

Istantanea e ripristino di VM CPAR

Sommario

[Introduzione](#)

[Premesse](#)

[Impatto sulla rete](#)

[Allarmi](#)

[Backup snapshot VM](#)

[Arresto applicazione CPAR](#)

[Attività snapshot backup VM](#)

[Snapshot VM](#)

[Ripristina istanza con snapshot](#)

[Processo di ripristino](#)

[Crea e assegna indirizzo IP mobile](#)

[Abilitazione SSH](#)

[Definizione sessione SSH](#)

[Avvio istanza CPAR](#)

[Controllo dello stato post-attività](#)

Introduzione

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

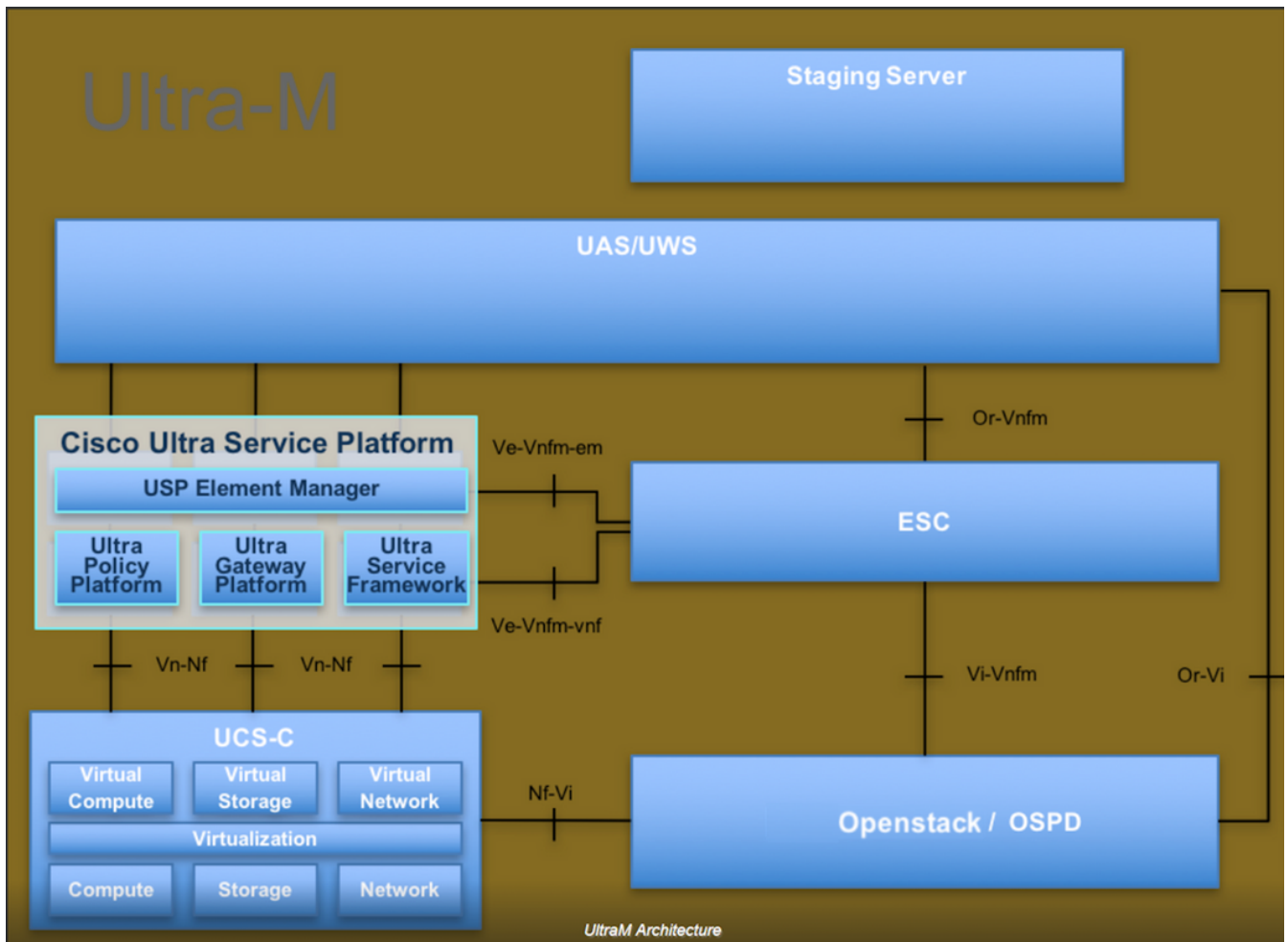
Premesse

È essenziale 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/CSC0ar/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/CSC0ar/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:

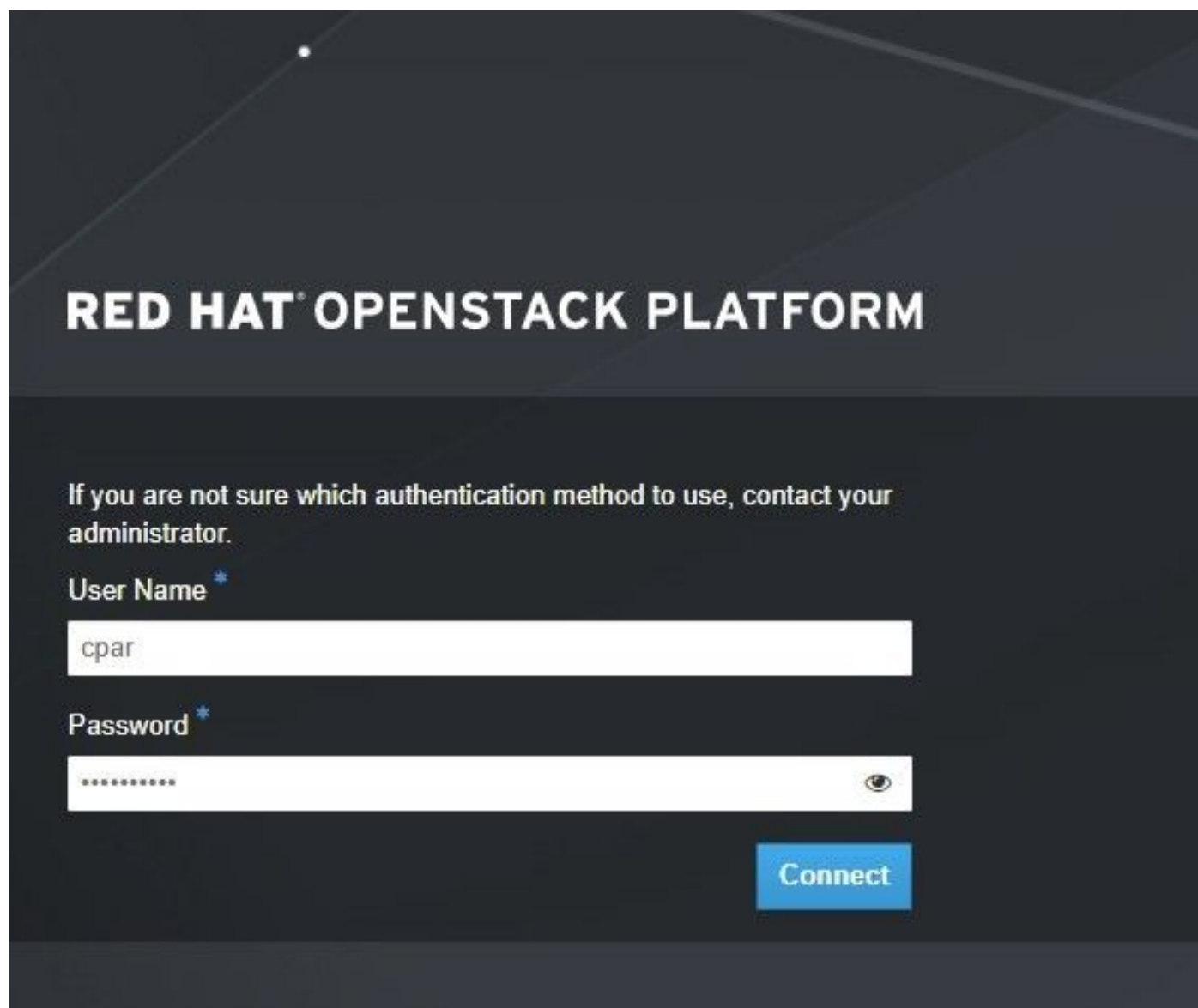
```
Cisco Prime Access Registrar Server Agent not running
```

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

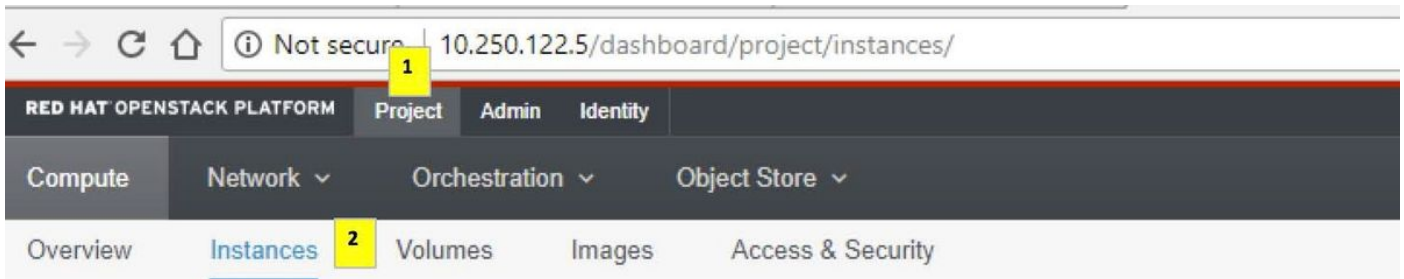
Attività snapshot backup VM

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.

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

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.

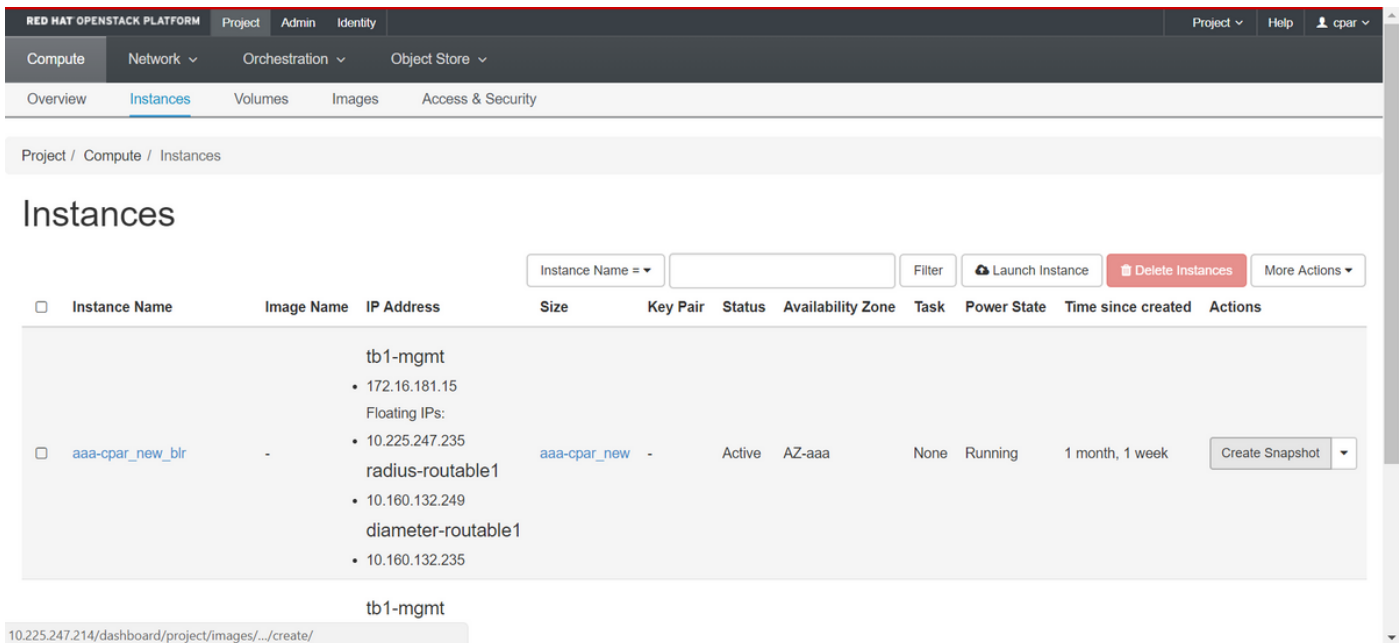
I quattro file QCOW2 vengono creati in parallelo.

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

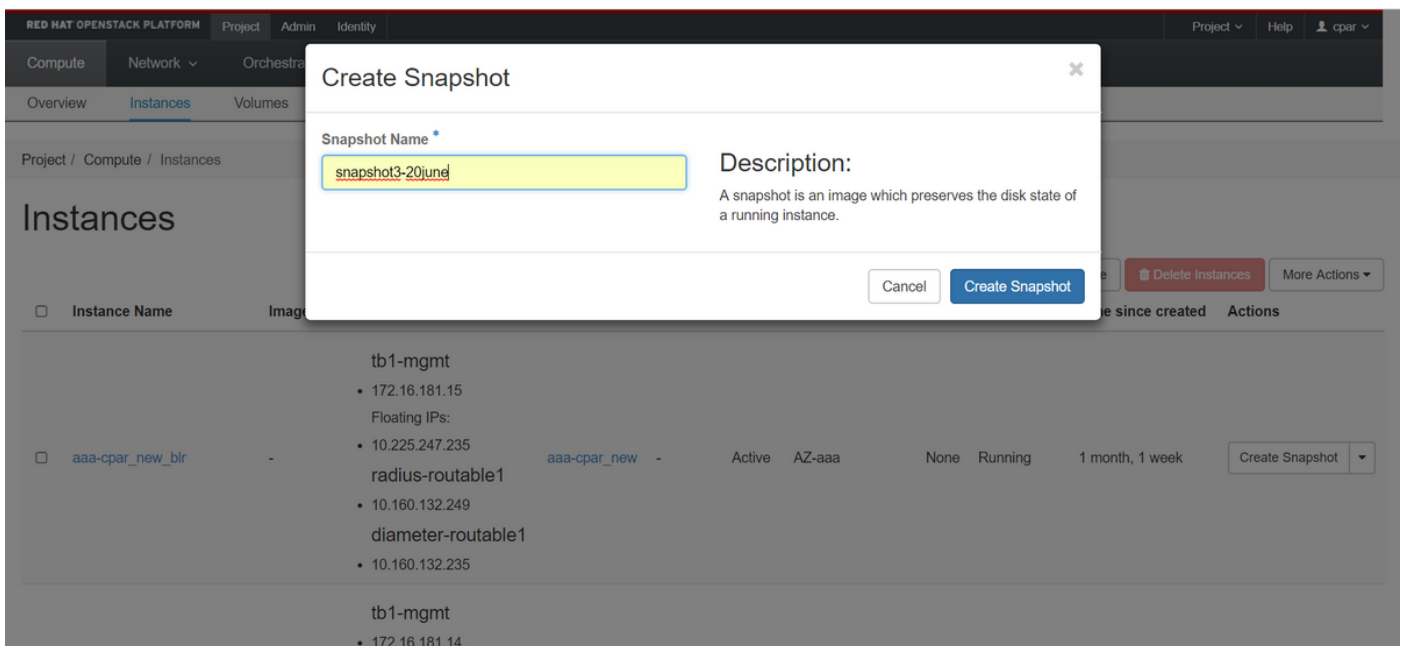
Nota: 25 minuti per le istanze che utilizzano un'immagine QCOW come origine e 1 ora per le istanze che utilizzano un'immagine raw come origine.

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.

RED HAT OPENSTACK PLATFORM Project Admin Identity Project Help cpar

Compute Network Orchestration Object Store

Overview Instances Volumes Images Access & Security

Images

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

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.x** dove **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

È possibile 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`.

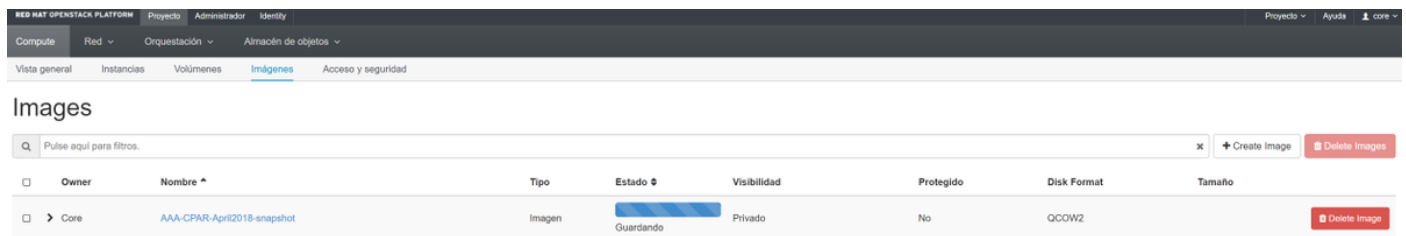
Passaggio 2. Connettersi al nodo OSPD in cui l'istanza viene ridistribuita come mostrato nell'immagine.

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

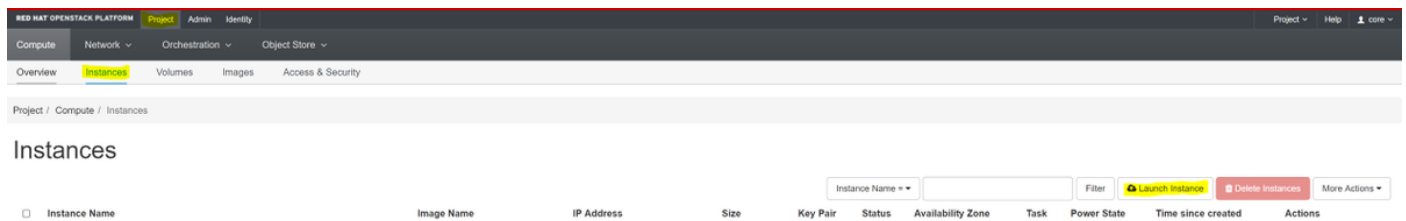
Passaggio 3. Per utilizzare l'istantanea come immagine, è necessario caricarla in Horizon come tale. A tale scopo, utilizzare il comando successivo.

```
#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.

Details

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

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

Instance Name *
dalaaa10

Availability Zone
AZ-dalaaa10

Count *
1

Total Instances (100 Max)
27%

- 26 Current Usage
- 1 Added
- 73 Remaining

✕ Cancel < Back Next > Launch Instance

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.

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

Source

Select Boot Source: Create New Volume:

Allocated

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

▼ Available 8 Select one

🔍 Click here for filters. ✕

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

✕ Cancel < Back Next > Launch Instance

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

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	-

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

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.



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	+

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

RED HAT OPENSTACK PLATFORM | Progetto | Amministrador | Identity

Sistema

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

Administrador / Sistema / Instancias

Instancias

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-April2019-snapshot	tb1-mgmt • 172.16.181.11 radius-routable1 • 10.178.6.56 diameter-routable1 • 10.178.6.40	AAA-CPAR	Construir	Generando	Sin estado	1 minuto	<input type="button" value=" Editar instancia"/>

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.

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

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.

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

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>

```
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 ~]#
```

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.

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

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.

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

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.

```
[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 ~]#
```

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.

```
[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 ~]#
```

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.

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

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/CSC0ar/logs/tps-11-21-2017.csv
```

```
11-21-2017,23:57:35,263,0
```

```
11-21-2017,23:57:50,237,0
```

```
11-21-2017,23:58:05,237,0
```

```
11-21-2017,23:58:20,257,0
```

```
11-21-2017,23:58:35,254,0
```

```
11-21-2017,23:58:50,248,0
```

11-21-2017,23:59:05,272,0

11-21-2017,23:59:20,243,0

11-21-2017,23:59:35,244,0

11-21-2017,23:59:50,233,0

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.

