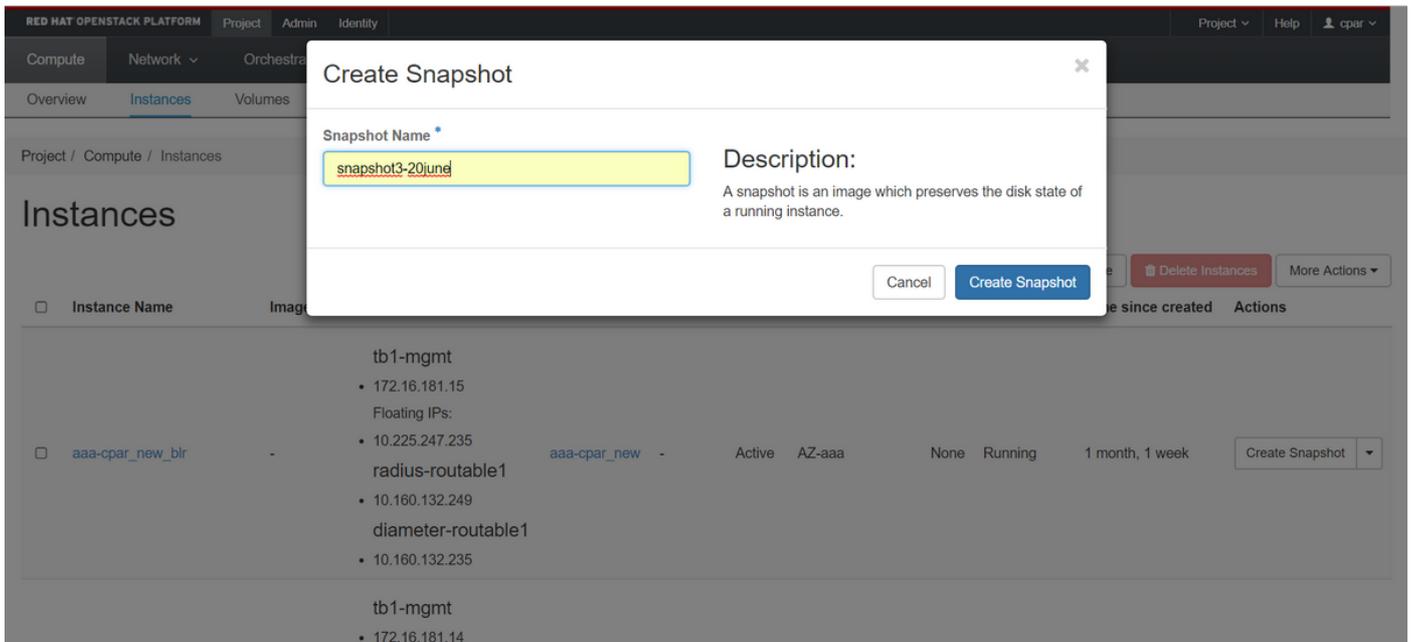
Nota: 25 minutos para las instancias que utilizan una imagen QCOW como origen y 1 hora para las instancias que utilizan una imagen sin formato como origen.

Paso 2. Inicie sesión en la **GUI** Horizonte de Openstack de POD.

Paso 3. Una vez que inicie sesión, navegue hasta **Project > Compute > Instancias** en el menú superior y busque las instancias AAA como se muestra en la imagen.



Paso 3. Haga clic en **Crear instantánea** para continuar con la creación de la instantánea como se muestra en la imagen. Esto debe ejecutarse en la instancia AAA correspondiente.



Paso 4. Una vez ejecutada la instantánea, navegue hasta el menú **Images** y verifique que todos terminen y no informen de ningún problema, como se muestra en la imagen.

RED HAT OPENSTACK PLATFORM Project Admin Identity Project Help cpar

Compute Network Orchestration Object Store

Overview Instances Volumes Images Access & Security

Images

Q Click here for filters. + Create Image Delete Images

Owner	Name ^	Type	Status	Visibility	Protected	Disk Format	Size	
Core	cluman_snapshot	Image	Active	Shared with Project	No	RAW	100.00 GB	Launch
Core	ESC-image	Image	Active	Shared with Project	No	QCOW2	925.06 MB	Launch
Core	rebuild_cluman	Image	Active	Shared with Project	No	QCOW2	100.00 GB	Launch
Cpar	rhel-guest-image-testing	Image	Active	Public	No	QCOW2	422.69 MB	Launch
Cpar	snapshot3-20june	Image	Active	Private	No	QCOW2	0 bytes	Launch
Cpar	snapshot_cpar_20june	Image	Active	Private	No	QCOW2	0 bytes	Launch
Cpar	snapshot_cpar_20june	Image	Active	Private	No	QCOW2	0 bytes	Launch

Paso 5. El siguiente paso es descargar la instantánea en un formato QCOW2 y transferirla a una entidad remota, en caso de que la OSPD se pierda en este proceso. Para lograr esto, identifique la instantánea ejecutando el comando **glance image-list** en el nivel OSPD como se muestra en la imagen.

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

Paso 6. Una vez que identifique la instantánea que se descargará (en este caso, es la marcada en verde), puede descargarla en formato QCOW2 con el comando **glance image-download** como se muestra aquí:

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

El comando **&** envía el proceso al fondo. Lleva algún tiempo completar la acción. Una vez hecho, la imagen se puede encontrar en el directorio **/tmp**.

- Cuando envía el proceso al fondo y si se pierde la conectividad, el proceso también se detiene.
- Ejecute el comando **disown -h** para que en caso de que se pierda la conexión SSH, el proceso se ejecute y termine en el OSPD.

Paso 7. Una vez finalizado el proceso de descarga, es necesario ejecutar un proceso de compresión, ya que esa instantánea se puede rellenar con ZEROES debido a los procesos, tareas y archivos temporales manejados por el sistema operativo (OS). El comando que se

ejecutará para la compresión de archivos es **virt-sparsify**.

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

Este proceso puede tardar algún tiempo (entre 10 y 15 minutos). Una vez terminado, el archivo que resulta es el que debe transferirse a una entidad externa como se especifica en el paso siguiente.

Para lograr esto, se requiere la verificación de la integridad del archivo, ejecute el siguiente comando y busque el atributo "corrupto" al final de su salida.

```
[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
```

Paso 8. Para evitar un problema donde se pierde la OSPD, la instantánea creada recientemente en formato QCOW2 debe transferirse a una entidad externa. Antes de iniciar la transferencia de archivos, debe verificar si el destino tiene suficiente espacio disponible en disco, ejecute el comando **df -kh** para verificar el espacio de memoria.

Un consejo es transferirla temporalmente al OSPD de otro sitio con el uso de SFTP **sftp root@x.x.x.x**, donde **x.x.x.x** es la IP de un OSPD remoto.

Paso 9. Para acelerar la transferencia, el destino se puede enviar a varios OSPD. De la misma manera, puede ejecutar el comando **scp *name_of_the_file*.qcow2 root@x.x.x.x:/tmp** (donde **x.x.x.x** es la IP de un OSPD remoto) para transferir el archivo a otro OSPD.

Recuperación de instancias con Snapshot

Proceso de recuperación

Es posible volver a implementar la instancia anterior con la instantánea tomada en pasos anteriores.

Paso 1. [OPCIONAL] Si no hay ninguna instantánea de VM anterior disponible, conéctese al nodo OSPD donde se envió la copia de seguridad y devuelva la copia de seguridad a su nodo OSPD original. Utilice `sftp root@x.x.x.x`, donde `x.x.x.x` es la IP de un OSPD original. Guarde el archivo de instantánea en el directorio `/tmp`.

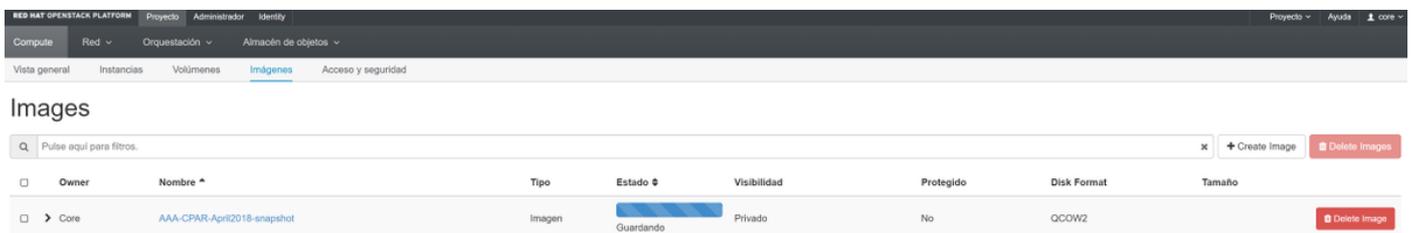
Paso 2. Conéctese al nodo OSPD donde se vuelve a implementar la instancia como se muestra en la imagen.

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

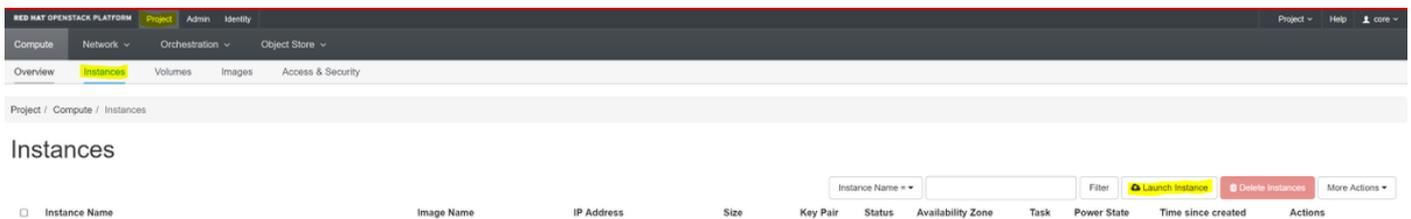
Paso 3. Para utilizar la instantánea como una imagen, es necesario cargarla en el horizonte como tal. Utilice el siguiente comando para hacerlo.

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

El proceso se puede ver en el horizonte y como se muestra en la imagen.



Paso 4. En Horizonte, navegue hasta **Project > Inases** y haga clic en **Iniciar Instancia** como se muestra en la imagen.



Paso 5. Ingrese el nombre de la instancia y elija la zona de disponibilidad como se muestra en la imagen.



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 (selected)
Source *
Flavor *
Networks *
Network Ports
Security Groups
Key Pair
Configuration
Server Groups
Scheduler Hints
Metadata

Paso 6. En la ficha Origen, elija la imagen para crear la instancia. En el menú Seleccionar origen de arranque, seleccione **imagen** y aquí se muestra una lista de imágenes. Elija el que se ha cargado previamente haciendo clic en su signo + como se muestra en la imagen.

Details

Source

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

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.



Select Boot Source

Image

Create New Volume

Yes

No

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

< Back

Next >

Launch Instance

Paso 7. En la pestaña Sabor, elija el Sabor AAA haciendo clic en el signo + como se muestra en la imagen.

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

Paso 8. Finalmente, navegue hasta la pestaña **Redes** y elija las redes que la instancia necesitará haciendo clic en el + signo+. Para este caso, seleccione **diámetro-soutable1**, **radius-routable1** y **tb1-mgmt** como se muestra en la imagen.

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

Q Click here for filters. x

	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	+

Paso 9. Haga clic en **Iniciar instancia** para crearla. El progreso se puede monitorear en Horizon como se muestra en la imagen.

RED HAT OPENSTACK PLATFORM Proyecto Administrador Identity Proyecto Ayuda core

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

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	dsaaaa10	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"/>

Paso 10. Después de unos minutos, la instancia se implementa completamente y está lista para utilizarse, como se muestra en la imagen.

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 						

Creación y asignación de direcciones IP flotantes

Una dirección IP flotante es una dirección enrutable, lo que significa que se puede alcanzar desde el exterior de la arquitectura Ultra M/Openstack, y es capaz de comunicarse con otros nodos desde la red.

Paso 1. En el menú superior Horizonte, navegue hasta **Admin > Floating IPs**.

Paso 2. Haga clic en **Asignar IP al proyecto**.

Paso 3. En la ventana **Asignar IP Flotante**, seleccione el **Pool** del que pertenece la nueva IP flotante, el **Proyecto** donde se va a asignar y la nueva **Dirección IP Flotante** como se muestra en la imagen.

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

Paso 4. Haga clic en **Asignar IP flotante**.

Paso 5. En el menú superior Horizonte, vaya a **Proyecto > Instancias**.

Paso 6. En la columna **Acción**, haga clic en la flecha que apunta hacia abajo en el botón **Crear instantánea**, se muestra un menú. Haga clic en la opción **Asociar IP flotante**.

Paso 7. Seleccione la dirección IP flotante correspondiente que se utilizará en el campo **IP Address**, y elija la interfaz de administración correspondiente (eth0) de la nueva instancia donde se va a asignar esta IP flotante en el **puerto que se va a asociar** como se muestra en la imagen.

Manage Floating IP Associations



IP Address *

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

Port to be associated *

Cancel

Associate

Paso 8. Haga clic en **Asociar**.

Habilitar SSH

Paso 1. En el menú superior Horizonte, vaya a **Proyecto > Instancias**.

Paso 2. Haga clic en el nombre de la instancia/VM que se creó en la sección **Iniciar una nueva instancia**.

Paso 3. Haga clic en **Consola**. Muestra la CLI de la máquina virtual.

Paso 4. Una vez que se muestre la CLI, introduzca las credenciales de inicio de sesión adecuadas, como se muestra en la imagen:

Nombre de usuario: **raíz**

Contraseña <**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 ~]#
```

Paso 5. En la CLI, ejecute el comando `vi /etc/ssh/sshd_config` para editar la configuración de SSH.

Paso 6. Una vez abierto el archivo de configuración de SSH, presione I para editar el archivo. A continuación, cambie la primera línea de **PasswordAuthentication no** a **PasswordAuthentication yes** como se muestra en la imagen.

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

Paso 7. Presione **ESC** e ingrese **:wq!** para guardar los cambios en el archivo **sshd_config**.

Paso 8. Ejecute el comando **service sshd restart** como se muestra en la imagen.

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

Paso 9. Para probar si los cambios de configuración de SSH se han aplicado correctamente, abra cualquier cliente SSH e intente establecer una conexión segura remota con la IP flotante asignada a la instancia (es decir, **10.145.0.249**) y la **raíz del usuario** como se muestra en la imagen.

```
[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 ~]#
```

Establecer sesión SSH

Paso 1. Abra una sesión SSH con la dirección IP de la VM/servidor correspondiente donde se instala la aplicación, como se muestra en la imagen.

```
[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 ~]#
```

Inicio de instancia de CPAR

Siga estos pasos una vez que se haya completado la actividad y los servicios CPAR puedan restablecerse en el Sitio que se cerró.

Paso 1. Vuelva a iniciar sesión en Horizon, navegue hasta **project > instance > start instance**.

Paso 2. Verifique que el estado de la instancia sea **Activo** y que el estado de energía esté en **ejecución** como se muestra en la imagen.

Instances



Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
dl1aaa04	dl1aaa01-sept092017	diameter-routable1 • 10.160.132.231 radius-routable1 • 10.160.132.247 tb1-mgmt • 172.16.181.16 Floating IPs: • 10.250.122.114	AAA-CPAR		Active	AZ-dl1aaa04	None	Running	3 months	Create Snapshot

Comprobación de estado posterior a la actividad

Paso 1. Ejecute el comando `/opt/CSCOar/bin/arstatus` a nivel del 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 ~]#
```

Paso 2. Ejecute el comando `/opt/CSCOar/bin/aregcmd` a nivel del sistema operativo e ingrese las credenciales de administración. Verifique que CPAR Health sea 10 de 10 y que salga de 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
```

Paso 3. Ejecute el comando **netstat | diámetro grep** y verifique que se hayan establecido todas las conexiones DRA.

El resultado mencionado aquí es para un entorno en el que se esperan links Diámetro. Si se muestran menos enlaces, esto representa una desconexión del DRA que se debe analizar.

```
[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
```

Paso 4. Compruebe que el registro TelePresence Server (TPS) muestre las solicitudes procesadas por CPAR. Los valores resaltados representan el TPS y son a los que debe prestar atención.

El valor de TPS no debe ser superior a 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

Paso 5. Busque cualquier mensaje de "error" o "alarma" en name_radius_1_log:

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

Paso 6. Para verificar la cantidad de memoria que utiliza el proceso CPAR, ejecute el 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
```

Este valor resaltado debe ser inferior a 7 Gb, que es el máximo permitido en el nivel de aplicación.

