Red Hat Enterprise Linux 8

Implantación de Red Hat Enterprise Linux 8 en plataformas de nube pública

Creación de imágenes personalizadas de Red Hat Enterprise Linux y configuración de un clúster de alta disponibilidad de Red Hat para plataformas de nube pública

Last Updated: 2021-03-07

Red Hat Enterprise Linux 8 Implantación de Red Hat Enterprise Linux 8 en plataformas de nube pública

Creación de imágenes personalizadas de Red Hat Enterprise Linux y configuración de un clúster de alta disponibilidad de Red Hat para plataformas de nube pública

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

Legal Notice

Resumen

Puede crear e implementar imágenes personalizadas de Red Hat Enterprise Linux en varias plataformas de nube, incluyendo Microsoft Azure, Amazon Web Services (AWS) y Google Cloud Platform (GCP). También puede crear y configurar un cluster de alta disponibilidad de Red Hat en cada plataforma de nube. Este documento incluye procedimientos para la creación de clusters de alta disponibilidad, incluyendo la instalación de los paquetes y agentes requeridos, la configuración de las cercas y la instalación de agentes de recursos de red. Cada proveedor de nube tiene su propio capítulo que describe la creación e implementación de una imagen personalizada. También hay un capítulo separado para configurar clusters de HA para cada proveedor de nube.

Table of Contents

HACER QUE EL CÓDIGO ABIERTO SEA MÁS INCLUSIVO

Red Hat se compromete a sustituir el lenguaje problemático en nuestro código, documentación y propiedades web. Estamos empezando con estos cuatro términos: maestro, esclavo, lista negra y lista blanca. Debido a la enormidad de este esfuerzo, estos cambios se implementarán gradualmente a lo largo de varias versiones próximas. Para más detalles, consulte el mensaje de nuestro CTO Chris Wright .

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT

Agradecemos su opinión sobre nuestra documentación. Por favor, díganos cómo podemos mejorarla. Para ello:

- Para comentarios sencillos sobre pasajes concretos:
  1. Asegúrese de que está viendo la documentación en el formato *Multi-page HTML*. Además, asegúrese de ver el botón **Feedback** en la esquina superior derecha del documento.
  2. Utilice el cursor del ratón para resaltar la parte del texto que desea comentar.
  3. Haga clic en la ventana emergente **Add Feedback** que aparece debajo del texto resaltado.
  4. Siga las instrucciones mostradas.
- Para enviar comentarios más complejos, cree un ticket de Bugzilla:
  1. Vaya al sitio web de Bugzilla.
  2. Como componente, utilice **Documentation**.
  3. Rellene el campo **Description** con su sugerencia de mejora. Incluya un enlace a la(s) parte(s) pertinente(s) de la documentación.
  4. Haga clic en **Submit Bug**.

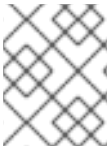
CAPÍTULO 1. IMPLANTACIÓN DE UNA IMAGEN DE RED HAT ENTERPRISE LINUX 8 COMO MÁQUINA VIRTUAL EN MICROSOFT AZURE

Tiene varias opciones para implementar una imagen de Red Hat Enterprise Linux (RHEL) 8 en Azure. Este capítulo discute sus opciones para elegir una imagen y enumera o se refiere a los requisitos del sistema para su sistema anfitrión y máquina virtual (VM). Este capítulo también proporciona procedimientos para crear una VM personalizada a partir de una imagen ISO, subirla a Azure y lanzar una instancia de VM de Azure.

IMPORTANTE

Aunque puede crear una VM personalizada a partir de una imagen ISO, Red Hat recomienda que utilice el producto Red Hat Image Builder para crear imágenes personalizadas para su uso en proveedores de nube específicos. Con Image Builder, puede crear y cargar una imagen de disco Azure (formato VHD). Consulte Composición de una imagen de sistema RHEL personalizada para obtener más información.

Este capítulo hace referencia a la documentación de Azure en varios lugares. Para muchos procedimientos, consulte la documentación de Azure a la que se hace referencia para obtener más detalles.



NOTA

Para obtener una lista de los productos de Red Hat que puede utilizar de forma segura en Azure, consulte Red Hat en Microsoft Azure.

Requisitos previos

- Regístrese para obtener una cuenta en el Portal del Cliente de Red Hat.
- Regístrese para obtener una cuenta de Microsoft Azure.
- Habilite sus suscripciones en el programa Red Hat Cloud Access. El programa Red Hat Cloud Access le permite trasladar sus suscripciones de Red Hat desde sistemas físicos o locales a Azure con el apoyo total de Red Hat.

Recursos adicionales

- Red Hat en la nube pública
- Guía de referencia de Red Hat Cloud Access
- Preguntas frecuentes y prácticas recomendadas para Microsoft Azure

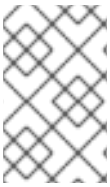
1.1. OPCIONES DE IMAGEN DE RED HAT ENTERPRISE LINUX EN AZURE

La siguiente tabla enumera las opciones de imagen y señala las diferencias entre ellas.

Tabla 1.1. Opciones de imagen

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones
Elija implementar una imagen de Red Hat Gold.	Aproveche sus suscripciones existentes a Red Hat.	Habilite las suscripciones a través del programa Red Hat Cloud Access y luego elija una Red Hat Gold Image en Azure. Consulte el Manual de referencia de Red Hat Cloud Access para obtener detalles sobre las imágenes Gold y cómo acceder a ellas en Azure.	La suscripción incluye el coste del producto de Red Hat; el resto de los costes de las instancias se pagan a Microsoft. Las imágenes Red Hat Gold se denominan imágenes "Cloud Access" porque aprovechan sus suscripciones existentes a Red Hat. Red Hat proporciona soporte directamente para las imágenes de Cloud Access.
Elija desplegar una imagen personalizada que traslade a Azure.	Aproveche sus suscripciones existentes a Red Hat.	Habilite las suscripciones a través del programa Red Hat Cloud Access, cargue su imagen personalizada y adjunte sus suscripciones.	La suscripción incluye el coste del producto de Red Hat; el resto de los costes de las instancias se pagan a Microsoft. Las imágenes personalizadas que se trasladan a Azure son imágenes de "Acceso a la nube" porque se aprovechan las suscripciones existentes de Red Hat. Red Hat proporciona soporte directamente para las imágenes de Cloud Access.

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones
Elija desplegar una imagen de Azure existente que incluya RHEL.	Las imágenes de Azure incluyen un producto de Red Hat.	Elija una imagen RHEL cuando cree una VM utilizando la consola de Azure, o elija una VM de Azure Marketplace.	Se paga a Microsoft por hora en un modelo de pago por uso. Este tipo de imágenes se denominan "on-demand" Azure proporciona soporte para las imágenes bajo demanda a través de un acuerdo de soporte. Red Hat proporciona las actualizaciones de las imágenes. Azure hace que las actualizaciones estén disponibles a través de Red Hat Update Infrastructure (RHUI).



NOTA

Puede crear una imagen personalizada para Azure utilizando Red Hat Image Builder. Consulte Composición de una imagen de sistema RHEL personalizada para obtener más información.

El resto de este capítulo incluye información y procedimientos relacionados con las imágenes personalizadas de Red Hat Enterprise Linux.

Recursos adicionales

- Imágenes Red Hat Gold en Microsoft Azure
- Programa Red Hat Cloud Access
- Mercado Azure
- Opciones de facturación en Azure Marketplace
- Imágenes Gold de Red Hat Enterprise Linux con suscripción propia en Azure

1.2. COMPRENDER LAS IMÁGENES BASE

Esta sección incluye información sobre el uso de imágenes base preconfiguradas y sus ajustes de configuración.

1.2.1. Utilizar una imagen base personalizada

Para configurar manualmente una VM, se empieza con una imagen de VM base (de inicio). Una vez creada la imagen de la VM base, puede modificar los ajustes de configuración y añadir los paquetes que la VM necesita para funcionar en la nube. Puede realizar cambios de configuración adicionales para su

aplicación específica después de cargar la imagen.

Para preparar una imagen de nube de RHEL, siga las siguientes instrucciones. Para preparar una imagen de nube Hyper-V de RHEL, consulte la sección Preparar una máquina virtual basada en Red Hat desde Hyper-V Manager.

Recursos adicionales

Red Hat Enterprise Linux

1.2.2. Paquetes de sistema necesarios

Los procedimientos en este capítulo asumen que usted está usando un sistema anfitrión que ejecuta Red Hat Enterprise Linux. Para completar con éxito los procedimientos, su sistema anfitrión debe tener instalados los siguientes paquetes.

Tabla 1.2. Paquetes del sistema

Paquete	Repositorio	Descripción
libvirt	rhel-8-for-x86_64-appstream-rpms	API, demonio y herramienta de gestión de código abierto para gestionar la virtualización de plataformas
virt-install	rhel-8-for-x86_64-appstream-rpms	Una utilidad de línea de comandos para crear máquinas virtuales
libguestfs	rhel-8-for-x86_64-appstream-rpms	Una biblioteca para acceder y modificar los sistemas de archivos de las máquinas virtuales
libguestfs-tools	rhel-8-for-x86_64-appstream-rpms	Herramientas de administración del sistema para máquinas virtuales; incluye la utilidad guestfish

1.2.3. Ajustes de configuración de Azure VM

Las VM de Azure deben tener los siguientes ajustes de configuración. Algunos de estos ajustes se habilitan durante la creación inicial de la VM. Otros ajustes se establecen cuando se aprovisiona la imagen de la VM para Azure. Tenga en cuenta estos ajustes a medida que avanza en los procedimientos. Consúltelos cuando sea necesario.

Tabla 1.3. Ajustes de configuración de la máquina virtual

Configuración	Recomendación
ssh	ssh debe estar habilitado para proporcionar acceso remoto a sus máquinas virtuales de Azure.

Configuración	Recomendación
dhcp	El adaptador virtual primario debe estar configurado para dhcp (sólo IPv4).
Espacio de intercambio	No cree un archivo de intercambio dedicado o una partición de intercambio. Puede configurar el espacio de intercambio con el agente de Windows Azure Linux (WALinuxAgent).
NIC	Elija **virtio** para el adaptador de red virtual primario.
codificación	Para las imágenes personalizadas, utilice Network Bound Disk Encryption (NBDE) para el cifrado completo del disco en Azure.

1.2.4. Creación de una imagen base a partir de una imagen ISO

El siguiente procedimiento enumera los pasos y requisitos de configuración inicial para crear una imagen ISO personalizada. Una vez que haya configurado la imagen, puede utilizarla como plantilla para crear instancias VM adicionales.

Procedimiento

1. Descargue la última imagen ISO de Red Hat Enterprise Linux 8 Binary DVD desde el Portal del Cliente de Red Hat.
2. Asegúrese de que ha habilitado su máquina anfitriona para la virtualización. Consulte Activación de la virtualización en RHEL 8 para obtener información y procedimientos.
3. Cree e inicie una VM básica de Red Hat Enterprise Linux. Consulte Creación de máquinas virtuales para obtener instrucciones.
    a. Si utiliza la línea de comandos para crear su VM, asegúrese de configurar la memoria y las CPUs por defecto a la capacidad que desea para la VM. Establezca su interfaz de red virtual en **virtio**.
    A continuación se presenta un ejemplo de línea de comandos básica.

    ```
    virt-install --name isotest --memory 2048 --vcpus 2 --disk size=8,bus=virtio --location rhel-8.0-x86_64-dvd.iso --os-variant=rhel8.0
    ```

    b. Si utiliza la consola web para crear su VM, siga el procedimiento en Creación de máquinas virtuales utilizando la consola web, con estas advertencias:
        - No compruebe **Immediately Start VM**.
        - Cambie su **Memory** y **Storage Size** a su configuración preferida.
        - Antes de comenzar la instalación, asegúrese de haber cambiado **Model** en **Virtual Network Interface Settings** a **virtio** y cambie su **vCPUs** a la configuración de capacidad que desee para la VM.

4. Revise la siguiente selección de instalación adicional y las modificaciones.
   - Seleccione **Minimal Install** con la opción **standard RHEL**.
   - Para **Installation Destination**, seleccione **Custom Storage Configuration**. Utilice la siguiente información de configuración para realizar sus selecciones.
     - Verifique al menos 500 MB para **/boot**.
     - Para el sistema de archivos, utilice xfs, ext4 o ext3 para las particiones **boot** y **root**.
     - Eliminar el espacio de intercambio. El espacio de intercambio se configura en el servidor blade físico en Azure por el WALinuxAgent.
   - En la pantalla **Installation Summary**, seleccione **Network and Host Name**. Cambie **Ethernet** por **On**.
5. Cuando se inicia la instalación:
   - Cree una contraseña en **root**.
   - Cree una cuenta de usuario administrativo.
6. Cuando la instalación se haya completado, reinicie la máquina virtual e inicie sesión con la cuenta raíz.
7. Una vez que haya iniciado la sesión como **root**, podrá configurar la imagen.

1.3. CONFIGURACIÓN DE LA IMAGEN BASE PARA MICROSOFT AZURE

La imagen base requiere cambios de configuración para servir como imagen de su VM RHEL 8 en Azure. Las siguientes secciones proporcionan los cambios de configuración adicionales que requiere Azure.

1.3.1. Instalación de los controladores de dispositivos de Hyper-V

Microsoft proporciona controladores de dispositivos de red y de almacenamiento como parte de su paquete de servicios de integración de Linux (LIS) para Hyper-V. Es posible que tenga que instalar los controladores de dispositivos de Hyper-V en la imagen de la VM antes de aprovisionarla como una VM de Azure. Utilice el comando **lsinitrd | grep hv** para verificar que los controladores están instalados.

Procedimiento

1. Introduzca el siguiente comando **grep** para determinar si los controladores de dispositivos Hyper-V necesarios están instalados.

```
# lsinitrd | grep hv
```

   En el ejemplo siguiente, todos los controladores necesarios están instalados.

```
# lsinitrd | grep hv
drwxr-xr-x   2 root     root            0 Aug 12 14:21 usr/lib/modules/3.10.0-
932.el7.x86_64/kernel/drivers/hv
-rw-r--r--   1 root     root        31272 Aug 11 08:45 usr/lib/modules/3.10.0-
932.el7.x86_64/kernel/drivers/hv/hv_vmbus.ko.xz
-rw-r--r--   1 root     root        25132 Aug 11 08:46 usr/lib/modules/3.10.0-
```

```
932.el7.x86_64/kernel/drivers/net/hyperv/hv_netvsc.ko.xz
-rw-r--r--   1 root     root         9796 Aug 11 08:45 usr/lib/modules/3.10.0-
932.el7.x86_64/kernel/drivers/scsi/hv_storvsc.ko.xz
```

Si todos los controladores no están instalados, complete los pasos restantes.

NOTA

Es posible que exista un controlador **hv_vmbus** en el entorno. Incluso si este controlador está presente, complete los siguientes pasos.

2. Cree un archivo llamado **hv.conf** en /**etc**/**dracut.conf.d**.
3. Añada los siguientes parámetros del controlador al archivo **hv.conf**.

```
add_drivers+=" hv_vmbus "
add_drivers+=" hv_netvsc "
add_drivers+=" hv_storvsc "
```

NOTA

Tenga en cuenta los espacios antes y después de las comillas, por ejemplo, **add_drivers =" hv_vmbus "**. Esto asegura que se carguen controladores únicos en el caso de que ya existan otros controladores Hyper-V en el entorno.

4. Regenerar la imagen **initramfs**.

```
# dracut -f -v --regenerate-all
```

Pasos de verificación

1. Reinicie la máquina.
2. Ejecute el comando **lsinitrd | grep hv** para verificar que los controladores están instalados.

1.3.2. Realización de cambios de configuración adicionales

La VM requiere más cambios de configuración para operar en Azure. Realice el siguiente procedimiento para realizar los cambios adicionales.

Procedimiento

1. Si es necesario, encienda la máquina virtual.
2. Registre la VM y habilite el repositorio de Red Hat Enterprise Linux 8.

```
# subscription-manager register --auto-attach
```

Detención y eliminación de cloud-init

1. Detenga el servicio **cloud-init** (si está presente).

```
# systemctl stop cloud-init
```

2. Retire el software **cloud-init**.

```
# yum remove cloud-init
```

Completar otros cambios de la MV

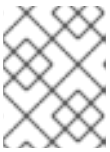
1. Edite el archivo **/etc/ssh/sshd_config** y habilite la autenticación con contraseña.

```
PasswordAuthentication sí
```

2. Establezca un nombre de host genérico.

```
# hostnamectl set-hostname localhost.localdomain
```

3. Edite (o cree) el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0**. Utilice únicamente los parámetros que se indican a continuación.



NOTA

El archivo **ifcfg-eth0** no existe en la imagen ISO del DVD de RHEL 8 y debe ser creado.

```
DEVICE="eth0"
ONBOOT="yes"
BOOTPROTO="dhcp"
TYPE="Ethernet"
USERCTL="yes"
PEERDNS="yes"
IPV6INIT="no"
```

4. Eliminar todas las reglas de dispositivos de red persistentes, si están presentes.

```
# rm -f /etc/udev/rules.d/70-persistent-net.rules
# rm -f /etc/udev/rules.d/75-persistent-net-generator.rules
# rm -f /etc/udev/rules.d/80-net-name-slot-rules
```

5. Configure **ssh** para que se inicie automáticamente.

```
# systemctl enable sshd
# systemctl is-enabled sshd
```

6. Modificar los parámetros de arranque del kernel.

   a. Añada **crashkernel=256M** al principio de la línea **GRUB_CMDLINE_LINUX** en el archivo **/etc/default/grub**. Si **crashkernel=auto** está presente, cámbielo por **crashkernel=256M**.

   b. Añada las siguientes líneas al final de la línea **GRUB_CMDLINE_LINUX**, si no están presentes.

```
earlyprintk=ttyS0
console=ttyS0
rootdelay=300
```

c. Elimine las siguientes opciones, si están presentes.

```
rhgb
quiet
```

7. Regenerar el archivo **grub.cfg**.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

8. Instale y habilite el Agente de Windows Azure Linux (WALinuxAgent). Red Hat Enterprise Linux 8 Application Stream (AppStream) incluye el WALinuxAgent. Consulte Uso de AppStream para obtener más información.

```
# yum install WALinuxAgent -y
# systemctl enable waagent
```

9. Edite las siguientes líneas en el archivo **/etc/waagent.conf** para configurar el espacio de intercambio para las máquinas virtuales provisionadas. Configure el espacio de intercambio para lo que sea apropiado para sus máquinas virtuales aprovisionadas.

```
Provisioning.DeleteRootPassword=n
ResourceDisk.Filesystem=ext4
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048
```

Preparando la provisión

1. Desregistre la VM de Red Hat Subscription Manager.

```
# subscription-manager unregister
```

2. Prepara la VM para el aprovisionamiento de Azure limpiando los detalles de aprovisionamiento existentes. Azure vuelve a aprovisionar la VM en Azure. Este comando genera advertencias, lo cual es de esperar.

```
# waagent -force -deprovision
```

3. Limpia el historial del shell y apaga la VM.

```
# export HISTSIZE=0
# poweroff
```

1.4. CONVERTIR LA IMAGEN A UN FORMATO VHD FIJO

Todas las imágenes de Microsoft Azure VM deben estar en un formato fijo **VHD**. La imagen debe estar alineada en un límite de 1 MB antes de ser convertida a VHD. Esta sección describe cómo convertir la imagen de **qcow2** a un formato fijo de **VHD** y alinear la imagen, si es necesario. Una vez que haya convertido la imagen, puede subirla a Azure.

Procedimiento

1. Convierte la imagen de **qcow2** al formato **raw**.

```
$ qemu-img convert -f qcow2 -O raw <image-name>.qcow2 <image-name>.raw
```

2. Cree un script de shell con el contenido que se indica a continuación.

```
#!/bin/bash
MB=$((1024 * 1024))
size=$(qemu-img info -f raw --output json "$1" | gawk 'match($0, /"virtual-size": ([0-9]+),/, val)
{print val[1]}')
rounded_size=$((($size/$MB + 1) * $MB))
if [ $(($size % $MB)) -eq  0 ]
then
 echo "Your image is already aligned. You do not need to resize."
 exit 1
fi
echo "rounded size = $rounded_size"
export rounded_size
```

3. Ejecute el script. Este ejemplo utiliza el nombre **align.sh**.

```
$ sh align.sh <image-xxx>.raw
```

- Si aparece el mensaje *"Your image is already aligned. You do not need to resize."* , continúe con el siguiente paso.
- Si aparece un valor, su imagen no está alineada.

4. Utilice el siguiente comando para convertir el archivo a un formato fijo **VHD**.
The sample uses qemu-img version 2.12.0.

```
$ qemu-img convert -f raw -o subformat=fixed,force_size -O vpc <image-xxx>.raw
<image.xxx>.vhd
```

Una vez convertido, el archivo **VHD** está listo para subir a Azure.

Aligning the image

Complete los siguientes pasos sólo si el archivo **raw** no está alineado.

1. Cambie el tamaño del archivo **raw** utilizando el valor redondeado que se muestra al ejecutar el script de verificación.

```
$ qemu-img resize -f raw <image-xxx>.raw <rounded-value>
```

2. Convierte el archivo de imagen **raw** a un formato **VHD**.
The sample uses qemu-img version 2.12.0.

```
$ qemu-img convert -f raw -o subformat=fixed,force_size -O vpc <image-xxx>.raw
<image.xxx>.vhd
```

Una vez convertido, el archivo **VHD** está listo para subir a Azure.

1.5. INSTALACIÓN DE LA CLI DE AZURE

Complete los siguientes pasos para instalar la interfaz de línea de comandos de Azure (Azure CLI 2.1). Azure CLI 2.1 es una utilidad basada en Python que crea y gestiona máquinas virtuales en Azure.

Requisitos previos

- Es necesario tener una cuenta en Microsoft Azure para poder utilizar la CLI de Azure.
- La instalación de Azure CLI requiere Python 3.x.

Procedimiento

1. Importe la clave de repositorio de Microsoft.

```
$ sudo rpm --import https://packages.microsoft.com/keys/microsoft.asc
```

2. Cree una entrada en el repositorio local de Azure CLI.

```
$ sudo sh -c 'echo -e \N"[azure-cli]\Nombre=Azure
CLI\nbaseurl=https://packages.microsoft.com/yumrepos/azure-
cli\nenabled=1\ngpgcheck=1\ngpgkey=https://packages.microsoft.com/keys/microsoft.asc" >
/etc/yum.repos.d/azure-cli.repo'
```

3. Actualice el índice de paquetes de **yum**.

```
$ yum check-update
```

4. Compruebe su versión de Python (**python --version**) e instale Python 3.x, si es necesario.

```
$ sudo yum install python3
```

5. Instale la CLI de Azure.

```
$ sudo yum install -y azure-cli
```

6. Ejecute la CLI de Azure.

```
$ az
```

Recursos adicionales

- Azure CLI
- Referencia de comandos de la CLI de Azure

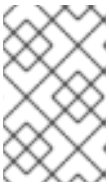
1.6. CREACIÓN DE RECURSOS EN AZURE

Complete el siguiente procedimiento para crear los recursos de Azure que necesita antes de poder cargar el archivo **VHD** y crear la imagen de Azure.

Procedimiento

1. Introduzca el siguiente comando para autenticar su sistema con Azure e iniciar la sesión.

```
$ az login
```



NOTA

Si hay un navegador disponible en su entorno, la CLI abre su navegador a la página de inicio de sesión de Azure. Consulte Iniciar sesión con Azure CLI para obtener más información y opciones.

2. Cree un grupo de recursos en una región de Azure.

```
$ az group create --nombre <grupo de recursos> --ubicación <región>
```

Ejemplo:

```
[clouduser@localhost]$ az group create --name azrhelclirsgrp --location southcentralus
{
  "id": "/subscriptions//resourceGroups/azrhelclirsgrp",
  "location": "southcentralus",
  "managedBy": null,
  "name": "azrhelclirsgrp",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null
}
```

3. Cree una cuenta de almacenamiento. Consulte Tipos de SKU para obtener más información sobre los valores de SKU válidos.

```
$ az storage account create -l <azure-region> -n <storage-account-name> -g <resource-group> --sku <sku_type>
```

Ejemplo:

```
[clouduser@localhost]$ az storage account create -l southcentralus -n azrhelclistact -g azrhelclirsgrp --sku Standard_LRS
{
  "accessTier": null,
  "creationTime": "2017-04-05T19:10:29.855470+00:00",
  "customDomain": null,
  "encryption": null,
  "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Storage/storageAccounts/azrhelclistact",
  "kind": "StorageV2",
  "lastGeoFailoverTime": null,
  "location": "southcentralus",
  "name": "azrhelclistact",
  "primaryEndpoints": {
    "blob": "https://azrhelclistact.blob.core.windows.net/",
    "file": "https://azrhelclistact.file.core.windows.net/",
```

```
    "queue": "https://azrhelclistact.queue.core.windows.net/",
    "table": "https://azrhelclistact.table.core.windows.net/"
},
"primaryLocation": "southcentralus",
"provisioningState": "Succeeded",
"resourceGroup": "azrhelclirsgrp",
"secondaryEndpoints": null,
"secondaryLocation": null,
"sku": {
  "name": "Standard_LRS",
  "tier": "Standard"
},
"statusOfPrimary": "available",
"statusOfSecondary": null,
"tags": {},
  "type": "Microsoft.Storage/storageAccounts"
}
```

4. Obtiene la cadena de conexión de la cuenta de almacenamiento.

```
$ az storage account show-connection-string -n <storage-account-name> -g <resource-
group>
```

Ejemplo:

```
[clouduser@localhost]$ az storage account show-connection-string -n azrhelclistact -g
azrhelclirsgrp
{
  "connectionString":
"DefaultEndpointsProtocol=https;EndpointSuffix=core.windows.net;AccountName=azrhelclistact
AccountKey=NreGk...=="
}
```

5. Exporte la cadena de conexión copiando la cadena de conexión y pegándola en el siguiente comando. Esta cadena conecta su sistema con la cuenta de almacenamiento.

```
$ export AZURE_STORAGE_CONNECTION_STRING="<cadena de conexión de
almacenamiento>"
```

Ejemplo:

```
[clouduser@localhost]$ export
AZURE_STORAGE_CONNECTION_STRING="DefaultEndpointsProtocol=https;EndpointSuffi
x=core.windows.net;AccountName=azrhelclistact;AccountKey=NreGk...=="
```

6. Crear el contenedor de almacenamiento.

```
$ az storage container create -n <nombre-contenedor>
```

Ejemplo:

```
[clouduser@localhost]$ az storage container create -n azrhelclistcont
{
  "created": true
```

```
}
```

7. Crea una red virtual.

```
$ az network vnet create -g <grupo de recursos> -nombre <nombre de la red> -nombre de la subred <nombre de la subred>
```

Ejemplo:

```
[clouduser@localhost]$ az network vnet create --resource-group azrhelclirsgrp --name azrhelclivnet1 --subnet-name azrhelclisubnet1
{
  "newVNet": {
    "addressSpace": {
      "addressPrefixes": [
      "10.0.0.0/16"
      ]
  },
  "dhcpOptions": {
    "dnsServers": []
  },
  "etag": "W/\"\"",
  "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Network/virtualNetworks/azrhelclivnet1",
  "location": "southcentralus",
  "name": "azrhelclivnet1",
  "provisioningState": "Succeeded",
  "resourceGroup": "azrhelclirsgrp",
  "resourceGuid": "0f25efee-e2a6-4abe-a4e9-817061ee1e79",
  "subnets": [
    {
      "addressPrefix": "10.0.0.0/24",
      "etag": "W/\"\"",
      "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Network/virtualNetworks/azrhelclivnet1/subnets/azrhelclisubnet1",
      "ipConfigurations": null,
      "name": "azrhelclisubnet1",
      "networkSecurityGroup": null,
      "provisioningState": "Succeeded",
      "resourceGroup": "azrhelclirsgrp",
      "resourceNavigationLinks": null,
      "routeTable": null
    }
  ],
  "tags": {},
  "type": "Microsoft.Network/virtualNetworks",
  "virtualNetworkPeerings": null
  }
}
```

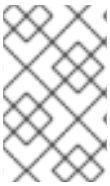
Recursos adicionales

- Visión general de los discos gestionados de Azure

- Tipos de SKU

1.7. CARGA Y CREACIÓN DE UNA IMAGEN DE AZURE

Complete los siguientes pasos para cargar el archivo **VHD** en su contenedor y crear una imagen personalizada de Azure.



NOTA

La cadena de conexión de almacenamiento exportada no persiste después de un reinicio del sistema. Si alguno de los comandos de los siguientes pasos falla, exporte de nuevo la cadena de conexión.

Procedimiento

1. Suba el archivo **VHD** al contenedor de almacenamiento. Puede tardar varios minutos. Para obtener una lista de contenedores de almacenamiento, introduzca el comando **az storage container list**.

```
$ az storage blob upload --account-name <storage-account-name> --container-name
<container-name> --type page --file <path-to-vhd> --name <image-name>.vhd
```

   Ejemplo:

```
[clouduser@localhost]$ az storage blob upload --account-name azrhelclistact --container-
name azrhelclistcont --type page --file rhel-image-8.vhd --name rhel-image-8.vhd
Percent complete: %100.0
```

2. Obtenga la URL del archivo **VHD** cargado para utilizarlo en el siguiente paso.

```
$ az storage blob url -c <nombre-contenedor> -n <nombre-imagen>.vhd
```

   Ejemplo:

```
[clouduser@localhost]$ az storage blob url -c azrhelclistcont -n rhel-image-8.vhd
"https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-8.vhd"
```

3. Cree la imagen personalizada de Azure.

```
$ az image create -n <image-name> -g <resource-group> -l <azure-region> --source <URL>
--os-type linux
```

NOTA

La generación de hipervisor por defecto de la VM es V1. Puede especificar opcionalmente una generación de hipervisor V2 incluyendo la opción **--hyper-v-generation V2**. Las VM de generación 2 utilizan una arquitectura de arranque basada en UEFI. Consulte Soporte para máquinas virtuales de generación 2 en Azure para obtener información sobre las máquinas virtuales de generación 2.

El comando puede devolver el error "Sólo se pueden importar blobs formateados como VHDs" Este error puede significar que la imagen no fue alineada al límite más cercano de 1 MB antes de ser convertida a **VHD**.

Ejemplo:

```
[clouduser@localhost]$ az image create -n rhel8 -g azrhelclirsgrp2 -l southcentralus --source
https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-8.vhd --os-type linux
```

1.8. CREACIÓN E INICIO DE LA VM EN AZURE

Los siguientes pasos proporcionan las opciones mínimas del comando para crear una VM Azure de disco gestionado a partir de la imagen. Consulte az vm create para conocer las opciones adicionales.

Procedimiento

1. Introduzca el siguiente comando para crear la VM.

NOTA

La opción **--generate-ssh-keys** crea un par de claves privadas/públicas. Los archivos de claves privadas y públicas se crean en ~/**.ssh** en su sistema. La clave pública se añade al archivo **authorized_keys** en la VM para el usuario especificado por la opción **--admin-username**. Consulte Otros métodos de autenticación para obtener información adicional.

```
$ az vm create -g <nombre-de-recursos> -l <región> -n <nombre-de-vm> --nombre-de-red
<nombre-de-red> --subred <nombre-de-subred> --size Standard_A2 --os-disk-name
<simple-name> --admin-username <administrator-name> --generate-ssh-keys --image
<path-to-image>
```

Ejemplo:

```
[clouduser@localhost]$ az vm create -g azrhelclirsgrp2 -l southcentralus -n rhel-azure-vm-1 -
-vnet-name azrhelclivnet1 --subnet azrhelclisubnet1  --size Standard_A2 --os-disk-name vm-
1-osdisk --admin-username clouduser --generate-ssh-keys --image rhel8

{
  "fqdns": "",
  "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Compute/virtualMachines/rhe
l-azure-vm-1",
  "location": "southcentralus",
  "macAddress": "",
  "powerState": "VM running",
```

```
    "privateIpAddress": "10.0.0.4",
    "publicIpAddress": "<public-IP-address>",
    "resourceGroup": "azrhelclirsgrp2"
```

Tenga en cuenta la dirección **publicIpAddress**. Necesitará esta dirección para iniciar la sesión en la máquina virtual en el siguiente paso.

2. Inicie una sesión SSH e inicie sesión en la VM.

```
[clouduser@localhost]$ ssh  -i /home/clouduser/.ssh/id_rsa clouduser@<public-IP-address>.
The authenticity of host ',<public-IP-address>' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '<public-IP-address>' (ECDSA) to the list of known hosts.

[clouduser@rhel-azure-vm-1 ~]$
```

Si ve un aviso de usuario, ha desplegado con éxito su VM de Azure.

Ahora puede ir al portal de Microsoft Azure y comprobar los registros de auditoría y las propiedades de sus recursos. Puede gestionar sus máquinas virtuales directamente en este portal. Si está gestionando varias máquinas virtuales, debe utilizar la CLI de Azure. La CLI de Azure proporciona una potente interfaz para sus recursos en Azure. Introduzca **az --help** en la CLI o consulte la referencia de comandos de la CLI de Azure para obtener más información sobre los comandos que utiliza para gestionar sus máquinas virtuales en Microsoft Azure.

1.9. OTROS MÉTODOS DE AUTENTICACIÓN

Aunque se recomienda para aumentar la seguridad, no es necesario utilizar el par de claves generado por Azure. Los siguientes ejemplos muestran dos métodos de autenticación SSH.

Example 1: Estas opciones de comando aprovisionan una nueva VM sin generar un archivo de clave pública. Permiten la autenticación SSH utilizando una contraseña.

```
$ az vm create -g <nombre-del-grupo-de-recursos> -l <nombre-de-la-región> -n <nombre-del-mundo> --nombre-de-la-red <nombre-de-la-red> --subred <nombre-de-la-red> --tamaño-Estándar_A2 --os-disk-name <simple-name> --authentication-type password --admin-username <administrator-name> --admin-password <ssh-password> --image <path-to-image>
```

```
$ ssh <nombre-de-usuario>@<dirección-ip-pública>
```

Example 2: Estas opciones de comando aprovisionan una nueva VM de Azure y permiten la autenticación SSH utilizando un archivo de clave pública existente.

```
$ az vm create -g <nombre-del-grupo-de-recursos> -l <nombre-de-la-región> -n <nombre-del-vm> --nombre-de-la-red <nombre-de-la-red> --subred <nombre-de-la-red> --size Standard_A2 --os-disk-name <simple-name> --admin-username <administrator-name> --ssh-key-value <path-to-existing-ssh-key> --image <path-to-image>
```

```
$ ssh -i <path-to-existing-ssh-key> <admin-username>@<public-ip-address>
```

1.10. ADJUNTAR SUSCRIPCIONES A RED HAT

Complete los siguientes pasos para adjuntar las suscripciones que haya habilitado previamente a través del programa Red Hat Cloud Access.

Requisitos previos

Debe haber activado sus suscripciones.

Procedimiento

1. Registre su sistema.

```
subscription-manager register --auto-attach
```

2. Adjunte sus suscripciones.
   - Puede utilizar una clave de activación para adjuntar suscripciones. Consulte Creación de claves de activación del Portal del Cliente de Red Hat para obtener más información.
   - Como alternativa, puede adjuntar manualmente una suscripción utilizando el ID del grupo de suscripciones (ID del grupo). Consulte Adjuntar y eliminar suscripciones a través de la línea de comandos.

Recursos adicionales

- Creación de claves de activación del Portal del Cliente de Red Hat
- Adjuntar y eliminar suscripciones a través de la línea de comandos
- Uso y configuración de Red Hat Subscription Manager

CAPÍTULO 2. CONFIGURACIÓN DE UN CLÚSTER DE ALTA DISPONIBILIDAD DE RED HAT EN MICROSOFT AZURE

Este capítulo incluye información y procedimientos para configurar un cluster de Alta Disponibilidad (HA) de Red Hat en Azure utilizando instancias de máquinas virtuales (VM) de Azure como nodos de cluster. Los procedimientos en este capítulo asumen que usted está creando una imagen personalizada para Azure. Tiene varias opciones para obtener las imágenes de RHEL 8 que utiliza para su cluster. Consulte Opciones de imagen de Red Hat Enterprise Linux en Azure para obtener información sobre las opciones de imagen para Azure.

Este capítulo incluye los procedimientos necesarios para configurar su entorno para Azure. Una vez que haya configurado su entorno, puede crear y configurar instancias de VM de Azure.

El capítulo también incluye procedimientos específicos para la creación de clústeres de alta disponibilidad, que transforman nodos individuales en un clúster de nodos de alta disponibilidad en Azure. Estos incluyen procedimientos para la instalación de los paquetes y agentes de alta disponibilidad en cada nodo del clúster, la configuración del cercado y la instalación de los agentes de recursos de red de Azure.

El capítulo hace referencia a la documentación de Azure en varios lugares. Para muchos procedimientos, consulte la documentación de Azure a la que se hace referencia para obtener más información.

Requisitos previos

- Regístrese para obtener una cuenta en el Portal del Cliente de Red Hat.
- Regístrese en una cuenta de Microsoft Azure con privilegios de administrador.
- Es necesario instalar la interfaz de línea de comandos (CLI) de Azure. Para obtener más información, consulte Sección 1.5, “Instalación de la CLI de Azure” .
- Habilite sus suscripciones en el programa Red Hat Cloud Access. El programa Red Hat Cloud Access le permite trasladar sus suscripciones de Red Hat desde sistemas físicos o locales a Azure con el apoyo total de Red Hat.

Recursos adicionales

- Políticas de soporte para clústeres de alta disponibilidad de RHEL - Máquinas virtuales de Microsoft Azure como miembros del clúster
- Configuración y gestión de clusters de alta disponibilidad

2.1. CREACIÓN DE RECURSOS EN AZURE

Complete el siguiente procedimiento para crear una región, un grupo de recursos, una cuenta de almacenamiento, una red virtual y un conjunto de disponibilidad. Necesitará estos recursos para completar las tareas posteriores de este capítulo.

Procedimiento

1. Autentifique su sistema con Azure e inicie sesión.

```
$ az login
```

NOTA

Si hay un navegador disponible en su entorno, la CLI abre su navegador a la página de inicio de sesión de Azure.

Ejemplo:

```
[clouduser@localhost]$ az login
To sign in, use a web browser to open the page https://aka.ms/devicelogin and enter the code
FDMSCMETZ to authenticate.
 [
  {
   "cloudName": "AzureCloud",
   "id": "Subscription ID",
   "isDefault": true,
   "name": "MySubscriptionName",
   "state": "Enabled",
   "tenantId": "Tenant ID",
   "user": {
    "name": "clouduser@company.com",
    "type": "user"
   }
  }
 ]
```

2. Cree un grupo de recursos en una región de Azure.

```
$ az group create --name resource-group --location azure-region
```

Ejemplo:

```
[clouduser@localhost]$ az group create --name azrhelclirsgrp --location southcentralus
{
 "id": "/subscriptions//resourceGroups/azrhelclirsgrp",
 "location": "southcentralus",
 "managedBy": null,
 "name": "azrhelclirsgrp",
 "properties": {
  "provisioningState": "Succeeded"
 },
 "tags": null
}
```

3. Crea una cuenta de almacenamiento.

```
$ az storage account create -l azure-region -n storage-account-name -g resource-group --
sku sku_type --kind StorageV2
```

Ejemplo:

```
[clouduser@localhost]$ az storage account create -l southcentralus -n azrhelclistact -g
azrhelclirsgrp --sku Standard_LRS --kind StorageV2
{
 "accessTier": null,
```

```
  "creationTime": "2017-04-05T19:10:29.855470+00:00",
  "customDomain": null,
  "encryption": null,
  "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Storage/storageAccounts/azr
helclistact",
  "kind": "StorageV2",
  "lastGeoFailoverTime": null,
  "location": "southcentralus",
  "name": "azrhelclistact",
  "primaryEndpoints": {
    "blob": "https://azrhelclistact.blob.core.windows.net/",
    "file": "https://azrhelclistact.file.core.windows.net/",
    "queue": "https://azrhelclistact.queue.core.windows.net/",
    "table": "https://azrhelclistact.table.core.windows.net/"
},
"primaryLocation": "southcentralus",
"provisioningState": "Succeeded",
"resourceGroup": "azrhelclirsgrp",
"secondaryEndpoints": null,
"secondaryLocation": null,
"sku": {
  "name": "Standard_LRS",
  "tier": "Standard"
},
"statusOfPrimary": "available",
"statusOfSecondary": null,
"tags": {},
  "type": "Microsoft.Storage/storageAccounts"
}
```


4. Obtiene la cadena de conexión de la cuenta de almacenamiento.

```
$ az storage account show-connection-string -n storage-account-name -g resource-group
```

Ejemplo:


```
[clouduser@localhost]$ az storage account show-connection-string -n azrhelclistact -g
azrhelclirsgrp
{
  "connectionString":
"DefaultEndpointsProtocol=https;EndpointSuffix=core.windows.net;AccountName=azrhelclistact
AccountKey=NreGk...=="
}
```


5. Exporte la cadena de conexión copiando la cadena de conexión y pegándola en el siguiente comando. Esta cadena conecta su sistema con la cuenta de almacenamiento.

```
$ export AZURE_STORAGE_CONNECTION_STRING="storage-connection-string"
```

Ejemplo:

```
[clouduser@localhost]$ export
AZURE_STORAGE_CONNECTION_STRING="DefaultEndpointsProtocol=https;EndpointSuffi
x=core.windows.net;AccountName=azrhelclistact;AccountKey=NreGk...=="
```

6. Crear el contenedor de almacenamiento.

```
$ az storage container create -n container-name
```

Ejemplo:

```
[clouduser@localhost]$ az storage container create -n azrhelclistcont
{
  "created": true
}
```

7. Cree una red virtual. Todos los nodos del clúster deben estar en la misma red virtual.

```
$ az network vnet create -g resource group --name vnet-name --subnet-name subnet-name
```

Ejemplo:

```
[clouduser@localhost]$ az network vnet create --resource-group azrhelclirsgrp --name
azrhelclivnet1 --subnet-name azrhelclisubnet1
{
  "newVNet": {
    "addressSpace": {
      "addressPrefixes": [
      "10.0.0.0/16"
      ]
  },
  "dhcpOptions": {
    "dnsServers": []
  },
  "etag": "W/\"\"",
  "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Network/virtualNetworks/azr
helclivnet1",
  "location": "southcentralus",
  "name": "azrhelclivnet1",
  "provisioningState": "Succeeded",
  "resourceGroup": "azrhelclirsgrp",
  "resourceGuid": "0f25efee-e2a6-4abe-a4e9-817061ee1e79",
  "subnets": [
    {
      "addressPrefix": "10.0.0.0/24",
      "etag": "W/\"\"",
      "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Network/virtualNetworks/azr
helclivnet1/subnets/azrhelclisubnet1",
      "ipConfigurations": null,
      "name": "azrhelclisubnet1",
      "networkSecurityGroup": null,
      "provisioningState": "Succeeded",
      "resourceGroup": "azrhelclirsgrp",
```

```
      "resourceNavigationLinks": null,
      "routeTable": null
    }
  ],
  "tags": {},
  "type": "Microsoft.Network/virtualNetworks",
  "virtualNetworkPeerings": null
  }
}
```

8. Cree un conjunto de disponibilidad. Todos los nodos del clúster deben estar en el mismo conjunto de disponibilidad.

```
$ az vm availability-set create --name MyAvailabilitySet --resource-group MyResourceGroup
```

Ejemplo:

```
[clouduser@localhost]$ az vm availability-set create --name rhelha-avset1 --resource-group
azrhelclirsgrp
{
  "additionalProperties": {},
    "id":
"/subscriptions/.../resourceGroups/azrhelclirsgrp/providers/Microsoft.Compute/availabilitySets/rh
elha-avset1",
    "location": "southcentralus",
    "name": “rhelha-avset1",
    "platformFaultDomainCount": 2,
    "platformUpdateDomainCount": 5,

...omitted
```

Recursos adicionales

- Iniciar sesión con Azure CLI
- Tipos de SKU
- Visión general de los discos gestionados de Azure

2.2. PAQUETES DE SISTEMA NECESARIOS PARA LA ALTA DISPONIBILIDAD

El procedimiento asume que está creando una imagen de VM para Azure HA usando Red Hat Enterprise Linux. Para completar con éxito el procedimiento, los siguientes paquetes deben ser instalados.

Tabla 2.1. Paquetes del sistema

Paquete	Repositorio	Descripción
libvirt	rhel-8-for-x86_64-appstream-rpms	API, demonio y herramienta de gestión de código abierto para gestionar la virtualización de plataformas

Paquete	Repositorio	Descripción
virt-install	rhel-8-for-x86_64-appstream-rpms	Una utilidad de línea de comandos para crear máquinas virtuales
libguestfs	rhel-8-for-x86_64-appstream-rpms	Una biblioteca para acceder y modificar los sistemas de archivos de las máquinas virtuales
libguestfs-tools	rhel-8-for-x86_64-appstream-rpms	Herramientas de administración del sistema para máquinas virtuales; incluye la utilidad guestfish

2.3. AJUSTES DE CONFIGURACIÓN DE AZURE VM

Las VM de Azure deben tener los siguientes ajustes de configuración. Algunos de estos ajustes se habilitan durante la creación inicial de la VM. Otros ajustes se establecen cuando se aprovisiona la imagen de la VM para Azure. Tenga en cuenta estos ajustes a medida que avanza en los procedimientos. Consúltelos cuando sea necesario.

Tabla 2.2. Ajustes de configuración de la máquina virtual

Configuración	Recomendación
ssh	ssh debe estar habilitado para proporcionar acceso remoto a sus máquinas virtuales de Azure.
dhcp	El adaptador virtual primario debe estar configurado para dhcp (sólo IPv4).
Espacio de intercambio	No cree un archivo de intercambio dedicado o una partición de intercambio. Puede configurar el espacio de intercambio con el agente de Windows Azure Linux (WALinuxAgent).
NIC	Elija **virtio** para el adaptador de red virtual primario.
codificación	Para las imágenes personalizadas, utilice Network Bound Disk Encryption (NBDE) para el cifrado completo del disco en Azure.

2.4. INSTALACIÓN DE LOS CONTROLADORES DE DISPOSITIVOS DE HYPER-V

Microsoft proporciona controladores de dispositivos de red y de almacenamiento como parte de su paquete de servicios de integración de Linux (LIS) para Hyper-V. Es posible que tenga que instalar los controladores de dispositivos de Hyper-V en la imagen de la VM antes de aprovisionarla como una VM

de Azure. Utilice el comando **lsinitrd | grep hv** para verificar que los controladores están instalados.

Procedimiento

1. Introduzca el siguiente comando **grep** para determinar si los controladores de dispositivos Hyper-V necesarios están instalados.

```
# lsinitrd | grep hv
```

En el ejemplo siguiente, todos los controladores necesarios están instalados.

```
# lsinitrd | grep hv
drwxr-xr-x   2 root     root            0 Aug 12 14:21 usr/lib/modules/3.10.0-
932.el7.x86_64/kernel/drivers/hv
-rw-r--r--   1 root     root        31272 Aug 11 08:45 usr/lib/modules/3.10.0-
932.el7.x86_64/kernel/drivers/hv/hv_vmbus.ko.xz
-rw-r--r--   1 root     root        25132 Aug 11 08:46 usr/lib/modules/3.10.0-
932.el7.x86_64/kernel/drivers/net/hyperv/hv_netvsc.ko.xz
-rw-r--r--   1 root     root         9796 Aug 11 08:45 usr/lib/modules/3.10.0-
932.el7.x86_64/kernel/drivers/scsi/hv_storvsc.ko.xz
```

Si todos los controladores no están instalados, complete los pasos restantes.

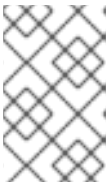
NOTA

Es posible que exista un controlador **hv_vmbus** en el entorno. Incluso si este controlador está presente, complete los siguientes pasos.

2. Cree un archivo llamado **hv.conf** en **/etc/dracut.conf.d**.

3. Añada los siguientes parámetros del controlador al archivo **hv.conf**.

```
add_drivers+=" hv_vmbus "
add_drivers+=" hv_netvsc "
add_drivers+=" hv_storvsc "
```



NOTA

Tenga en cuenta los espacios antes y después de las comillas, por ejemplo, **add_drivers =" hv_vmbus "**. Esto asegura que se carguen controladores únicos en el caso de que ya existan otros controladores Hyper-V en el entorno.

4. Regenerar la imagen **initramfs**.

```
# dracut -f -v --regenerate-all
```

Pasos de verificación

1. Reinicie la máquina.

2. Ejecute el comando **lsinitrd | grep hv** para verificar que los controladores están instalados.

2.5. REALIZACIÓN DE CAMBIOS DE CONFIGURACIÓN ADICIONALES

La VM requiere más cambios de configuración para operar en Azure. Realice el siguiente procedimiento para realizar los cambios adicionales.

Procedimiento

1. Si es necesario, encienda la máquina virtual.
2. Registre la VM y habilite el repositorio de Red Hat Enterprise Linux 8.

```
# subscription-manager register --auto-attach
```

Detención y eliminación de cloud-init

1. Detenga el servicio **cloud-init** (si está presente).

```
# systemctl stop cloud-init
```

2. Retire el software **cloud-init**.

```
# yum remove cloud-init
```

Completar otros cambios de la MV

1. Edite el archivo **/etc/ssh/sshd_config** y habilite la autenticación con contraseña.

```
PasswordAuthentication sí
```

2. Establezca un nombre de host genérico.

```
# hostnamectl set-hostname localhost.localdomain
```

3. Edite (o cree) el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0**. Utilice únicamente los parámetros que se indican a continuación.

NOTA

El archivo **ifcfg-eth0** no existe en la imagen ISO del DVD de RHEL 8 y debe ser creado.

```
DEVICE="eth0"
ONBOOT="yes"
BOOTPROTO="dhcp"
TYPE="Ethernet"
USERCTL="yes"
PEERDNS="yes"
IPV6INIT="no"
```

4. Eliminar todas las reglas de dispositivos de red persistentes, si están presentes.

```
# rm -f /etc/udev/rules.d/70-persistent-net.rules
# rm -f /etc/udev/rules.d/75-persistent-net-generator.rules
# rm -f /etc/udev/rules.d/80-net-name-slot-rules
```

5. Configure **ssh** para que se inicie automáticamente.

```
# systemctl enable sshd
# systemctl is-enabled sshd
```

6. Modificar los parámetros de arranque del kernel.

   a. Añada **crashkernel=256M** al principio de la línea **GRUB_CMDLINE_LINUX** en el archivo **/etc/default/grub**. Si **crashkernel=auto** está presente, cámbielo por **crashkernel=256M**.

   b. Añada las siguientes líneas al final de la línea **GRUB_CMDLINE_LINUX**, si no están presentes.

```
earlyprintk=ttyS0
console=ttyS0
rootdelay=300
```

   c. Elimine las siguientes opciones, si están presentes.

```
rhgb
quiet
```

7. Regenerar el archivo **grub.cfg**.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

8. Instale y habilite el Agente de Windows Azure Linux (WALinuxAgent). Red Hat Enterprise Linux 8 Application Stream (AppStream) incluye el WALinuxAgent. Consulte Uso de AppStream para obtener más información.

```
# yum install WALinuxAgent -y
# systemctl enable waagent
```

9. Edite las siguientes líneas en el archivo **/etc/waagent.conf** para configurar el espacio de intercambio para las máquinas virtuales provisionadas. Configure el espacio de intercambio para lo que sea apropiado para sus máquinas virtuales aprovisionadas.

```
Provisioning.DeleteRootPassword=n
ResourceDisk.Filesystem=ext4
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048
```

Preparando la provisión

1. Desregistre la VM de Red Hat Subscription Manager.

```
# subscription-manager unregister
```

2. Prepara la VM para el aprovisionamiento de Azure limpiando los detalles de aprovisionamiento existentes. Azure vuelve a aprovisionar la VM en Azure. Este comando genera advertencias, lo cual es de esperar.

```
# waagent -force -deprovision
```

3. Limpia el historial del shell y apaga la VM.

```
# export HISTSIZE=0
# poweroff
```

2.6. CREACIÓN DE UNA APLICACIÓN DE AZURE ACTIVE DIRECTORY

Complete el siguiente procedimiento para crear una aplicación Azure AD. La aplicación Azure AD autoriza y automatiza el acceso a las operaciones de HA para todos los nodos del clúster.

Requisitos previos

Instale la interfaz de línea de comandos (CLI) de Azure .

Procedimiento

1. Asegúrese de que es administrador o propietario de la suscripción de Microsoft Azure. Necesita esta autorización para crear una aplicación de Azure AD.

2. Inicie sesión en su cuenta de Azure.

```
$ az login
```

3. Introduzca el siguiente comando para crear la aplicación Azure AD. Para utilizar su propia contraseña, añada la opción **--password** al comando. Asegúrese de crear una contraseña fuerte.

```
$ az ad sp create-for-rbac --name FencingApplicationName --role owner --scopes
"/subscriptions/SubscriptionID/resourceGroups/MyResourseGroup"
```

Ejemplo:

```
[clouduser@localhost ~] $ az ad sp create-for-rbac --name FencingApp --role owner --
scopes "/subscriptions/2586c64b-xxxxxx-xxxxxxx-xxxxxxx/resourceGroups/azrhelclirsgrp"
Retrying role assignment creation: 1/36
Retrying role assignment creation: 2/36
Retrying role assignment creation: 3/36
{
  "appId": "1a3dfe06-df55-42ad-937b-326d1c211739",
  "displayName": "FencingApp",
  "name": "http://FencingApp",
  "password": "43a603f0-64bb-482e-800d-402efe5f3d47",
  "tenant": "77ecefb6-xxxxxxxxxx-xxxxxxx-757a69cb9485"
}
```

4. Guarde la siguiente información antes de continuar. Necesita esta información para configurar el agente de cercado.

   - ID de aplicación de Azure AD

- Contraseña de la aplicación Azure AD
- Identificación del inquilino
- ID de suscripción a Microsoft Azure

Recursos adicionales

Ver el acceso que tiene un usuario a los recursos de Azure

2.7. CONVERTIR LA IMAGEN A UN FORMATO VHD FIJO

Todas las imágenes de Microsoft Azure VM deben estar en un formato fijo **VHD**. La imagen debe estar alineada en un límite de 1 MB antes de ser convertida a VHD. Esta sección describe cómo convertir la imagen de **qcow2** a un formato fijo de **VHD** y alinear la imagen, si es necesario. Una vez que haya convertido la imagen, puede subirla a Azure.

Procedimiento

1. Convierte la imagen de **qcow2** al formato **raw**.

```
$ qemu-img convert -f qcow2 -O raw <image-name>.qcow2 <image-name>.raw
```

2. Cree un script de shell con el contenido que se indica a continuación.

```
#!/bin/bash
MB=$((1024 * 1024))
size=$(qemu-img info -f raw --output json "$1" | gawk 'match($0, /"virtual-size": ([0-9]+),/, val)
{print val[1]}')
rounded_size=$((($size/$MB + 1) * $MB))
if [ $(($size % $MB)) -eq  0 ]
then
 echo "Your image is already aligned. You do not need to resize."
 exit 1
fi
echo "rounded size = $rounded_size"
export rounded_size
```

3. Ejecute el script. Este ejemplo utiliza el nombre **align.sh**.

```
$ sh align.sh <image-xxx>.raw
```

- Si aparece el mensaje *"Your image is already aligned. You do not need to resize."* , continúe con el siguiente paso.
- Si aparece un valor, su imagen no está alineada.

4. Utilice el siguiente comando para convertir el archivo a un formato fijo **VHD**.
The sample uses qemu-img version 2.12.0.

```
$ qemu-img convert -f raw -o subformat=fixed,force_size -O vpc <image-xxx>.raw
<image.xxx>.vhd
```

Una vez convertido, el archivo **VHD** está listo para subir a Azure.

Aligning the image

Complete los siguientes pasos sólo si el archivo **raw** no está alineado.

1. Cambie el tamaño del archivo **raw** utilizando el valor redondeado que se muestra al ejecutar el script de verificación.

```
$ qemu-img resize -f raw <image-xxx>.raw <rounded-value>
```

2. Convierte el archivo de imagen **raw** a un formato **VHD**.
The sample uses qemu-img version 2.12.0.

```
$ qemu-img convert -f raw -o subformat=fixed,force_size -O vpc <image-xxx>.raw
<image.xxx>.vhd
```

Una vez convertido, el archivo **VHD** está listo para subir a Azure.

2.8. CARGA Y CREACIÓN DE UNA IMAGEN DE AZURE

Complete los siguientes pasos para cargar el archivo **VHD** en su contenedor y crear una imagen personalizada de Azure.

NOTA

La cadena de conexión de almacenamiento exportada no persiste después de un reinicio del sistema. Si alguno de los comandos de los siguientes pasos falla, exporte de nuevo la cadena de conexión.

Procedimiento

1. Suba el archivo **VHD** al contenedor de almacenamiento. Puede tardar varios minutos. Para obtener una lista de contenedores de almacenamiento, introduzca el comando **az storage container list**.

```
$ az storage blob upload --account-name <storage-account-name> --container-name
<container-name> --type page --file <path-to-vhd> --name <image-name>.vhd
```

Ejemplo:

```
[clouduser@localhost]$ az storage blob upload --account-name azrhelclistact --container-
name azrhelclistcont --type page --file rhel-image-8.vhd --name rhel-image-8.vhd
Percent complete: %100.0
```

2. Obtenga la URL del archivo **VHD** cargado para utilizarlo en el siguiente paso.

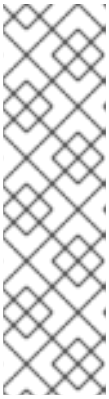
```
$ az storage blob url -c <nombre-contenedor> -n <nombre-imagen>.vhd
```

Ejemplo:

```
[clouduser@localhost]$ az storage blob url -c azrhelclistcont -n rhel-image-8.vhd
"https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-8.vhd"
```

3. Cree la imagen personalizada de Azure.

```
$ az image create -n <image-name> -g <resource-group> -l <azure-region> --source <URL>
--os-type linux
```



NOTA

La generación de hipervisor por defecto de la VM es V1. Puede especificar opcionalmente una generación de hipervisor V2 incluyendo la opción **--hyper-v-generation V2**. Las VM de generación 2 utilizan una arquitectura de arranque basada en UEFI. Consulte Soporte para máquinas virtuales de generación 2 en Azure para obtener información sobre las máquinas virtuales de generación 2.

El comando puede devolver el error "Sólo se pueden importar blobs formateados como VHDs" Este error puede significar que la imagen no fue alineada al límite más cercano de 1 MB antes de ser convertida a **VHD**.

Ejemplo:

```
[clouduser@localhost]$ az image create -n rhel8 -g azrhelclirsgrp2 -l southcentralus --source
https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-8.vhd --os-type linux
```

2.9. INSTALACIÓN DE PAQUETES Y AGENTES DE RED HAT HA

Complete los siguientes pasos en todos los nodos.

Procedimiento

1. Inicie una sesión de terminal SSH y conéctese a la máquina virtual utilizando el nombre del administrador y la dirección IP pública.

```
$ ssh administrator@PublicIP
```

Para obtener la dirección IP pública de una VM de Azure, abra las propiedades de la VM en el Portal de Azure o introduzca el siguiente comando de la CLI de Azure.

```
$ az vm list -g <grupo de recursos> -d --tabla de salida
```

Ejemplo:

```
[clouduser@localhost ~] $ az vm list -g azrhelclirsgrp -d --output table
Name    ResourceGroup          PowerState      PublicIps       Location
------  ---------------------  --------------  -------------   --------------
node01  azrhelclirsgrp         VM running      192.98.152.251  southcentralus
```

2. Registre la VM con Red Hat.

```
$ sudo -i
# subscription-manager register --auto-attach
```

NOTA

Si el comando **--auto-attach** falla, registre manualmente la VM en su suscripción.

3. Desactivar todos los repositorios.

```
# subscription-manager repos --disable=*
```

4. Habilite los repositorios de RHEL 8 Server y RHEL 8 Server HA.

```
# subscription-manager repos --enable=rhel-8-server-rpms
# subscription-manager repos --enable=rhel-ha-for-rhel-8-server-rpms
```

5. Actualice todos los paquetes.

```
# yum update -y
```

6. Instale los paquetes de software Red Hat High Availability Add-On, junto con todos los agentes de cercado disponibles en el canal de Alta Disponibilidad.

```
# yum install pcs pacemaker fence-agents-azure-arm
```

7. El usuario **hacluster** fue creado durante la instalación de pcs y pacemaker en el paso anterior. Cree una contraseña para **hacluster** en todos los nodos del clúster. Utilice la misma contraseña para todos los nodos.

```
# passwd hacluster
```

8. Añada el servicio **high availability** al cortafuegos de RHEL si está instalado **firewalld.service**.

```
# firewall-cmd --permanent --add-service=high-availability
# firewall-cmd --reload
```

9. Inicie el servicio **pcs** y permita que se inicie en el arranque.

```
# systemctl start pcsd.service
# systemctl enable pcsd.service

Created symlink from /etc/systemd/system/multi-user.target.wants/pcsd.service to
/usr/lib/systemd/system/pcsd.service.
```

Paso de verificación

Asegúrese de que el servicio **pcs** está funcionando.

```
# systemctl status pcsd.service
pcsd.service - PCS GUI and remote configuration interface
Loaded: loaded (/usr/lib/systemd/system/pcsd.service; enabled; vendor preset: disabled)
Active: active (running) since Fri 2018-02-23 11:00:58 EST; 1min 23s ago
Docs: man:pcsd(8)
        man:pcs(8)
```

```
Main PID: 46235 (pcsd)
  CGroup: /system.slice/pcsd.service
          └─46235 /usr/bin/ruby /usr/lib/pcsd/pcsd > /dev/null &
```

2.10. CREACIÓN DE UN CLÚSTER

Complete los siguientes pasos para crear el cluster de nodos.

Procedimiento

1. En uno de los nodos, introduzca el siguiente comando para autenticar al usuario pcs **hacluster**. En el comando, especifique el nombre de cada nodo del clúster.

```
# pcs host auth  hostname1 hostname2 hostname3
Username: hacluster
Password:
hostname1: Authorized
hostname2: Authorized
hostname3: Authorized
```

   Ejemplo:

```
[root@node01 clouduser]# pcs host auth node01 node02 node03
Username: hacluster
Password:
node01: Authorized
node02: Authorized
node03: Authorized
```

2. Crea el clúster.

```
# pcs cluster setup cluster-name hostname1 hostname2 hostname3
```

   Ejemplo:

```
[root@node01 clouduser]# pcs cluster setup --name newcluster node01 node02 node03

...omitted

Synchronizing pcsd certificates on nodes node01, node02, node03...
node02: Success
node03: Success
node01: Success
Restarting pcsd on the nodes in order to reload the certificates...
node02: Success
node03: Success
node01: Success
```

Pasos de verificación

1. Habilitar el clúster.

```
root@node01 clouduser]# pcs cluster enable --all
```

2. Poner en marcha el clúster.

```
[root@node01 clouduser]# pcs cluster start --all
```

Ejemplo:

```
[root@node01 clouduser]# pcs cluster enable --all
node02: Cluster Enabled
node03: Cluster Enabled
node01: Cluster Enabled

[root@node01 clouduser]# pcs cluster start --all
node02: Starting Cluster...
node03: Starting Cluster...
node01: Starting Cluster...
```

2.11. VISIÓN GENERAL DE LA ESGRIMA

Si la comunicación con un solo nodo del clúster falla, los demás nodos del clúster deben ser capaces de restringir o liberar el acceso a los recursos a los que el nodo del clúster que ha fallado pueda tener acceso. Esto no puede lograrse contactando con el propio nodo del clúster, ya que éste puede no responder. En su lugar, debe proporcionar un método externo, que se llama fencing con un agente de fencing.

Un nodo que no responde puede seguir accediendo a los datos. La única manera de estar seguro de que sus datos están a salvo es cercar el nodo utilizando STONITH. STONITH es un acrónimo de "Shoot The Other Node In The Head" (Disparar al otro nodo en la cabeza) y protege sus datos de la corrupción de nodos deshonestos o del acceso concurrente. Utilizando STONITH, puede estar seguro de que un nodo está realmente desconectado antes de permitir que se acceda a los datos desde otro nodo.

Recursos adicionales

Esgrima en Red Hat High Availability Cluster

2.12. CREACIÓN DE UN DISPOSITIVO DE ESGRIMA

Complete los siguientes pasos para configurar el cercado. Complete estos comandos desde cualquier nodo del clúster

Requisitos previos

Es necesario establecer la propiedad del clúster **stonith-enabled** en **true**.

Procedimiento

1. Identifique el nombre del nodo Azure para cada VM RHEL. Utilice los nombres de nodo de Azure para configurar el dispositivo de valla.

```
fence_azure_arm -l AD-Application-ID -p AD-Password --resourceGroup MyResourceGroup --tenantId Tenant-ID --subscriptionId Subscription-ID -o list
```

Ejemplo:

```
[root@node01 clouduser]# fence_azure_arm -l e04a6a49-9f00-xxxx-xxxx-a8bdda4af447 -p
```

```
z/a05AwCN0IzAjVwXXXXXXXEWIoeVp0xg7QT//JE= --resourceGroup azrhelclirsgrp --
tenantId 77ecefb6-cff0-XXXX-XXXX-757XXXX9485 --subscriptionId XXXXXXXX-38b4-4527-
XXXX-012d49dfc02c -o list
node01,
node02,
node03,
```

2. Vea las opciones del agente Azure ARM STONITH.

```
pcs stonith describe fence_azure_arm
```

Ejemplo:

```
# pass:quotes[pcs stonith describe fence_apc]
Stonith options:
password: Authentication key
password_script: Script to run to retrieve password
```

AVISO

Para los agentes de la valla que proporcionan una opción de método, no especifique un valor de ciclo, ya que no es compatible y puede causar la corrupción de datos.

Algunos dispositivos de cercado sólo pueden cercar un único nodo, mientras que otros dispositivos pueden cercar varios nodos. Los parámetros que se especifican al crear un dispositivo de vallado dependen de lo que el dispositivo de vallado admita y requiera.

Puede utilizar el parámetro **pcmk_host_list** al crear un dispositivo de cercado para especificar todas las máquinas que están controladas por ese dispositivo de cercado.

Puede utilizar el parámetro **pcmk_host_map** al crear un dispositivo de vallado para asignar nombres de host a las especificaciones que comprende el dispositivo de vallado.

3. Crea un dispositivo de vallas.

```
# pcs stonith create clusterfence fence_azure_arm
```

4. Pruebe el agente de esgrima para uno de los otros nodos.

```
# pcs stonith fence azurenodename
```

Ejemplo:

```
[root@node01 clouduser]# pcs status
Cluster name: newcluster
Stack: corosync
Current DC: node01 (version 1.1.18-11.el7-2b07d5c5a9) - partition with quorum
Last updated: Fri Feb 23 11:44:35 2018
```

```
Last change: Fri Feb 23 11:21:01 2018 by root via cibadmin on node01

3 nodes configured
1 resource configured

Online: [ node01 node03 ]
OFFLINE: [ node02 ]

Full list of resources:

 clusterfence  (stonith:fence_azure_arm):  Started node01

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

5. Inicie el nodo que fue cercado en el paso anterior.

```
# pcs cluster start hostname
```

6. Comprueba el estado para verificar que el nodo se ha iniciado.

```
# estado de las pcs
```

Ejemplo:

```
[root@node01 clouduser]# pcs status
Cluster name: newcluster
Stack: corosync
Current DC: node01 (version 1.1.18-11.el7-2b07d5c5a9) - partition with quorum
Last updated: Fri Feb 23 11:34:59 2018
Last change: Fri Feb 23 11:21:01 2018 by root via cibadmin on node01

3 nodes configured
1 resource configured

Online: [ node01 node02 node03 ]

Full list of resources:

clusterfence    (stonith:fence_azure_arm):  Started node01

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

Recursos adicionales

- Esgrima en un cluster de alta disponibilidad de Red Hat
- Propiedades generales de los dispositivos de esgrima

2.13. CREACIÓN DE UN EQUILIBRADOR DE CARGA INTERNO DE AZURE

El equilibrador de carga interno de Azure elimina los nodos del clúster que no responden a las solicitudes de sondeo de salud.

Realice el siguiente procedimiento para crear un equilibrador de carga interno de Azure. Cada paso hace referencia a un procedimiento específico de Microsoft e incluye la configuración para personalizar el equilibrador de carga para HA.

Requisitos previos

Panel de control Azure

Procedimiento

1. Creeun equilibrador de carga básico . Seleccione **Internal load balancer**, el **Basic SKU**, y **Dynamic** para el tipo de asignación de direcciones IP.

2. Creeun pool de direcciones back -end. Asocie el pool de backend al conjunto de disponibilidad creado al crear los recursos de Azure en HA. No establezca ninguna configuración de IP de red de destino.

3. Cree una sonda de salud. Para la sonda de salud, seleccione **TCP** e introduzca el puerto **61000**. Puede utilizar un número de puerto TCP que no interfiera con otro servicio. Para determinadas aplicaciones de productos de HA (por ejemplo, SAP HANA y SQL Server), es posible que tenga que trabajar con Microsoft para identificar el puerto correcto que debe utilizar.

4. Creeuna regla de equilibrio de carga. Para crear la regla de balanceo de carga, los valores por defecto están pre-rellenados. Asegúrese de establecer **Floating IP (direct server return)** en **Enabled**.

2.14. CONFIGURACIÓN DEL AGENTE DE RECURSOS DEL EQUILIBRADOR DE CARGA

Después de crear la sonda de salud, debe configurar el agente de recursos **load balancer**. Este agente de recursos ejecuta un servicio que responde a las solicitudes de sonda de salud del equilibrador de carga de Azure y elimina los nodos del clúster que no responden a las solicitudes.

Procedimiento

1. Instale los agentes de recursos de **nmap-ncat** en todos los nodos.

```
# yum install nmap-ncat resource-agents
```

   Realice los siguientes pasos en un solo nodo.

2. Cree los recursos y el grupo **pcs**. Utilice su FrontendIP del equilibrador de carga para la dirección IPaddr2.

```
# pcs resource create resource-name IPaddr2 ip="10.0.0.7" --grupo cluster-resources-group
```

3. Configure el agente de recursos **load balancer**.

```
# pcs resource create resource-loadbalancer-name azure-lb port=port-number --group
cluster-resources-group
```

Paso de verificación

Ejecute **pcs status** para ver los resultados.

```
[root@node01 clouduser]# pcs status
```

Ejemplo:

```
Cluster name: clusterfence01
Stack: corosync
Current DC: node02 (version 1.1.16-12.el7_4.7-94ff4df) - partition with quorum
Last updated: Tue Jan 30 12:42:35 2018
Last change: Tue Jan 30 12:26:42 2018 by root via cibadmin on node01

3 nodes configured
3 resources configured

Online: [ node01 node02 node03 ]

Full list of resources:

clusterfence (stonith:fence_azure_arm):      Started node01
Resource Group: g_azure
    vip_azure  (ocf::heartbeat:IPaddr2):       Started node02
    lb_azure   (ocf::heartbeat:azure-lb):      Started node02

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

2.15. CONFIGURACIÓN DEL ALMACENAMIENTO EN BLOQUE COMPARTIDO

Esta sección proporciona un procedimiento opcional para configurar el almacenamiento de bloques compartido para un clúster de alta disponibilidad de Red Hat con discos compartidos de Microsoft Azure. El procedimiento asume tres VMs de Azure (un cluster de tres nodos) con un disco compartido de 1 TB.

NOTA

Este es un procedimiento de ejemplo independiente para configurar el almacenamiento en bloque. El procedimiento asume que aún no ha creado su clúster.

Requisitos previos

- Debe haber instalado la CLI de Azure en su sistema anfitrión y haber creado su(s) clave(s) SSH.
- Debe haber creado su entorno de clúster en Azure, lo que incluye la creación de los siguientes recursos. Los enlaces son a la documentación de Microsoft Azure.

- Grupo de recursos
- Red virtual
- Grupo(s) de seguridad de la red
- Reglas del grupo de seguridad de la red
- Subred(es)
- Equilibrador de carga (opcional)
- Cuenta de almacenamiento
- Grupo de colocación de proximidad
- Conjunto de disponibilidad

Procedimiento

1. Crear un volumen de bloques compartido mediante el comando Azure **az disk create**.

```
$ az disk create -g <resource_group> -n <shared_block_volume_name> --size-gb
<disk_size> --max-shares <number_vms> -l <location>
```

Por ejemplo, el siguiente comando crea un volumen de bloques compartido llamado **shared-block-volume.vhd** en el grupo de recursos **sharedblock** dentro de la zona de disponibilidad de Azure **westcentralus**.

```
$ az disk create -g sharedblock-rg -n shared-block-volume.vhd --size-gb 1024 --max-shares
3 -l westcentralus

{
  "creationData": {
    "createOption": "Empty",
    "galleryImageReference": null,
    "imageReference": null,
    "sourceResourceId": null,
    "sourceUniqueId": null,
    "sourceUri": null,
    "storageAccountId": null,
    "uploadSizeBytes": null
  },
  "diskAccessId": null,
  "diskIopsReadOnly": null,
  "diskIopsReadWrite": 5000,
  "diskMbpsReadOnly": null,
  "diskMbpsReadWrite": 200,
  "diskSizeBytes": 1099511627776,
  "diskSizeGb": 1024,
  "diskState": "Unattached",
  "encryption": {
    "diskEncryptionSetId": null,
    "type": "EncryptionAtRestWithPlatformKey"
  },
  "encryptionSettingsCollection": null,
```

```
  "hyperVgeneration": "V1",
  "id": "/subscriptions/12345678910-12345678910/resourceGroups/sharedblock-
rg/providers/Microsoft.Compute/disks/shared-block-volume.vhd",
  "location": "westcentralus",
  "managedBy": null,
  "managedByExtended": null,
  "maxShares": 3,
  "name": "shared-block-volume.vhd",
  "networkAccessPolicy": "AllowAll",
  "osType": null,
  "provisioningState": "Succeeded",
  "resourceGroup": "sharedblock-rg",
  "shareInfo": null,
  "sku": {
    "name": "Premium_LRS",
    "tier": "Premium"
  },
  "tags": {},
  "timeCreated": "2020-08-27T15:36:56.263382+00:00",
  "type": "Microsoft.Compute/disks",
  "uniqueId": "cd8b0a25-6fbe-4779-9312-8d9cbb89b6f2",
  "zones": null
}
```


2. Compruebe que ha creado el volumen de bloques compartido mediante el comando Azure **az disk show**.

```
$ az disk show -g <grupo_de_recursos> -n <nombre_de_bloque_compartido>
```

Por ejemplo, el siguiente comando muestra los detalles del volumen de bloques compartido **shared-block-volume.vhd** dentro del grupo de recursos **sharedblock-rg**.

```
$ az disk show -g sharedblock-rg -n shared-block-volume.vhd

{
  "creationData": {
    "createOption": "Empty",
    "galleryImageReference": null,
    "imageReference": null,
    "sourceResourceId": null,
    "sourceUniqueId": null,
    "sourceUri": null,
    "storageAccountId": null,
    "uploadSizeBytes": null
  },
  "diskAccessId": null,
  "diskIopsReadOnly": null,
  "diskIopsReadWrite": 5000,
  "diskMbpsReadOnly": null,
  "diskMbpsReadWrite": 200,
  "diskSizeBytes": 1099511627776,
  "diskSizeGb": 1024,
  "diskState": "Unattached",
  "encryption": {
    "diskEncryptionSetId": null,
```

```
    "type": "EncryptionAtRestWithPlatformKey"
  },
  "encryptionSettingsCollection": null,
  "hyperVgeneration": "V1",
  "id": "/subscriptions/12345678910-12345678910/resourceGroups/sharedblock-
rg/providers/Microsoft.Compute/disks/shared-block-volume.vhd",
  "location": "westcentralus",
  "managedBy": null,
  "managedByExtended": null,
  "maxShares": 3,
  "name": "shared-block-volume.vhd",
  "networkAccessPolicy": "AllowAll",
  "osType": null,
  "provisioningState": "Succeeded",
  "resourceGroup": "sharedblock-rg",
  "shareInfo": null,
  "sku": {
    "name": "Premium_LRS",
    "tier": "Premium"
  },
  "tags": {},
  "timeCreated": "2020-08-27T15:36:56.263382+00:00",
  "type": "Microsoft.Compute/disks",
  "uniqueId": "cd8b0a25-6fbe-4779-9312-8d9cbb89b6f2",
  "zones": null
}
```


3. Crear tres interfaces de red con el comando Azure **az network nic create**. Ejecute el siguiente comando tres veces utilizando un **<nic_name>** diferente para cada uno.

```
az network nic create -g <resource_group> -n <nic_name> --subnet <subnet_name> --vnet-
name <virtual_network> --location <location> --network-security-group
<network_security_group> --private-ip-address-version IPv4
```

Por ejemplo, el siguiente comando crea una interfaz de red con el nombre **shareblock-nodea-vm-nic-protected**.

```
$ az network nic create -g sharedblock-rg -n sharedblock-nodea-vm-nic-protected --subnet
sharedblock-subnet-protected --vnet-name sharedblock-vn --location westcentralus --
network-security-group sharedblock-nsg --private-ip-address-version IPv4
```

4. Cree tres máquinas virtuales y adjunte el volumen de bloques compartido mediante el comando Azure **az vm create**. Los valores de las opciones son los mismos para cada VM excepto que cada VM tiene su propio **<vm_name>**, **<new_vm_disk_name>**, y **<nic_name>**.

```
az vm create -n <nombre_del_móvil> -g <grupo_de_recursos> --attach-data-disks
<nombre_del_volumen_de_bloques_compartidos> --data-disk-caching None --os-disk-
caching ReadWrite --os-disk-name <new-vm-disk-name> --os-disk-size-gb <disk_size> --
location <location> --size <virtual_machine_size> --image <image_name> --admin-
username <vm_username> --authentication-type ssh --ssh-key-values <ssh_key> --nics
<nic_name> --availability-set <availability_set> --ppg <proximity_placement_group>
```

Por ejemplo, el siguiente comando crea una VM llamada **sharedblock-nodea-vm**.

```
$ az vm create -n sharedblock-nodea-vm -g sharedblock-rg --attach-data-disks shared-
block-volume.vhd --data-disk-caching None --os-disk-caching ReadWrite --os-disk-name
sharedblock-nodea-vm.vhd --os-disk-size-gb 64 --location westcentralus --size
Standard_D2s_v3 --image /subscriptions/12345678910-
12345678910/resourceGroups/sample-
azureimagesgroupwestcentralus/providers/Microsoft.Compute/images/sample-azure-rhel-
8.3.0-20200713.n.0.x86_64 --admin-username sharedblock-user --authentication-type ssh --
ssh-key-values @sharedblock-key.pub --nics sharedblock-nodea-vm-nic-protected --
availability-set sharedblock-as --ppg sharedblock-ppg

{
  "fqdns": "",
  "id": "/subscriptions/12345678910-12345678910/resourceGroups/sharedblock-
rg/providers/Microsoft.Compute/virtualMachines/sharedblock-nodea-vm",
  "location": "westcentralus",
  "macAddress": "00-22-48-5D-EE-FB",
  "powerState": "VM running",
  "privateIpAddress": "198.51.100.3",
  "publicIpAddress": "",
  "resourceGroup": "sharedblock-rg",
  "zones": ""
}
```

Pasos de verificación

1. Para cada una de las máquinas virtuales de su clúster, verifique que el dispositivo de bloque está disponible utilizando el comando **ssh** con su máquina virtual **<ip_address>**.

```
# ssh <ip_address> "hostname ; lsblk -d | grep ' 1T '"
```

Por ejemplo, el siguiente comando enumera los detalles, incluyendo el nombre del host y el dispositivo de bloque para la IP de la VM **198.51.100.3**.

```
# ssh 198.51.100.3 "hostname ; lsblk -d | grep ' 1T '"

nodea
sdb    8:16   0    1T  0 disk
```

2. Utilice el comando **ssh** para verificar que cada máquina virtual de su clúster utiliza el mismo disco compartido.

```
# ssh <ip_address> "hostname ; lsblk -d | grep ' 1T ' | awk '{print \$1}' | xargs -i udevadm info
--query=all --name=/dev/{} | grep '^E: ID_SERIAL='"
```

Por ejemplo, el siguiente comando enumera los detalles, incluyendo el nombre del host y el ID del volumen de disco compartido para la dirección IP de la instancia **198.51.100.3**.

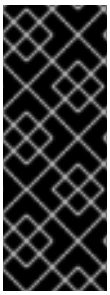
```
# ssh 198.51.100.3 "hostname ; lsblk -d | grep ' 1T ' | awk '{print \$1}' | xargs -i udevadm info -
-query=all --name=/dev/{} | grep '^E: ID_SERIAL='"

nodea
E: ID_SERIAL=3600224808dd8eb102f6ffc5822c41d89
```

Después de haber verificado que el disco compartido está conectado a cada VM, puede configurar el almacenamiento resistente para el cluster. Para obtener información sobre la configuración del almacenamiento resistente para un cluster de Alta Disponibilidad de Red Hat, consulte Configuración de un sistema de archivos GFS2 en un cl uster. Para obtener información general sobre el sistema de archivos GFS2, consulte Configuración de sistemas de archivos GFS2 .

CAPÍTULO 3. IMPLANTACIÓN DE UNA IMAGEN DE RED HAT ENTERPRISE LINUX COMO INSTANCIA EC2 EN AMAZON WEB SERVICES

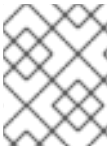
Tiene varias opciones para implementar una imagen de Red Hat Enterprise Linux (RHEL) 8 como una instancia EC2 en Amazon Web Services (AWS). Este capítulo discute sus opciones para elegir una imagen y enumera o se refiere a los requisitos del sistema para su sistema anfitrión y máquina virtual (VM). Este capítulo también proporciona procedimientos para crear una VM personalizada a partir de una imagen ISO, subirla a EC2 y lanzar una instancia EC2.



IMPORTANTE

Aunque puede crear una VM personalizada a partir de una imagen ISO, Red Hat recomienda que utilice el producto Red Hat Image Builder para crear imágenes personalizadas para su uso en proveedores de nube específicos. Con Image Builder, puede crear y cargar una imagen de máquina de Amazon (AMI) en el formato **ami**. Consulte Composición de una imagen de sistema RHEL personalizada para obtener más información.

Este capítulo hace referencia a la documentación de Amazon en varios lugares. Para muchos procedimientos, consulte la documentación de Amazon a la que se hace referencia para obtener más detalles.



NOTA

Para obtener una lista de los productos de Red Hat que puede utilizar de forma segura en AWS, consulte Red Hat en Amazon Web Services .

Requisitos previos

- Regístrese para obtener una cuenta en el Portal del Cliente de Red Hat.
- Regístrese en AWS y configure sus recursos de AWS. Consulte Configuración con Amazon EC2 para obtener más información.
- Habilite sus suscripciones en el programa Red Hat Cloud Access. El programa Red Hat Cloud Access le permite trasladar sus suscripciones de Red Hat desde sistemas físicos o locales a AWS con el apoyo total de Red Hat.

Recursos adicionales

- Guía de referencia de Red Hat Cloud Access
- Red Hat en la nube pública
- Red Hat Enterprise Linux en Amazon EC2 - Preguntas frecuentes
- Configuración con Amazon EC2
- Red Hat en Amazon Web Services

3.1. OPCIONES DE IMAGEN DE RED HAT ENTERPRISE LINUX EN AWS

La siguiente tabla enumera las opciones de imagen y señala las diferencias entre ellas.

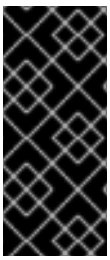
Tabla 3.1. Opciones de imagen

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones
Elija implementar una imagen de Red Hat Gold.	Aproveche sus suscripciones existentes a Red Hat.	Habilite las suscripciones a través del programa Red Hat Cloud Access y, a continuación, elija una Red Hat Gold Image en AWS.	La suscripción incluye el coste del producto de Red Hat; el resto de los costes de las instancias se pagan a Amazon. Las imágenes Red Hat Gold se denominan imágenes "Cloud Access" porque aprovechan sus suscripciones existentes a Red Hat. Red Hat proporciona soporte directamente para las imágenes de Cloud Access.
Elija desplegar una imagen personalizada que traslade a AWS.	Aproveche sus suscripciones existentes a Red Hat.	Habilite las suscripciones a través del programa Red Hat Cloud Access, cargue su imagen personalizada y adjunte sus suscripciones.	La suscripción incluye el coste del producto de Red Hat; el resto de los costes de las instancias se pagan a Amazon. Las imágenes personalizadas que traslada a AWS son imágenes de "Acceso a la nube" porque aprovecha sus suscripciones existentes a Red Hat. Red Hat proporciona soporte directamente para las imágenes de Cloud Access.

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones
Elija desplegar una imagen de Amazon existente que incluya RHEL.	Las imágenes de AWS EC2 incluyen un producto de Red Hat.	Elija una imagen de RHEL cuando lance una instancia en la consola de administración de AWS o elija una imagen de AWS Marketplace.	Usted paga a Amazon por hora en un modelo de pago por uso. Estas imágenes se denominan imágenes "a la carta". Amazon ofrece soporte para las imágenes bajo demanda. Red Hat proporciona las actualizaciones de las imágenes. AWS hace que las actualizaciones estén disponibles a través de Red Hat Update Infrastructure (RHUI).

NOTA

Puede crear una imagen personalizada para AWS utilizando Red Hat Image Builder. Consulte Composición de una imagen del sistema RHEL personalizada para obtener más información.



IMPORTANTE

No se puede convertir una instancia bajo demanda en una instancia de Red Hat Cloud Access. Para cambiar de una imagen bajo demanda a una imagen de Red Hat Cloud Access de suscripción propia (BYOS), cree una nueva instancia de Red Hat Cloud Access y migre los datos de su instancia bajo demanda. Cancele su instancia bajo demanda después de migrar sus datos para evitar la doble facturación.

El resto de este capítulo incluye información y procedimientos relativos a las imágenes personalizadas.

Recursos adicionales

- Programa Red Hat Cloud Access
- Cómo componer una imagen de sistema RHEL personalizada
- Consola de administración de AWS
- AWS Marketplace

3.2. COMPRENDER LAS IMÁGENES BASE

Esta sección incluye información sobre el uso de imágenes base preconfiguradas y sus ajustes de configuración.

3.2.1. Utilizar una imagen base personalizada

Para configurar manualmente una VM, se empieza con una imagen de VM base (de inicio). Una vez creada la imagen de la VM base, puede modificar los ajustes de configuración y añadir los paquetes que la VM necesita para funcionar en la nube. Puede realizar cambios de configuración adicionales para su aplicación específica después de cargar la imagen.

Recursos adicionales

Red Hat Enterprise Linux

3.2.2. Ajustes de configuración de la máquina virtual

Las VM de la nube deben tener los siguientes ajustes de configuración.

Tabla 3.2. Ajustes de configuración de la máquina virtual

Configuración	Recomendación
ssh	ssh debe estar habilitado para proporcionar acceso remoto a sus máquinas virtuales.
dhcp	El adaptador virtual primario debe estar configurado para dhcp.

3.3. CREACIÓN DE UNA VM BASE A PARTIR DE UNA IMAGEN ISO

Siga los procedimientos de esta sección para crear una imagen base a partir de una imagen ISO.

Requisitos previos

Habilite la virtualización para su máquina anfitriona Red Hat Enterprise Linux 8.

3.3.1. Descarga de la imagen ISO

Procedimiento

1. Descargue la última imagen ISO de Red Hat Enterprise Linux desde el Portal del Cliente de Red Hat.
2. Mueve la imagen a **/var/lib/libvirt/images**.

3.3.2. Creación de una VM a partir de la imagen ISO

Procedimiento

1. Asegúrese de que ha habilitado su máquina anfitriona para la virtualización. Consulte Activación de la virtualización en RHEL 8 para obtener información y procedimientos.
2. Cree e inicie una VM básica de Red Hat Enterprise Linux. Consulte Creación de máquinas virtuales para obtener instrucciones.

a. Si utiliza la línea de comandos para crear su VM, asegúrese de configurar la memoria y las CPUs por defecto a la capacidad que desea para la VM. Establezca su interfaz de red virtual en **virtio**.
A continuación, un ejemplo básico de línea de comandos.

```
virt-install --name isotest --memory 2048 --vcpus 2 --disk size=8,bus=virtio --location
rhel-8.0-x86_64-dvd.iso --os-variant=rhel8.0
```

b. Si utiliza la consola web para crear su VM, siga el procedimiento en Creación de máquinas virtuales utilizando la consola web, con estas advertencias:

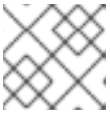
- No compruebe **Immediately Start VM**.
- Cambie su **Memory** y **Storage Size** a su configuración preferida.
- Antes de comenzar la instalación, asegúrese de haber cambiado **Model** en **Virtual Network Interface Settings** a **virtio** y cambie su **vCPUs** a la configuración de capacidad que desee para la VM.

3.3.3. Completar la instalación de RHEL

Realice los siguientes pasos para completar la instalación y para habilitar el acceso de root una vez que se inicie la VM.

Procedimiento

1. Elija el idioma que desea utilizar durante el proceso de instalación.
2. En la vista **Installation Summary**:
   a. Haga clic en **Software Selection** y marque **Minimal Install**.
   b. Haga clic en **Done**.
   c. Haga clic en **Installation Destination** y marque **Custom** en **Storage Configuration**.
      - Verifique al menos 500 MB para /**boot**. Puede utilizar el espacio restante para la raíz /.
      - Se recomiendan las particiones estándar, pero se puede utilizar Logical Volume Management (LVM).
      - Puedes usar xfs, ext4 o ext3 para el sistema de archivos.
      - Haga clic en **Done** cuando haya terminado con los cambios.
3. Haga clic en **Begin Installation**.
4. Establezca un **Root Password**. Cree otros usuarios según corresponda.
5. Reinicie la máquina virtual e inicie sesión como **root** una vez que la instalación se haya completado.
6. Configurar la imagen.



NOTA

Asegúrese de que el paquete **cloud-init** está instalado y habilitado.

7. **Important: This step is only for VMs you intend to upload to AWS.**

   a. Para las máquinas virtuales x86, instale los controladores **nvme**, **xen-netfront** y **xen-blkfront**.

   ```
   # dracut -f --add-drivers \ "nvme xen-netfront xen-blkfront"
   ```

   b. Para las máquinas virtuales aarch64, instale el controlador **nvme**.

   ```
   # dracut -f --add-drivers \ "nvme"
   ```

   La inclusión de estos controladores elimina la posibilidad de que se produzca un tiempo muerto de draconiano.

   También puede añadir los controladores a **/etc/dracut.conf.d/** y luego introducir **dracut -f** para sobrescribir el archivo existente **initramfs**.

8. Apague la máquina virtual.

3.4. CARGA DE LA IMAGEN DE RED HAT ENTERPRISE LINUX EN AWS

Sigue los procedimientos de esta sección para subir tu imagen a AWS.

3.4.1. Instalación de la CLI de AWS

Muchos de los procedimientos de este capítulo incluyen el uso de la CLI de AWS. Complete los siguientes pasos para instalar la CLI de AWS.

Requisitos previos

Necesita haber creado y tener acceso a un ID de clave de acceso de AWS y a una clave de acceso secreta de AWS. Consulte Configuración rápida de la CLI de AWS para obtener información e instrucciones.

Procedimiento

1. Instale Python 3 y la herramienta **pip**.

```
# yum install python3
# yum install python3-pip
```

2. Instale las herramientas de línea de comandos de AWS con el comando **pip**.

```
# pip3 install awscli
```

3. Ejecute el comando **aws --version** para verificar que ha instalado la CLI de AWS.

```
$ aws --version
aws-cli/1.16.182 Python/2.7.5 Linux/3.10.0-957.21.3.el7.x86_64 botocore/1.12.172
```

4. Configure el cliente de línea de comandos de AWS según sus datos de acceso a AWS.

```
$ aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]:
```

Recursos adicionales

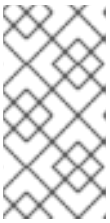
- Configuración rápida de la CLI de AWS
- Herramientas de línea de comandos de AWS

3.4.2. Creación de un bucket S3

La importación a AWS requiere un bucket de Amazon S3. Un cubo de Amazon S3 es un recurso de Amazon en el que se almacenan objetos. Como parte del proceso de carga de su imagen, debe crear un bucket de S3 y luego mover su imagen al bucket. Complete los siguientes pasos para crear un cubo.

Procedimiento

1. Inicie la consola de Amazon S3 .
2. Haga clic en **Create Bucket**. Aparece el cuadro de diálogo **Create Bucket**.
3. En la vista **Name and region**:
   a. Introduzca un **Bucket name**.
   b. Introduzca un **Region**.
   c. Haga clic en **Next**.
4. En la vista **Configure options**, seleccione las opciones deseadas y haga clic en **Next**.
5. En la vista **Set permissions**, cambie o acepte las opciones por defecto y haga clic en **Next**.
6. Revise la configuración de su cubo.
7. Haga clic en **Create bucket**.



NOTA

También puede utilizar la CLI de AWS para crear un cubo. Por ejemplo, el comando **aws s3 mb s3://my-new-bucket** crea un bucket de S3 denominado **my-new-bucket**. Consulte la Referencia de comandos de la CLI de AWS para obtener más información sobre el comando **mb**.

Recursos adicionales

- Consola de Amazon S3
- Referencia de comandos de la CLI de AWS

3.4.3. Creación del rol vmimport

Realice el siguiente procedimiento para crear el rol **vmimport**, que es necesario para la importación de VM. Consulta el rol de servicio de importación de VM en la documentación de Amazon para obtener más información.

Procedimiento

1. Cree un archivo llamado **trust-policy.json** e incluya la siguiente política. Guarde el archivo en su sistema y anote su ubicación.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
            }
         }
      }
   ]
}
```

2. Utilice el comando **create role** para crear el rol **vmimport**. Especifique la ruta completa a la ubicación del archivo **trust-policy.json**. Añada el prefijo **file://** a la ruta. A continuación se muestra un ejemplo.

```
aws iam create-role --role-name vmimport --assume-role-policy-document
file:///home/sample/ImportService/trust-policy.json
```

3. Crea un archivo llamado **role-policy.json** e incluye la siguiente política. Sustituye **s3-bucket-name** por el nombre de tu bucket de S3.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::s3-bucket-name",
            "arn:aws:s3:::s3-bucket-name/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
```

```
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
        ],
        "Resource":"*"
    }
  ]
}
```

4. Utilice el comando **put-role-policy** para adjuntar la política al rol que ha creado. Especifique la ruta completa del archivo **role-policy.json**. A continuación se muestra un ejemplo.

```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file:///home/sample/ImportService/role-policy.json
```

Recursos adicionales

- Función del servicio de importación de máquinas virtuales
- Función de servicio requerida

3.4.4. Conversión y envío de la imagen a S3

Complete el siguiente procedimiento para convertir y enviar su imagen a S3. Los ejemplos son representativos; convierten una imagen formateada en el formato de archivo **qcow2** al formato **raw**. Amazon acepta imágenes en los formatos **OVA**, **VHD**, **VHDX**, **VMDK** y **raw**. Consulte Cómo funciona la importación/exportación de VM para obtener más información sobre los formatos de imagen que acepta Amazon.

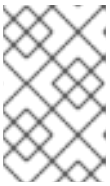
Procedimiento

1. Ejecute el comando **qemu-img** para convertir su imagen. A continuación se muestra un ejemplo.

```
qemu-img convert -f qcow2 -O raw rhel-8.2-sample.qcow2 rhel-8.2-sample.raw
```

2. Empuje la imagen a S3.

```
aws s3 cp rhel-8.2-sample.raw s3://s3-bucket-name
```



NOTA

Este procedimiento puede tardar unos minutos. Una vez completado, puede comprobar que su imagen se ha cargado correctamente en su cubo de S3 utilizando la consola de AWS S3 .

Recursos adicionales

- Cómo funciona la importación/exportación de máquinas virtuales
- Consola de AWS S3

3.4.5. Importar la imagen como una instantánea

Realice el siguiente procedimiento para importar una imagen como instantánea.

Procedimiento

1. Cree un archivo para especificar un cubo y una ruta para su imagen. Nombra el archivo **containers.json**. En el ejemplo que sigue, sustituye **s3-bucket-name** por el nombre de tu cubo y **s3-key** por tu clave. Puedes obtener la clave de la imagen mediante la consola de Amazon S3.

```
{
    "Description": "rhel-8.2-sample.raw",
    "Format": "raw",
    "UserBucket": {
        "S3Bucket": "s3-bucket-name",
        "S3Key": "s3-key"
    }
}
```

2. Importe la imagen como una instantánea. Este ejemplo utiliza un archivo público de Amazon S3; puede utilizar la consola de Amazon S3 para cambiar la configuración de los permisos en su bucket.

```
aws ec2 import-snapshot --disk-container file://containers.json
```

El terminal muestra un mensaje como el siguiente. Observe el **ImportTaskID** dentro del mensaje.

```
{
    "SnapshotTaskDetail": {
        "Status": "active",
        "Format": "RAW",
        "DiskImageSize": 0.0,
        "UserBucket": {
            "S3Bucket": "s3-bucket-name",
            "S3Key": "rhel-8.2-sample.raw"
        },
        "Progress": "3",
        "StatusMessage": "pending"
    },
    "ImportTaskId": "import-snap-06cea01fa0f1166a8"
}
```

3. Siga el progreso de la importación utilizando el comando **describe-import-snapshot-tasks**. Incluya el comando **ImportTaskID**.

```
aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-06cea01fa0f1166a8
```

El mensaje devuelto muestra el estado actual de la tarea. Cuando se completa, **Status** muestra **completed**. Dentro del estado, anote el ID de la instantánea.

Recursos adicionales

- Consola de Amazon S3

- Importación de un disco como una instantánea utilizando VM Import/Export

3.4.6. Creación de una AMI a partir de la instantánea cargada

En EC2, debe elegir una imagen de máquina de Amazon (AMI) al lanzar una instancia. Realice el siguiente procedimiento para crear una AMI a partir de su instantánea cargada.

Procedimiento

1. Vaya al panel de control de AWS EC2.
2. En **Elastic Block Store**, seleccione **Snapshots**.
3. Busque su ID de instantánea (por ejemplo, **snap-0e718930bd72bcda0**).
4. Haga clic con el botón derecho del ratón en la instantánea y seleccione **Create image**.
5. Nombra tu imagen.
6. En **Virtualization type**, seleccione **Hardware-assisted virtualization**.
7. Haga clic en **Create**. En la nota relativa a la creación de imágenes, hay un enlace a su imagen.
8. Haz clic en el enlace de la imagen. Su imagen aparece en **Images>AMIs**.

NOTA

Como alternativa, puede utilizar el comando de la CLI de AWS **register-image** para crear una AMI a partir de una instantánea. Consulte register-image para obtener más información. A continuación se muestra un ejemplo.

```
$ aws ec2 register-image --name "myimagename" --description
"myimagedescription" --architecture x86_64  --virtualization-type hvm --root-
device-name "/dev/sda1" --block-device-mappings "{\"DeviceName\":
\"/dev/sda1\",\"Ebs\": {\"SnapshotId\": \"snap-0ce7f009b69ab274d\"}}" --ena-
support
```

Debe especificar el volumen de dispositivo raíz **/dev/sda1** como su **root-device-name**. Para obtener información conceptual sobre la asignación de dispositivos para AWS, consulte Ejemplo de asignación de dispositivos de bloque .

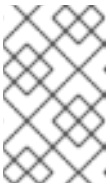
3.4.7. Lanzamiento de una instancia desde la AMI

Realice el siguiente procedimiento para lanzar y configurar una instancia desde la AMI.

Procedimiento

1. En el panel de control de AWS EC2, seleccione **Images** y luego **AMIs**.
2. Haga clic con el botón derecho del ratón en su imagen y seleccione **Launch**.
3. Elija un **Instance Type** que cumpla o supere los requisitos de su carga de trabajo. Consulte Tipos de instancias de Amazon EC2 para obtener información sobre los tipos de instancias.

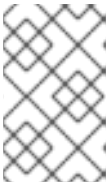
4. Haga clic en **Next: Configure Instance Details**.
   a. Introduzca la dirección **Number of instances** que desea crear.
   b. En **Network**, seleccione la VPC que creó al configurar su entorno de AWS . Seleccione una subred para la instancia o cree una nueva subred.
   c. Seleccione **Enable** para la autoasignación de la IP pública.



NOTA

Estas son las opciones de configuración mínimas necesarias para crear una instancia básica. Revise las opciones adicionales en función de los requisitos de su aplicación.

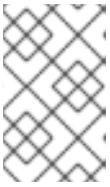
5. Haga clic en **Next: Add Storage**. Compruebe que el almacenamiento por defecto es suficiente.
6. Haga clic en **Next: Add Tags**.



NOTA

Las etiquetas pueden ayudarle a administrar sus recursos de AWS. Consulte Etiquetado de sus recursos de Amazon EC2 para obtener información sobre el etiquetado.

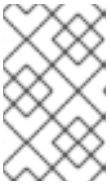
7. Haga clic en **Next: Configure Security Group**. Seleccione el grupo de seguridad que creó al configurar su entorno AWS .
8. Haga clic en **Review and Launch**. Verifique sus selecciones.
9. Haga clic en **Launch**. Se le pedirá que seleccione un par de claves existente o que cree un nuevo par de claves. Seleccione el par de claves que creó al configurar su entorno de AWS .



NOTA

Comprueba que los permisos de tu clave privada son correctos. Utiliza las opciones del comando **chmod 400 <keyname>.pem** para cambiar los permisos, si es necesario.

10. Haga clic en **Launch Instances**.
11. Haga clic en **View Instances**. Puede nombrar la(s) instancia(s).
    Ahora puede iniciar una sesión SSH en su(s) instancia(s) seleccionando una instancia y haciendo clic en **Connect**. Utilice el ejemplo proporcionado para **A standalone SSH client**.



NOTA

También puede lanzar una instancia utilizando la CLI de AWS. Consulte Lanzamiento, listado y finalización de instancias de Amazon EC2 en la documentación de Amazon para obtener más información.

Recursos adicionales

- Consola de administración de AWS

- Configuración con Amazon EC2
- Instancias de Amazon EC2
- Tipos de instancias de Amazon EC2

3.4.8. Adjuntar suscripciones a Red Hat

Complete los siguientes pasos para adjuntar las suscripciones que haya habilitado previamente a través del programa Red Hat Cloud Access.

Requisitos previos

Debe haber activado sus suscripciones.

Procedimiento

1. Registre su sistema.

```
subscription-manager register --auto-attach
```

2. Adjunte sus suscripciones.
   - Puede utilizar una clave de activación para adjuntar suscripciones. Consulte Creación de claves de activación del Portal del Cliente de Red Hat para obtener más información.
   - Como alternativa, puede adjuntar manualmente una suscripción utilizando el ID del grupo de suscripciones (ID del grupo). Consulte Adjuntar y eliminar suscripciones a través de la línea de comandos.

Recursos adicionales

- Creación de claves de activación del Portal del Cliente de Red Hat
- Adjuntar y eliminar suscripciones a través de la línea de comandos
- Uso y configuración de Red Hat Subscription Manager

CAPÍTULO 4. CONFIGURACIÓN DE UN CLÚSTER DE ALTA DISPONIBILIDAD DE RED HAT EN AWS

Este capítulo incluye información y procedimientos para configurar un cluster de Alta Disponibilidad (HA) de Red Hat en Amazon Web Services (AWS) utilizando instancias EC2 como nodos de cluster. Tenga en cuenta que tiene varias opciones para obtener las imágenes de Red Hat Enterprise Linux (RHEL) que utiliza para su cluster. Para obtener información sobre las opciones de imagen para AWS, consulte Opciones de imagen de Red Hat Enterprise Linux en AWS .

Este capítulo incluye los procedimientos necesarios para configurar su entorno para AWS. Una vez que haya configurado su entorno, puede crear y configurar instancias EC2.

Este capítulo también incluye procedimientos específicos para la creación de clústeres de HA, que transforman nodos individuales en un clúster de nodos de HA en AWS. Estos incluyen procedimientos para instalar los paquetes y agentes de alta disponibilidad en cada nodo del clúster, configurar el cercado e instalar los agentes de recursos de red de AWS.

El capítulo hace referencia a la documentación de Amazon en varios lugares. Para muchos procedimientos, consulte la documentación de Amazon a la que se hace referencia para obtener más información.

Requisitos previos

- Regístrese para obtener una cuenta en el Portal del Cliente de Red Hat.
- Regístrese en AWS y configure sus recursos de AWS. Consulte Configuración con Amazon EC2 para obtener más información.
- Habilite sus suscripciones en el programa Red Hat Cloud Access. El programa Red Hat Cloud Access le permite trasladar sus suscripciones de Red Hat desde sistemas físicos o locales a AWS con el apoyo total de Red Hat.

Recursos adicionales

- Guía de referencia de Red Hat Cloud Access
- Red Hat en la nube pública
- Red Hat Enterprise Linux en Amazon EC2 - Preguntas frecuentes
- Configuración con Amazon EC2
- Red Hat en Amazon Web Services

4.1. CREACIÓN DE LA CLAVE DE ACCESO DE AWS Y DE LA CLAVE DE ACCESO SECRETA DE AWS

Debe crear una clave de acceso de AWS y una clave de acceso secreta de AWS antes de instalar la CLI de AWS. Las API del agente de recursos y de fencing utilizan la clave de acceso de AWS y la clave de acceso secreta para conectarse a cada nodo del clúster.

Complete los siguientes pasos para crear estas claves.

Requisitos previos

Su cuenta de usuario IAM debe tener acceso programático. Consulte Configuración del entorno de AWS para obtener más información.

Procedimiento

1. Inicie la consola de AWS .
2. Haga clic en su ID de cuenta de AWS para que aparezca el menú desplegable y seleccione **My Security Credentials**.
3. Haga clic en **Users**.
4. Seleccione el usuario y abra la pantalla **Summary**.
5. Haga clic en la pestaña **Security credentials**.
6. Haga clic en **Create access key**.
7. Descargue el archivo **.csv** (o guarde ambas claves). Deberá introducir estas claves al crear el dispositivo de esgrima.

4.2. INSTALACIÓN DE LA CLI DE AWS

Muchos de los procedimientos de este capítulo incluyen el uso de la CLI de AWS. Complete los siguientes pasos para instalar la CLI de AWS.

Requisitos previos

Necesita haber creado y tener acceso a un ID de clave de acceso de AWS y a una clave de acceso secreta de AWS. Consulte Configuración rápida de la CLI de AWS para obtener información e instrucciones.

Procedimiento

1. Instale Python 3 y la herramienta **pip**.

```
# yum install python3
# yum install python3-pip
```

2. Instale las herramientas de línea de comandos de AWS con el comando **pip**.

```
# pip3 install awscli
```

3. Ejecute el comando **aws --version** para verificar que ha instalado la CLI de AWS.

```
$ aws --version
aws-cli/1.16.182 Python/2.7.5 Linux/3.10.0-957.21.3.el7.x86_64 botocore/1.12.172
```

4. Configure el cliente de línea de comandos de AWS según sus datos de acceso a AWS.

```
$ aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]:
```

Recursos adicionales

- Configuración rápida de la CLI de AWS
- Herramientas de línea de comandos de AWS

4.3. CREACIÓN DE UNA INSTANCIA EC2 EN HA

Complete los siguientes pasos para crear las instancias que utilizará como nodos de su cluster de HA. Tenga en cuenta que tiene varias opciones para obtener las imágenes RHEL que utiliza para su cluster. Consulte Opciones de imagen de Red Hat Enterprise Linux en AWS para obtener información sobre las opciones de imagen para AWS.

Puedes crear y subir una imagen personalizada que utilices para tus nodos de clúster, o puedes elegir una imagen Gold (imagen Cloud Access) o una imagen bajo demanda.

Requisitos previos

Necesita haber configurado un entorno de AWS. Consulte Configuración con Amazon EC2 para obtener más información.

Procedimiento

1. En el panel de control de AWS EC2, seleccione **Images** y luego **AMIs**.
2. Haga clic con el botón derecho del ratón en su imagen y seleccione **Launch**.
3. Elija un **Instance Type** que cumpla o supere los requisitos de su carga de trabajo. En función de su aplicación de HA, es posible que cada instancia deba tener mayor capacidad.

Consulte Tipos de instancias de Amazon EC2 para obtener información sobre los tipos de instancias.

1. Haga clic en **Next: Configure Instance Details**.
   a. Introduzca la dirección **Number of instances** que desea crear para el clúster. Los ejemplos de este capítulo utilizan tres nodos de clúster.

NOTA

No se lanza a un grupo de autoescalado.

   b. Para **Network**, seleccione la VPC que creó en Configurar el entorno de AWS . Seleccione la subred de la instancia para crear una nueva subred.

   c. Seleccione **Enable** para la autoasignación de la IP pública. Estas son las selecciones mínimas que debe hacer para **Configure Instance Details**. Dependiendo de su aplicación específica de HA, es posible que tenga que hacer selecciones adicionales.

NOTA

Estas son las opciones de configuración mínimas necesarias para crear una instancia básica. Revise las opciones adicionales en función de los requisitos de su aplicación de HA.

2. Haga clic en **Next: Add Storage** y compruebe que el almacenamiento por defecto es suficiente. No es necesario modificar esta configuración a menos que su aplicación de HA requiera otras opciones de almacenamiento.

3. Haga clic en **Next: Add Tags**.

NOTA

Las etiquetas pueden ayudarle a administrar sus recursos de AWS. Consulte Etiquetado de sus recursos de Amazon EC2 para obtener información sobre el etiquetado.

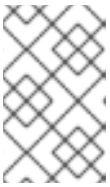
4. Haga clic en **Next: Configure Security Group**. Seleccione el grupo de seguridad existente que creó en Configuración del entorno de AWS .

5. Haga clic en **Review and Launch** y verifique sus selecciones.

6. Haga clic en **Launch**. Se le pedirá que seleccione un par de claves existente o que cree un nuevo par de claves. Seleccione el par de claves que creó al configurar el entorno de AWS .

7. Haga clic en **Launch Instances**.

8. Haga clic en **View Instances**. Puede nombrar la(s) instancia(s).



NOTA

Como alternativa, puede lanzar instancias utilizando la CLI de AWS. Consulte Lanzamiento, listado y finalización de instancias de Amazon EC2 en la documentación de Amazon para obtener más información.

Recursos adicionales

- Consola de administración de AWS
- Configuración con Amazon EC2
- Instancias de Amazon EC2
- Tipos de instancias de Amazon EC2

4.4. CONFIGURACIÓN DE LA CLAVE PRIVADA

Complete las siguientes tareas de configuración para utilizar el archivo de clave privada SSH (**.pem**) antes de que pueda ser utilizado en una sesión SSH.

Procedimiento

1. Mueva el archivo de claves del directorio **Downloads** a su directorio **Home** o a su **~/.ssh directory**.

2. Introduzca el siguiente comando para cambiar los permisos del archivo de claves para que sólo el usuario root pueda leerlo.

```
# chmod 400 NombreClave.pem
```

4.5. CONEXIÓN A UNA INSTANCIA

Complete los siguientes pasos en todos los nodos para conectarse a una instancia.

Procedimiento

1. Inicie la consola de AWS y seleccione la instancia EC2.
2. Haga clic en **Connect** y seleccione **A standalone SSH client**.
3. Desde su sesión de terminal SSH, conéctese a la instancia utilizando el ejemplo de AWS proporcionado en la ventana emergente. Añada la ruta correcta a su archivo **KeyName.pem** si la ruta no se muestra en el ejemplo.

4.6. INSTALACIÓN DE LOS PAQUETES Y AGENTES DE ALTA DISPONIBILIDAD

Complete los siguientes pasos en todos los nodos para instalar los paquetes y agentes de Alta Disponibilidad.

Procedimiento

1. Introduzca el siguiente comando para eliminar el cliente AWS Red Hat Update Infrastructure (RHUI). Dado que va a utilizar una suscripción a Red Hat Cloud Access, no debe utilizar AWS RHUI además de su suscripción.

```
$ sudo -i
# yum -y remove rh-amazon-rhui-client*
```

2. Registre la VM con Red Hat.

```
# subscription-manager register --auto-attach
```

3. Desactivar todos los repositorios.

```
# subscription-manager repos --disable=*
```

4. Habilite los repositorios de RHEL 8 Server y RHEL 8 Server HA.

```
# subscription-manager repos --enable=rhel-8-server-rpms
# subscription-manager repos --enable=rhel-ha-for-rhel-8-server-rpms
```

5. Actualice la instancia AWS de RHEL.

```
# yum update -y
```

6. Instale los paquetes de software Red Hat High Availability Add-On, junto con todos los agentes de cercado disponibles en el canal de Alta Disponibilidad.

```
# yum install pcs pacemaker fence-agents-aws
```

7. El usuario **hacluster** fue creado durante la instalación de **pcs** y **pacemaker** en el paso anterior. Cree una contraseña para **hacluster** en todos los nodos del clúster. Utilice la misma contraseña para todos los nodos.

```
# passwd hacluster
```

8. Añada el servicio **high availability** al cortafuegos de RHEL si está instalado **firewalld.service**.

```
# firewall-cmd --permanent --add-service=high-availability
# firewall-cmd --reload
```

9. Inicie el servicio **pcs** y permita que se inicie en el arranque.

```
# systemctl start pcsd.service
# systemctl enable pcsd.service
```

10. Edite **/etc/hosts** y añada los nombres de los hosts RHEL y las direcciones IP internas. Consulte ¿Cómo debe configurarse el archivo /etc/hosts en los nodos del clúster RHEL? para obtener más detalles.

Paso de verificación

Asegúrese de que el servicio **pcs** está funcionando.

```
# systemctl status pcsd.service

pcsd.service - PCS GUI and remote configuration interface
Loaded: loaded (/usr/lib/systemd/system/pcsd.service; enabled; vendor preset: disabled)
Active: active (running) since Thu 2018-03-01 14:53:28 UTC; 28min ago
Docs: man:pcsd(8)
man:pcs(8)
Main PID: 5437 (pcsd)
CGroup: /system.slice/pcsd.service
    └─5437 /usr/bin/ruby /usr/lib/pcsd/pcsd > /dev/null &
Mar 01 14:53:27 ip-10-0-0-48.ec2.internal systemd[1]: Starting PCS GUI and remote configuration
interface…
Mar 01 14:53:28 ip-10-0-0-48.ec2.internal systemd[1]: Started PCS GUI and remote configuration
interface.
```

4.7. CREACIÓN DE UN CLÚSTER

Complete los siguientes pasos para crear el cluster de nodos.

Procedimiento

1. En uno de los nodos, introduzca el siguiente comando para autenticar al usuario pcs **hacluster**. En el comando, especifique el nombre de cada nodo del clúster.

```
# pcs host auth  hostname1 hostname2 hostname3
Username: hacluster
Password:
hostname1: Authorized
hostname2: Authorized
hostname3: Authorized
```

Ejemplo:

```
[root@node01 clouduser]# pcs host auth node01 node02 node03
Username: hacluster
Password:
node01: Authorized
node02: Authorized
node03: Authorized
```

2. Crea el clúster.

```
# pcs cluster setup cluster-name hostname1 hostname2 hostname3
```

Ejemplo:

```
[root@node01 clouduser]# pcs cluster setup --name newcluster node01 node02 node03

...omitted

Synchronizing pcsd certificates on nodes node01, node02, node03...
node02: Success
node03: Success
node01: Success
Restarting pcsd on the nodes in order to reload the certificates...
node02: Success
node03: Success
node01: Success
```

Pasos de verificación

1. Habilitar el clúster.

```
root@node01 clouduser]# pcs cluster enable --all
```

2. Poner en marcha el clúster.

```
[root@node01 clouduser]# pcs cluster start --all
```

Ejemplo:

```
[root@node01 clouduser]# pcs cluster enable --all
node02: Cluster Enabled
node03: Cluster Enabled
node01: Cluster Enabled

[root@node01 clouduser]# pcs cluster start --all
node02: Starting Cluster...
node03: Starting Cluster...
node01: Starting Cluster...
```

4.8. CONFIGURACIÓN DE LAS VALLAS

Complete los siguientes pasos para configurar el cercado.

Procedimiento

1. Introduzca la siguiente consulta de metadatos de AWS para obtener el ID de instancia de cada nodo. Necesita estos IDs para configurar el dispositivo de la valla. Consulte Metadatos de la instancia y datos del usuario para obtener información adicional.

```
# echo $(curl -s http://169.254.169.254/latest/meta-data/instance-id)
```

Ejemplo:

```
root@ip-10-0-0-48 ~]# echo $(curl -s http://169.254.169.254/latest/meta-data/instance-id) i-07f1ac63af0ec0ac6
```

2. Introduzca el siguiente comando para configurar el dispositivo de valla. Utilice el comando **pcmk_host_map** para asignar el nombre del host RHEL al ID de la instancia. Utilice la clave de acceso de AWS y la clave de acceso secreta de AWS que configuró previamente.

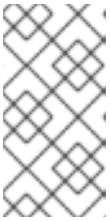
```
# pcs stonith create name fence_aws access_key=clave de acceso secret_key=secret-access-key region=region pcmk_host_map="rhel-hostname-1:Instance-ID-1;rhel-hostname-2:Instance-ID-2;rhel-hostname-3:Instance-ID-3" power_timeout=240 pcmk_reboot_timeout=480 pcmk_reboot_retries=4
```

Ejemplo:

```
root@ip-10-0-0-48 ~]# pcs stonith create clusterfence fence_aws access_key=AKIAI*******6MRMJA secret_key=a75EYIG4RVL3h*******K7koQ8dzaDyn5yoIZ/ region=us-east-1 pcmk_host_map="ip-10-0-0-48:i-07f1ac63af0ec0ac6;ip-10-0-0-46:i-063fc5fe93b4167b2;ip-10-0-0-58:i-08bd39eb03a6fd2c7" power_timeout=240 pcmk_reboot_timeout=480 pcmk_reboot_retries=4
```

3. Pruebe el agente de esgrima para uno de los otros nodos.

```
# pcs stonith fence awsnodename
```



NOTA

La respuesta del comando puede tardar varios minutos en aparecer. Si observa la sesión de terminal activa para el nodo que se está cercando, verá que la conexión de terminal se termina inmediatamente después de introducir el comando fence.

Ejemplo:

```
[root@ip-10-0-0-48 ~]# pcs stonith fence ip-10-0-0-58
Node: ip-10-0-0-58 fenced
```

Pasos de verificación

1. Compruebe el estado para verificar que el nodo está cercado.

```
# estado de las pcs
```

Ejemplo:

```
[root@ip-10-0-0-48 ~]# pcs status
Cluster name: newcluster
Stack: corosync
Current DC: ip-10-0-0-46 (version 1.1.18-11.el7-2b07d5c5a9) - partition with quorum
Last updated: Fri Mar  2 19:55:41 2018
Last change: Fri Mar  2 19:24:59 2018 by root via cibadmin on ip-10-0-0-46

3 nodes configured
1 resource configured

Online: [ ip-10-0-0-46 ip-10-0-0-48 ]
OFFLINE: [ ip-10-0-0-58 ]

Full list of resources:
clusterfence  (stonith:fence_aws):    Started ip-10-0-0-46

Daemon Status:
corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled
```

2. Inicie el nodo que fue cercado en el paso anterior.

```
# pcs cluster start awshostname
```

3. Comprueba el estado para verificar que el nodo se ha iniciado.

```
# estado de las pcs
```

Ejemplo:

```
[root@ip-10-0-0-48 ~]# pcs status
Cluster name: newcluster
Stack: corosync
Current DC: ip-10-0-0-46 (version 1.1.18-11.el7-2b07d5c5a9) - partition with quorum
Last updated: Fri Mar  2 20:01:31 2018
Last change: Fri Mar  2 19:24:59 2018 by root via cibadmin on ip-10-0-0-48

3 nodes configured
1 resource configured

Online: [ ip-10-0-0-46 ip-10-0-0-48 ip-10-0-0-58 ]

Full list of resources:

 clusterfence  (stonith:fence_aws):    Started ip-10-0-0-46

Daemon Status:
```

```
corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled
```

4.9. INSTALACIÓN DE LA CLI DE AWS EN LOS NODOS DEL CLÚSTER

Anteriormente, ha instalado la CLI de AWS en su sistema anfitrión. Debe instalar la CLI de AWS en los nodos del clúster antes de configurar los agentes de recursos de red.

Complete el siguiente procedimiento en cada nodo del clúster.

Requisitos previos

Debe haber creado una AWS Access Key y una AWS Secret Access Key. Consulte Crear la clave de acceso de AWS y la clave de acceso secreta de AWS para obtener más información.

Procedimiento

1. Realice el procedimiento de instalación de la CLI de AWS .
2. Introduzca el siguiente comando para verificar que la CLI de AWS está configurada correctamente. Deberían aparecer los ID de instancia y los nombres de instancia. Ejemplo:

```
[root@ip-10-0-0-48 ~]# aws ec2 describe-instances --output text --query
'Reservations[*].Instances[*].[InstanceId,Tags[?Key==`Name`].Value]'
i-07f1ac63af0ec0ac6
ip-10-0-0-48
i-063fc5fe93b4167b2
ip-10-0-0-46
i-08bd39eb03a6fd2c7
ip-10-0-0-58
```

4.10. INSTALACIÓN DE AGENTES DE RECURSOS DE RED

Para que las operaciones de HA funcionen, el clúster utiliza agentes de recursos de red de AWS para habilitar la funcionalidad de conmutación por error. Si un nodo no responde a una comprobación de heartbeat en un tiempo determinado, el nodo se bloquea y las operaciones pasan a un nodo adicional del clúster. Los agentes de recursos de red deben estar configurados para que esto funcione.

Añada los dos recursos al mismo grupo para aplicar las restricciones de **order** y **colocation**.

Create a secondary private IP resource and virtual IP resource

Complete el siguiente procedimiento para añadir una dirección IP privada secundaria y crear una IP virtual. Puede completar este procedimiento desde cualquier nodo del clúster.

Procedimiento

1. Introduzca el siguiente comando para ver la descripción del agente de recursos **AWS Secondary Private IP Address** (awsvip). Esto muestra las opciones y operaciones por defecto para este agente.

```
# pcs resource describe awsvip
```

2. Introduzca el siguiente comando para crear la dirección IP privada secundaria utilizando una dirección IP privada no utilizada en el bloque **VPC CIDR**.

```
# pcs resource create privip awsvip secondary_private_ip=Unused-IP-Address --group
group-name
```

Ejemplo:

```
root@ip-10-0-0-48 ~]# pcs resource create privip awsvip secondary_private_ip=10.0.0.68 --
group networking-group
```

3. Cree un recurso IP virtual. Se trata de una dirección IP de la VPC que se puede reasignar rápidamente del nodo vallado al nodo de conmutación por error, enmascarando el fallo del nodo vallado dentro de la subred.

```
# pcs resource create vip IPaddr2 ip=secondary-private-IP --group group-name
```

Ejemplo:

```
root@ip-10-0-0-48 ~]# pcs resource create vip IPaddr2 ip=10.0.0.68 --group networking-
group
```

Paso de verificación

Introduzca el comando **pcs status** para verificar que los recursos se están ejecutando.

```
# estado de las pcs
```

Ejemplo:

```
[root@ip-10-0-0-48 ~]# pcs status
Cluster name: newcluster
Stack: corosync
Current DC: ip-10-0-0-46 (version 1.1.18-11.el7-2b07d5c5a9) - partition with quorum
Last updated: Fri Mar  2 22:34:24 2018
Last change: Fri Mar  2 22:14:58 2018 by root via cibadmin on ip-10-0-0-46

3 nodes configured
3 resources configured

Online: [ ip-10-0-0-46 ip-10-0-0-48 ip-10-0-0-58 ]

Full list of resources:

clusterfence    (stonith:fence_aws):    Started ip-10-0-0-46
 Resource Group: networking-group
     privip (ocf::heartbeat:awsvip):    Started ip-10-0-0-48
     vip    (ocf::heartbeat:IPaddr2):   Started ip-10-0-0-58

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

Create an elastic IP address

Una dirección IP elástica es una dirección IP pública que puede ser rápidamente reasignada desde el nodo vallado al nodo de conmutación por error, enmascarando el fallo del nodo vallado.

Tenga en cuenta que esto es diferente del recurso IP virtual creado anteriormente. La dirección IP elástica se utiliza para las conexiones a Internet de cara al público en lugar de las conexiones de subred.

1. Añada los dos recursos al mismo grupo que se creó anteriormente para aplicar las restricciones de **order** y **colocation**.
2. Introduzca el siguiente comando de la CLI de AWS para crear una dirección IP elástica.

```
[root@ip-10-0-0-48 ~]# aws ec2 allocate-address --domain vpc --output text
eipalloc-4c4a2c45   vpc 35.169.153.122
```

3. Introduzca el siguiente comando para ver la descripción del agente de recursos AWS Secondary Elastic IP Address (awseip). Esto muestra las opciones y las operaciones predeterminadas para este agente.

```
# pcs resource describe awseip
```

4. Cree el recurso de dirección IP elástica secundaria utilizando la dirección IP asignada creada en el paso 1.

```
# pcs resource create elastic awseip elastic_ip=_Elastic-IP-Address_allocation_id=_Elastic-IP-Association-ID_ --group networking-group
```

Ejemplo:

```
# pcs resource create elastic awseip elastic_ip=35.169.153.122 allocation_id=eipalloc-4c4a2c45 --group networking-group
```

Paso de verificación

Introduzca el comando **pcs status** para verificar que el recurso se está ejecutando.

```
# estado de las pcs
```

Ejemplo:

```
[root@ip-10-0-0-58 ~]# pcs status
Cluster name: newcluster
Stack: corosync
Current DC: ip-10-0-0-58 (version 1.1.18-11.el7-2b07d5c5a9) - partition with quorum
Last updated: Mon Mar  5 16:27:55 2018
Last change: Mon Mar  5 15:57:51 2018 by root via cibadmin on ip-10-0-0-46

3 nodes configured
4 resources configured

Online: [ ip-10-0-0-46 ip-10-0-0-48 ip-10-0-0-58 ]

Full list of resources:
```

```
 clusterfence   (stonith:fence_aws):    Started ip-10-0-0-46
 Resource Group: networking-group
     privip (ocf::heartbeat:awsvip):  Started ip-10-0-0-48
     vip    (ocf::heartbeat:IPaddr2):    Started ip-10-0-0-48
     elastic (ocf::heartbeat:awseip):    Started ip-10-0-0-48

 Daemon Status:
   corosync: active/disabled
   pacemaker: active/disabled
   pcsd: active/enabled
```

Test the elastic IP address

Introduzca los siguientes comandos para verificar que los recursos de IP virtual (awsvip) e IP elástica (awseip) están funcionando.

Procedimiento

1. Inicie una sesión SSH desde su estación de trabajo local a la dirección IP elástica creada anteriormente.

   ```
   $ ssh -l ec2-user -i ~/.ssh/<Nombre-Clave>.pem elastic-IP
   ```

   Ejemplo:

   ```
   $ ssh -l ec2-user -i ~/.ssh/cluster-admin.pem 35.169.153.122
   ```

2. Comprueba que el host al que te has conectado vía SSH es el host asociado al recurso elástico creado.

Recursos adicionales

- Descripción del complemento de alta disponibilidad
- Administración del complemento de alta disponibilidad
- Referencia del complemento de alta disponibilidad

4.11. CONFIGURACIÓN DEL ALMACENAMIENTO EN BLOQUE COMPARTIDO

Esta sección proporciona un procedimiento opcional para configurar el almacenamiento de bloques compartido para un cluster de Red Hat High Availability con volúmenes de Amazon EBS Multi-Attach. El procedimiento supone tres instancias (un clúster de tres nodos) con un disco compartido de 1 TB.

Procedimiento

1. Crea un volumen de bloques compartido con el comando AWS create-volume.

   ```
   $ aws ec2 create-volume --availability-zone <availability_zone> --no-encrypted --size 1024 --
   volume-type io1 --iops 51200 --multi-attach-enabled
   ```

   Por ejemplo, el siguiente comando crea un volumen en la zona de disponibilidad **us-east-1a**.

```
$ aws ec2 create-volume --availability-zone us-east-1a --no-encrypted --size 1024 --volume-type io1 --iops 51200 --multi-attach-enabled

{
    "AvailabilityZone": "us-east-1a",
    "CreateTime": "2020-08-27T19:16:42.000Z",
    "Encrypted": false,
    "Size": 1024,
    "SnapshotId": "",
    "State": "creating",
    "VolumeId": "vol-042a5652867304f09",
    "Iops": 51200,
    "Tags": [ ],
    "VolumeType": "io1"
}
```

NOTA

Necesita el **VolumeId** en el siguiente paso.

2. Para cada instancia de su clúster, adjunte un volumen de bloques compartido utilizando el comando AWS attach-volume. Utilice su **<instance_id>** y **<volume_id>**.

```
$ aws ec2 attach-volume --device /dev/xvdd --instance-id <instance_id> --volume-id <volume_id>
```

Por ejemplo, el siguiente comando adjunta un volumen de bloques compartido **vol-042a5652867304f09** a **instance i-0eb803361c2c887f2**.

```
$ aws ec2 attach-volume --device /dev/xvdd --instance-id i-0eb803361c2c887f2 --volume-id vol-042a5652867304f09

{
    "AttachTime": "2020-08-27T19:26:16.086Z",
    "Device": "/dev/xvdd",
    "InstanceId": "i-0eb803361c2c887f2",
    "State": "attaching",
    "VolumeId": "vol-042a5652867304f09"
}
```

Pasos de verificación

1. Para cada instancia de su cluster, verifique que el dispositivo de bloque está disponible utilizando el comando **ssh** con su instancia **<ip_address>**.

```
# ssh <ip_address> "hostname ; lsblk -d | grep ' 1T '"
```

Por ejemplo, el siguiente comando enumera los detalles, incluyendo el nombre de host y el dispositivo de bloque para la instancia IP **198.51.100.3**.

```
# ssh 198.51.100.3 "hostname ; lsblk -d | grep ' 1T '"

nodea
```

```
nvme2n1 259:1    0   1T  0 disk
```

2. Utilice el comando **ssh** para verificar que cada instancia de su clúster utiliza el mismo disco compartido.

```
# ssh <ip_address> "hostname ; lsblk -d | grep ' 1T ' | awk '{print \$1}' | xargs -i udevadm info
--query=all --name=/dev/{} | grep '^E: ID_SERIAL='"
```

Por ejemplo, el siguiente comando enumera los detalles, incluyendo el nombre del host y el ID del volumen de disco compartido para la dirección IP de la instancia **198.51.100.3**.

```
 # ssh 198.51.100.3 "hostname ; lsblk -d | grep ' 1T ' | awk '{print \$1}' | xargs -i udevadm info
--query=all --name=/dev/{} | grep '^E: ID_SERIAL='"

nodea
E: ID_SERIAL=Amazon Elastic Block Store_vol0fa5342e7aedf09f7
```

Después de verificar que el disco compartido está conectado a cada instancia, puede configurar el almacenamiento resistente para el cluster. Para obtener información sobre la configuración del almacenamiento resistente para un cluster de Red Hat High Availability, consulte Configuración de un sistema de archivos GFS2 en un cluster. Para obtener información general sobre el sistema de archivos GFS2, consulte Configuración de sistemas de archivos GFS2 .

CAPÍTULO 5. IMPLANTACIÓN DE UNA IMAGEN DE RED HAT ENTERPRISE LINUX COMO INSTANCIA DE GOOGLE COMPUTE ENGINE EN GOOGLE CLOUD PLATFORM

Tiene varias opciones para implementar una imagen de Red Hat Enterprise Linux (RHEL) 8 como una instancia de Google Compute Engine (GCE) en Google Cloud Platform (GCP). Este capítulo discute sus opciones para elegir una imagen y enumera o se refiere a los requisitos del sistema para su sistema anfitrión y máquina virtual (VM). El capítulo proporciona procedimientos para crear una VM personalizada a partir de una imagen ISO, subirla a GCE y lanzar una instancia.

Este capítulo hace referencia a la documentación de Google en varios lugares. Para muchos procedimientos, consulte la documentación de Google a la que se hace referencia para obtener más detalles.

NOTA

Para ver una lista de certificaciones de productos Red Hat para GCP, consulte Red Hat en Google Cloud Platform.

Requisitos previos

- Necesita una cuenta en el Portal del Cliente de Red Hat para completar los procedimientos de este capítulo.
- Cree una cuenta en GCP para acceder a la consola de Google Cloud Platform. Consulte Google Cloud para obtener más información.
- Habilite sus suscripciones de Red Hat a través del programa Red Hat Cloud Access. El programa Red Hat Cloud Access le permite trasladar sus suscripciones de Red Hat desde sistemas físicos o locales a GCP con el apoyo total de Red Hat.

Recursos adicionales

- Red Hat en la nube pública
- Nube de Google

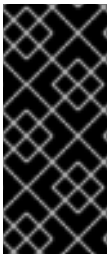
5.1. OPCIONES DE IMAGEN DE RED HAT ENTERPRISE LINUX EN GCP

La siguiente tabla enumera las opciones de imagen y las diferencias entre ellas.

Tabla 5.1. Opciones de imagen

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones
Elija desplegar una imagen personalizada que mueva a GCP.	Aproveche sus suscripciones existentes a Red Hat.	Habilite las suscripciones a través del programa Red Hat Cloud Access, cargue su imagen personalizada y adjunte sus suscripciones.	La suscripción incluye el coste del producto de Red Hat; usted paga todos los demás costes de la instancia. Las imágenes personalizadas que se trasladan a GCP se denominan imágenes de "Acceso a la nube" porque se aprovechan las suscripciones existentes de Red Hat. Red Hat proporciona soporte directamente para las imágenes de Cloud Access.
Elija desplegar una imagen de GCP existente que incluya RHEL.	Las imágenes de GCP incluyen un producto de Red Hat.	Elija una imagen RHEL cuando lance una instancia en GCP Compute Engine o elija una imagen de Google Cloud Platform Marketplace.	Usted paga a GCP por hora en un modelo de pago por uso. Estas imágenes se denominan imágenes "a la carta". GCP ofrece soporte para las imágenes bajo demanda a través de un acuerdo de soporte.



IMPORTANTE

No se puede convertir una instancia bajo demanda en una instancia de Red Hat Cloud Access. Para cambiar de una imagen bajo demanda a una imagen de Red Hat Cloud Access de suscripción propia (BYOS), cree una nueva instancia de Red Hat Cloud Access y migre los datos de su instancia bajo demanda. Cancele su instancia bajo demanda después de migrar sus datos para evitar la doble facturación.

El resto de este capítulo incluye información y procedimientos relativos a las imágenes personalizadas.

Recursos adicionales

- Red Hat en la nube pública
- Imágenes
- Guía de referencia de Red Hat Cloud Access
- Creación de una instancia a partir de una imagen personalizada

5.2. COMPRENDER LAS IMÁGENES BASE

Esta sección incluye información sobre el uso de imágenes base preconfiguradas y sus ajustes de configuración.

5.2.1. Utilizar una imagen base personalizada

Para configurar manualmente una VM, se empieza con una imagen de VM base (de inicio). Una vez creada la imagen de la VM base, puede modificar los ajustes de configuración y añadir los paquetes que la VM necesita para funcionar en la nube. Puede realizar cambios de configuración adicionales para su aplicación específica después de cargar la imagen.

Recursos adicionales

Red Hat Enterprise Linux

5.2.2. Ajustes de configuración de la máquina virtual

Las VM de la nube deben tener los siguientes ajustes de configuración.

Tabla 5.2. Ajustes de configuración de la máquina virtual

Configuración	Recomendación
ssh	ssh debe estar habilitado para proporcionar acceso remoto a sus máquinas virtuales.
dhcp	El adaptador virtual primario debe estar configurado para dhcp.

5.3. CREACIÓN DE UNA VM BASE A PARTIR DE UNA IMAGEN ISO

Siga los procedimientos de esta sección para crear una imagen base a partir de una imagen ISO.

Requisitos previos

Habilite la virtualización para su máquina anfitriona Red Hat Enterprise Linux 8.

5.3.1. Descarga de la imagen ISO

Procedimiento

1. Descargue la última imagen ISO de Red Hat Enterprise Linux desde el Portal del Cliente de Red Hat.
2. Mueve la imagen a **/var/lib/libvirt/images**.

5.3.2. Creación de una VM a partir de la imagen ISO

Procedimiento

1. Asegúrese de que ha habilitado su máquina anfitriona para la virtualización. Consulte Activación de la virtualización en RHEL 8 para obtener información y procedimientos.

2. Cree e inicie una VM básica de Red Hat Enterprise Linux. Consulte Creación de máquinas virtuales para obtener instrucciones.

   a. Si utiliza la línea de comandos para crear su VM, asegúrese de configurar la memoria y las CPUs por defecto a la capacidad que desea para la VM. Establezca su interfaz de red virtual en **virtio**.
   A continuación, un ejemplo básico de línea de comandos.

   ```
   virt-install --name isotest --memory 2048 --vcpus 2 --disk size=8,bus=virtio --location
   rhel-8.0-x86_64-dvd.iso --os-variant=rhel8.0
   ```

   b. Si utiliza la consola web para crear su VM, siga el procedimiento en Creación de máquinas virtuales utilizando la consola web, con estas advertencias:

   - No compruebe **Immediately Start VM**.
   - Cambie su **Memory** y **Storage Size** a su configuración preferida.
   - Antes de comenzar la instalación, asegúrese de haber cambiado **Model** en **Virtual Network Interface Settings** a **virtio** y cambie su **vCPUs** a la configuración de capacidad que desee para la VM.

5.3.3. Completar la instalación de RHEL

Realice los siguientes pasos para completar la instalación y para habilitar el acceso de root una vez que se inicie la VM.

Procedimiento

1. Elija el idioma que desea utilizar durante el proceso de instalación.
2. En la vista **Installation Summary**:

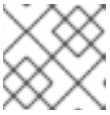
   a. Haga clic en **Software Selection** y marque **Minimal Install**.

   b. Haga clic en **Done**.

   c. Haga clic en **Installation Destination** y marque **Custom** en **Storage Configuration**.

   - Verifique al menos 500 MB para /**boot**. Puede utilizar el espacio restante para la raíz /.
   - Se recomiendan las particiones estándar, pero se puede utilizar Logical Volume Management (LVM).
   - Puedes usar xfs, ext4 o ext3 para el sistema de archivos.
   - Haga clic en **Done** cuando haya terminado con los cambios.

3. Haga clic en **Begin Installation**.
4. Establezca un **Root Password**. Cree otros usuarios según corresponda.
5. Reinicie la máquina virtual e inicie sesión como **root** una vez que la instalación se haya completado.
6. Configurar la imagen.



NOTA

Asegúrese de que el paquete **cloud-init** está instalado y habilitado.

7. Apague la máquina virtual.

5.4. CARGA DE LA IMAGEN RHEL EN GCP

Siga los procedimientos de esta sección para cargar su imagen en GCP.

5.4.1. Creación de un nuevo proyecto en GCP

Complete los siguientes pasos para crear un nuevo proyecto en GCP.

Requisitos previos

Debe haber creado una cuenta en GCP. Si no lo ha hecho, consulte Google Cloud para obtener más información.

Procedimiento

1. Inicie la consola de GCP .
2. Haga clic en el menú desplegable a la derecha de **Google Cloud Platform**.
3. En el menú emergente, haga clic en **NEW PROJECT**.
4. En la ventana **New Project**, introduzca un nombre para su nuevo proyecto.
5. Marque la casilla **Organization**. Haga clic en el menú desplegable para cambiar la organización, si es necesario.
6. Confirme el **Location** de su organización o carpeta principal. Haga clic en **Browse** para buscar y cambiar este valor, si es necesario.
7. Haga clic en **CREATE** para crear su nuevo proyecto GCP.

NOTA

Una vez instalado el SDK de Google Cloud, puede utilizar el comando CLI **gcloud projects create** para crear un proyecto. A continuación se presenta un ejemplo sencillo.

```
gcloud projects create mi-gcp-proyecto3 --nombre proyecto3
```

El ejemplo crea un proyecto con el ID de proyecto **my-gcp-project3** y el nombre de proyecto **project3**. Ver gcloud project create para más información.

Recursos adicionales

Creación y gestión de recursos

5.4.2. Instalación del SDK de Google Cloud

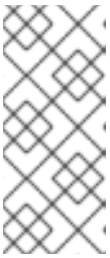
Complete los siguientes pasos para instalar el SDK de Google Cloud.

Requisitos previos

- Cree un proyecto en GCP si aún no lo ha hecho. Consulte Crear un nuevo proyecto en Google Cloud Platform para obtener más información.
- Asegúrese de que su sistema anfitrión incluye Python 2.7. Si no lo hace, instale Python 2.7.

Procedimiento

1. Siga las instrucciones de GCP para descargar y extraer el archivo del SDK de Google Cloud. Consulte el documento de GCP Quickstart for Linux para obtener más detalles.
2. Siga las mismas instrucciones para inicializar el SDK de Google Cloud.



NOTA

Una vez que haya inicializado el SDK de Google Cloud, puede utilizar los comandos de la CLI de **gcloud** para realizar tareas y obtener información sobre su proyecto e instancias. Por ejemplo, puede mostrar información del proyecto con el comando **gcloud compute project-info describe --project <project-name>**.

Recursos adicionales

- Inicio rápido para Linux
- referencia del comando gcloud
- visión general de la herramienta de línea de comandos gcloud

5.4.3. Creación de claves SSH para Google Compute Engine

Realice el siguiente procedimiento para generar y registrar claves SSH con GCE, de modo que pueda acceder directamente a una instancia utilizando su dirección IP pública.

Procedimiento

1. Utilice el comando **ssh-keygen** para generar un par de claves SSH para su uso con la CME.

```
# ssh-keygen -t rsa -f ~/.ssh/google_compute_engine
```

2. En la página del panel de control de la consola de GCP , haga clic en el menú **Navigation** situado a la izquierda de Google **Cloud Console banner** y seleccione **Compute Engine** y, a continuación, **Metadata**.
3. Haga clic en **SSH Keys** y luego en **Edit**.
4. Introduzca la salida generada desde el archivo **~/.ssh/google_compute_engine.pub** y haga clic en **Save**.
   Ahora puede conectarse a su instancia usando SSH estándar.

```
# ssh -i ~/.ssh/google_compute_engine <nombre_de_usuario>@<instance_external_ip>
```

NOTA

Puede ejecutar el comando **gcloud compute config-ssh** para rellenar su archivo de configuración con alias para sus instancias. Los alias permiten conexiones SSH simples por nombre de instancia. Para obtener información sobre el comando **gcloud compute config-ssh**, consulte gcloud compute config-ssh.

Recursos adicionales

- gcloud compute config-ssh
- Conexión a las instancias

5.4.4. Creación de un cubo de almacenamiento en GCP Storage

La importación a GCP requiere un cubo de almacenamiento de GCP. Complete los siguientes pasos para crear un cubo.

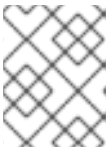
Procedimiento

1. Si aún no ha iniciado la sesión en GCP, hágalo con el siguiente comando.

```
# gcloud auth login
```

2. Crear un cubo de almacenamiento.

```
# gsutil mb gs://nombre_del_cubo
```



NOTA

También puedes utilizar la consola de Google Cloud para crear un cubo. Consulte Crear un cubo para obtener información.

Recursos adicionales

Crear un cubo

5.4.5. Conversión y carga de la imagen en el cubo de GCP

Complete el siguiente procedimiento para convertir y cargar su imagen en su cubo GCP. Los ejemplos son representativos; convierten una imagen de **qcow2** al formato **raw** y luego alquitranan esa imagen para cargarla.

Procedimiento

1. Ejecute el comando **qemu-img** para convertir su imagen. La imagen convertida debe tener el nombre **disk.raw**.

```
# qemu-img convert -f qcow2 -O raw rhel-8.2-sample.qcow2 disk.raw
```

2. Alquitrán la imagen.

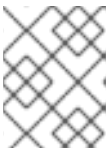
```
# tar --format=oldgnu -Sczf disk.raw.tar.gz disk.raw
```

3. Sube la imagen al cubo que has creado anteriormente. La subida puede tardar unos minutos.

```
# gsutil cp disco.raw.tar.gz gs://nombre_del_cubo
```

4. En la pantalla de inicio de **Google Cloud Platform**, haga clic en el icono del menú colapsado y seleccione **Storage** y luego **Browser**.

5. Haz clic en el nombre de tu cubo.
La imagen alquitranada aparece bajo el nombre de su cubo.



NOTA

También puedes subir tu imagen utilizando la página **GCP Console**. Para ello, haz clic en el nombre de tu cubo y luego en **Upload files**.

Recursos adicionales

- Importación manual de discos virtuales
- Elegir un método de importación

5.4.6. Creación de una imagen a partir del objeto en el cubo del GCP

Realice el siguiente procedimiento para crear una imagen del objeto en su cubo de GCP.

Procedimiento

1. Ejecute el siguiente comando para crear una imagen para la CME. Especifique el nombre de la imagen que está creando, el nombre del cubo y el nombre de la imagen alquitranada.

```
# gcloud compute images create my-image-name --source-uri gs://my-bucket-
name/disk.raw.tar.gz
```

NOTA

También puede utilizar la consola de Google Cloud para crear una imagen. Para obtener más información, consulte Creación, eliminación y eliminación de imágenes personalizadas.

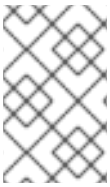
2. Opcionalmente, busque la imagen en la Consola GCP.
   a. Haga clic en el menú **Navigation** situado a la izquierda del banner **Google Cloud Console**.
   b. Seleccione **Compute Engine** y luego **Images**.

Recursos adicionales

- Creación, supresión y eliminación de imágenes personalizadas
- gcloud compute images create

5.4.7. Creación de una instancia de Google Compute Engine a partir de una imagen

Realice los siguientes pasos para configurar una instancia VM de GCE mediante la consola de GCP.



NOTA

El siguiente procedimiento proporciona instrucciones para crear una instancia VM básica utilizando la Consola GCP. Consulte Creación e inicio de una instancia VM para obtener más información sobre las instancias VM de GCE y sus opciones de configuración.

Procedimiento

1. En la página del panel de control de la consola de GCP , haga clic en el menú **Navigation** situado a la izquierda de Google **Cloud Console banner** y seleccione **Compute Engine** y, a continuación, **Images**.
2. Seleccione su imagen.
3. Haga clic en **Create Instance**.
4. En la página **Create an instance**, introduzca un **Name** para su instancia.
5. Elija un **Region** y **Zone**.
6. Elija un **Machine configuration** que cumpla o supere los requisitos de su carga de trabajo.
7. Asegúrese de que **Boot disk** especifica el nombre de su imagen.
8. Opcionalmente, en **Firewall**, seleccione **Allow HTTP traffic** o **Allow HTTPS traffic**.
9. Haga clic en **Create**.

NOTA

Estas son las opciones de configuración mínimas necesarias para crear una instancia básica. Revise las opciones adicionales en función de los requisitos de su aplicación.

10. Encuentre su imagen en **VM instances**.
11. En el panel de control de la consola de GCP, haga clic en el menú **Navigation** situado a la izquierda de Google **Cloud Console banner** y seleccione **Compute Engine** y, a continuación, **VM instances**.

NOTA

Como alternativa, puede utilizar el comando CLI **gcloud compute instances create** para crear una instancia de VM GCE a partir de una imagen. A continuación se presenta un ejemplo sencillo.

```
gcloud compute instances create myinstance3 --zone=us-central1-a --image
test-iso2-image
```

El ejemplo crea una instancia VM llamada **myinstance3** en la zona **us-central1-a** basada en la imagen existente **test-iso2-image**. Ver gcloud compute instances create para más información.

5.4.8. Conectarse a su instancia

Realice el siguiente procedimiento para conectarse a su instancia GCE utilizando su dirección IP pública.

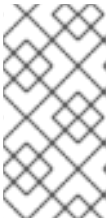
Procedimiento

1. Ejecute el siguiente comando para asegurarse de que su instancia se está ejecutando. El comando muestra información sobre su instancia GCE, incluyendo si la instancia se está ejecutando y, si es así, la dirección IP pública de la instancia en ejecución.

```
# lista de instancias de computación de gcloud
```

2. Conéctese a su instancia utilizando SSH estándar. El ejemplo utiliza la clave **google_compute_engine** creada anteriormente.

```
# ssh -i ~/.ssh/google_compute_engine <nombre_de_usuario>@<instance_external_ip>
```



NOTA

GCP ofrece varias formas de acceder a su instancia mediante SSH. Consulte Conectarse a las instancias para obtener más información. También puede conectarse a su instancia utilizando la cuenta y la contraseña de root que estableció anteriormente.

Recursos adicionales

- lista de instancias de computación de gcloud
- Conexión a las instancias

5.4.9. Adjuntar suscripciones a Red Hat

Complete los siguientes pasos para adjuntar las suscripciones que haya habilitado previamente a través del programa Red Hat Cloud Access.

Requisitos previos

Debe haber activado sus suscripciones.

Procedimiento

1. Registre su sistema.

```
subscription-manager register --auto-attach
```

2. Adjunte sus suscripciones.
   - Puede utilizar una clave de activación para adjuntar suscripciones. Consulte Creación de claves de activación del Portal del Cliente de Red Hat para obtener más información.
   - Como alternativa, puede adjuntar manualmente una suscripción utilizando el ID del grupo de suscripciones (ID del grupo). Consulte Adjuntar y eliminar suscripciones a través de la línea de comandos.

Recursos adicionales

Recursos adicionales

- Creación de claves de activación del Portal del Cliente de Red Hat
- Adjuntar y eliminar suscripciones a través de la línea de comandos
- Uso y configuración de Red Hat Subscription Manager

CAPÍTULO 6. CONFIGURACIÓN DE RED HAT HIGH AVAILABILITY CLUSTER EN GOOGLE CLOUD PLATFORM

Este capítulo incluye información y procedimientos para configurar un cluster de alta disponibilidad (HA) de Red Hat en Google Cloud Platform (GCP) utilizando instancias de máquinas virtuales (VM) de Google Compute Engine (GCE) como nodos de cluster.

Este capítulo incluye los procedimientos necesarios para configurar su entorno para GCP. Una vez que haya configurado su entorno, puede crear y configurar instancias de VM.

Este capítulo también incluye procedimientos específicos para la creación de clústeres de alta disponibilidad, que transforman nodos individuales en un clúster de nodos de alta disponibilidad en GCP. Estos procedimientos incluyen la instalación de los paquetes y agentes de alta disponibilidad en cada nodo del clúster, la configuración de las cercas y la instalación de agentes de recursos de red.

Requisitos previos

- Debe estar inscrito en el programa Red Hat Cloud Access y tener suscripciones a RHEL sin utilizar. La suscripción adjunta debe incluir el acceso a los siguientes repositorios para cada instancia de GCP.
  - Red Hat Enterprise Linux 8 Server: rhel-8-server-rpms/8Server/x86_64
  - Red Hat Enterprise Linux 8 Server (Alta Disponibilidad): rhel-8-server-ha-rpms/8Server/x86_64
- Debe pertenecer a un proyecto activo de GCP y tener permisos suficientes para crear recursos en el proyecto.
- Su proyecto debe tener una cuenta de servicio que pertenezca a una instancia de VM y no a un usuario individual. Consulte Uso de la cuenta de servicio predeterminada de Compute Engine para obtener información sobre el uso de la cuenta de servicio predeterminada en lugar de crear una cuenta de servicio independiente.

Si usted o el administrador de su proyecto crean una cuenta de servicio personalizada, la cuenta de servicio debe ser configurada para los siguientes roles.

- Agente de rastreo en la nube
- Administración informática
- Administración de la red informática
- Usuario del almacén de datos en la nube
- Administración del registro
- Editor de control
- Monitorización del escritor de métricas
- Administrador de cuentas de servicio
- Administración del almacenamiento

Recursos adicionales

- Políticas de soporte para clusters de alta disponibilidad de RHEL - Protocolos de transporte
- Resumen de la red VPC
- Exploración de los componentes, conceptos y características de RHEL High Availability - Visión general de los protocolos de transporte
- Guía de diseño para clusters de alta disponibilidad de RHEL - Selección del protocolo de transporte

6.1. PAQUETES DE SISTEMA NECESARIOS

Los procedimientos en este capítulo asumen que usted está usando un sistema anfitrión que ejecuta Red Hat Enterprise Linux. Para completar con éxito los procedimientos, su sistema anfitrión debe tener instalados los siguientes paquetes.

Tabla 6.1. Paquetes del sistema

Paquete	Repositorio	Descripción
libvirt	rhel-8-for-x86_64-appstream-rpms	API, demonio y herramienta de gestión de código abierto para gestionar la virtualización de plataformas
virt-install	rhel-8-for-x86_64-appstream-rpms	Una utilidad de línea de comandos para crear máquinas virtuales
libguestfs	rhel-8-for-x86_64-appstream-rpms	Una biblioteca para acceder y modificar los sistemas de archivos de las máquinas virtuales
libguestfs-tools	rhel-8-for-x86_64-appstream-rpms	Herramientas de administración del sistema para máquinas virtuales; incluye la utilidad guestfish

6.2. OPCIONES DE IMAGEN DE RED HAT ENTERPRISE LINUX EN GCP

La siguiente tabla enumera las opciones de imagen y las diferencias entre ellas.

Tabla 6.2. Opciones de imagen

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones

Opción de imagen	Suscripciones	Ejemplo de escenario	Consideraciones
Elija desplegar una imagen personalizada que mueva a GCP.	Aproveche sus suscripciones existentes a Red Hat.	Habilite las suscripciones a través del programa Red Hat Cloud Access, cargue su imagen personalizada y adjunte sus suscripciones.	La suscripción incluye el coste del producto de Red Hat; usted paga todos los demás costes de la instancia. Las imágenes personalizadas que se trasladan a GCP se denominan imágenes de "Acceso a la nube" porque se aprovechan las suscripciones existentes de Red Hat. Red Hat proporciona soporte directamente para las imágenes de Cloud Access.
Elija desplegar una imagen de GCP existente que incluya RHEL.	Las imágenes de GCP incluyen un producto de Red Hat.	Elija una imagen RHEL cuando lance una instancia en GCP Compute Engine o elija una imagen de Google Cloud Platform Marketplace.	Usted paga a GCP por hora en un modelo de pago por uso. Estas imágenes se denominan imágenes "a la carta". GCP ofrece soporte para las imágenes bajo demanda a través de un acuerdo de soporte.

IMPORTANTE

No se puede convertir una instancia bajo demanda en una instancia de Red Hat Cloud Access. Para cambiar de una imagen bajo demanda a una imagen de Red Hat Cloud Access de suscripción propia (BYOS), cree una nueva instancia de Red Hat Cloud Access y migre los datos de su instancia bajo demanda. Cancele su instancia bajo demanda después de migrar sus datos para evitar la doble facturación.

El resto de este capítulo incluye información y procedimientos relativos a las imágenes personalizadas.

Recursos adicionales

- Red Hat en la nube pública
- Imágenes
- Guía de referencia de Red Hat Cloud Access
- Creación de una instancia a partir de una imagen personalizada

6.3. INSTALACIÓN DEL SDK DE GOOGLE CLOUD

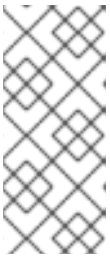
Complete los siguientes pasos para instalar el SDK de Google Cloud.

Requisitos previos

- Cree un proyecto en GCP si aún no lo ha hecho. Consulte Crear un nuevo proyecto en Google Cloud Platform para obtener más información.
- Asegúrese de que su sistema anfitrión incluye Python 2.7. Si no lo hace, instale Python 2.7.

Procedimiento

1. Siga las instrucciones de GCP para descargar y extraer el archivo del SDK de Google Cloud. Consulte el documento de GCP Quickstart for Linux para obtener más detalles.
2. Siga las mismas instrucciones para inicializar el SDK de Google Cloud.



NOTA

Una vez que haya inicializado el SDK de Google Cloud, puede utilizar los comandos de la CLI de **gcloud** para realizar tareas y obtener información sobre su proyecto e instancias. Por ejemplo, puede mostrar información del proyecto con el comando **gcloud compute project-info describe --project <project-name>**.

Recursos adicionales

- Inicio rápido para Linux
- referencia del comando gcloud
- visión general de la herramienta de línea de comandos gcloud

6.4. CREACIÓN DE UN CUBO DE IMÁGENES DE GCP

El siguiente documento incluye los requisitos mínimos para crear un cubo multirregional en su ubicación predeterminada.

Requisitos previos

Utilidad de almacenamiento de GCP (gsutil)

Procedimiento

1. Si aún no ha iniciado sesión en Google Cloud Platform, hágalo con el siguiente comando.

```
# gcloud auth login
```

2. Crear un cubo de almacenamiento.

```
$ gsutil mb gs://BucketName
```

Ejemplo:

```
$ gsutil mb gs://rhel-ha-bucket
```

Recursos adicionales

Hacer cubos

6.5. CREACIÓN DE UNA RED Y SUBRED DE NUBE PRIVADA VIRTUAL PERSONALIZADA

Complete los siguientes pasos para crear una red y una subred de nube privada virtual (VPC) personalizada.

Procedimiento

1. Inicie la consola de GCP.
2. Seleccione **VPC networks** en **Networking** en el panel de navegación izquierdo.
3. Haga clic en **Create VPC Network**
4. Introduzca un nombre para la red VPC.
5. En la página **New subnet**, cree un **Custom subnet** en la región en la que desea crear el clúster.
6. Haga clic en **Create**.

6.6. PREPARACIÓN E IMPORTACIÓN DE UNA IMAGEN BASE DE GCP

Complete los siguientes pasos para preparar la imagen para GCP.

Procedimiento

1. Introduzca el siguiente comando para convertir el archivo. Las imágenes cargadas en GCP deben estar en formato **raw** y llamarse **disk.raw**.

```
$ qemu-img convert -f qcow2 ImageName.qcow2 -O raw disk.raw
```

2. Introduzca el siguiente comando para comprimir el archivo **raw**. Las imágenes subidas a GCP deben estar comprimidas.

```
$ tar -Sczf ImageName.tar.gz disco.raw
```

3. Importe la imagen comprimida al cubo creado anteriormente.

```
$ gsutil cp ImageName.tar.gz gs://BucketName
```

6.7. CREACIÓN Y CONFIGURACIÓN DE UNA INSTANCIA BÁSICA DE GCP

Complete los siguientes pasos para crear y configurar una instancia de GCP que cumpla con los requisitos de funcionamiento y seguridad de GCP.

Procedimiento

1. Introduzca el siguiente comando para crear una imagen a partir del archivo comprimido en el cubo.

```
$ gcloud compute images create BaseImageName --source-uri
gs://BucketName/BaseImageName.tar.gz
```

Ejemplo:

```
[admin@localhost ~] $ gcloud compute images create rhel-76-server --source-uri gs://user-
rhelha/rhel-server-76.tar.gz
Created [https://www.googleapis.com/compute/v1/projects/MyProject/global/images/rhel-
server-76].
NAME          PROJECT                FAMILY  DEPRECATED  STATUS
rhel-76-server  rhel-ha-testing-on-gcp                     READY
```

2. Introduzca el siguiente comando para crear una instancia de plantilla a partir de la imagen. El tamaño mínimo requerido para una instancia RHEL base es n1-standard-2. Consulte gcloud compute instances create para conocer las opciones de configuración adicionales.

```
$ gcloud compute instances create BaseInstanceName --can-ip-forward --machine-type n1-
standard-2 --image BaseImageName --service-account ServiceAccountEmail
```

Ejemplo:

```
[admin@localhost ~] $ gcloud compute instances create rhel-76-server-base-instance --can-
ip-forward --machine-type n1-standard-2 --image rhel-76-server --service-account
account@project-name-on-gcp.iam.gserviceaccount.com
Created [https://www.googleapis.com/compute/v1/projects/rhel-ha-testing-on-gcp/zones/us-
east1-b/instances/rhel-76-server-base-instance].
NAME  ZONE  MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP
STATUS
rhel-76-server-base-instance  us-east1-bn1-standard-2          10.10.10.3  192.227.54.211
RUNNING
```

3. Conéctese a la instancia con una sesión de terminal SSH.

```
$ ssh root@DirecciónIPpública
```

4. Actualice el software RHEL.

   a. Regístrese en Red Hat Subscription Manager (RHSM).

   b. Habilitar un ID de grupo de suscripción (o utilizar el comando **--auto-attach**).

   c. Desactivar todos los repositorios.

```
# subscription-manager repos --disable=*
```

   d. Habilitar el siguiente repositorio.

```
# subscription-manager repos --enable=rhel-8-server-rpms
```

e. Ejecute el comando **yum update**.

```
# yum update -y
```

5. Instale el entorno invitado Linux de GCP en la instancia en ejecución (instalación in situ). Consulte Instalar el entorno de invitados en el lugar para obtener instrucciones.

6. Seleccione la opción **CentOS/RHEL**.

7. Copie la secuencia de comandos y péguela en el símbolo del sistema para ejecutar la secuencia de comandos inmediatamente.

8. Realice los siguientes cambios de configuración en la instancia. Estos cambios se basan en las recomendaciones de GCP para las imágenes personalizadas. Consulte la lista de imágenes de gcloudcompute para obtener más información.

a. Edite el archivo **/etc/chrony.conf** y elimine todos los servidores NTP.

b. Añade el siguiente servidor NTP.

```
metadata.google.internal iburst Servidor NTP de Google
```

c. Elimine cualquier regla de dispositivo de red persistente.

```
# rm -f /etc/udev/rules.d/70-persistent-net.rules

# rm -f /etc/udev/rules.d/75-persistent-net-generator.rules
```

d. Configure el servicio de red para que se inicie automáticamente.

```
# chkconfig network on
```

e. Configure el **sshd service** para que se inicie automáticamente.

```
# systemctl enable sshd
# systemctl is-enabled sshd
```

f. Introduzca el siguiente comando para ajustar la zona horaria a UTC.

```
# ln -sf /usr/share/zoneinfo/UTC /etc/localtime
```

g. (Opcional) Edite el archivo **/etc/ssh/ssh_config** y añada las siguientes líneas al final del archivo. Esto mantiene su sesión SSH activa durante largos períodos de inactividad.

```
# Server times out connections after several minutes of inactivity.
# Keep alive ssh connections by sending a packet every 7 minutes.
ServerAliveInterval 420
```

h. Edite el archivo **/etc/ssh/sshd_config** y haga los siguientes cambios, si es necesario. El ajuste **ClientAliveInterval 420** es opcional; esto mantiene su sesión SSH activa durante largos períodos de inactividad.

```
PermitRootLogin no
```

```
PasswordAuthentication no
AllowTcpForwarding yes
X11Forwarding no
PermitTunnel no
# Compute times out connections after 10 minutes of inactivity.
# Keep ssh connections alive by sending a packet every 7 minutes.
ClientAliveInterval 420
```

9. Introduzca el siguiente comando para desactivar el acceso con contraseña. Edite el archivo **/etc/cloud/cloud.cfg**.

```
ssh_pwauth from 1 to 0.
ssh_pwauth: 0
```

IMPORTANTE

Anteriormente, usted habilitó el acceso con contraseña para permitir el acceso a la sesión SSH para configurar la instancia. Debe desactivar el acceso con contraseña. Todo el acceso a la sesión SSH debe ser sin contraseña.

10. Introduzca el siguiente comando para anular el registro de la instancia desde el gestor de suscripciones.

```
# subscription-manager unregister
```

11. Introduzca el siguiente comando para limpiar el historial del shell. Mantenga la instancia en funcionamiento para el siguiente procedimiento.

```
# export HISTSIZE=0
```

6.8. CREACIÓN DE UNA IMAGEN INSTANTÁNEA

Complete los siguientes pasos para conservar los ajustes de configuración de la instancia y crear una instantánea.

Procedimiento

1. En la instancia en ejecución, introduzca el siguiente comando para sincronizar los datos en el disco.

```
# sync
```

2. En su sistema anfitrión, introduzca el siguiente comando para crear la instantánea.

```
$ gcloud compute disks snapshot InstanceName --snapshot-names SnapshotName
```

3. En su sistema anfitrión, introduzca el siguiente comando para crear la imagen configurada a partir de la instantánea.

```
$ gcloud compute images create ConfiguredImageFromSnapshot --source-snapshot
SnapshotName
```

Recursos adicionales

Creación de instantáneas de disco persistente

6.9. CREACIÓN DE UNA INSTANCIA DE PLANTILLA DE NODO DE HA Y DE NODOS DE HA

Una vez que haya configurado una imagen desde la instantánea, puede crear una plantilla de nodo. Utilice esta plantilla para crear todos los nodos de HA. Complete los siguientes pasos para crear la plantilla y los nodos de HA.

Procedimiento

1. Introduzca el siguiente comando para crear una plantilla de instancia.

```
$ gcloud compute instance-templates create InstanceTemplateName --can-ip-forward --
machine-type n1-standard-2  --image ConfiguredImageFromSnapshot --service-account
ServiceAccountEmailAddress
```

Ejemplo:

```
[admin@localhost ~] $ gcloud compute instance-templates create rhel-81-instance-template
--can-ip-forward --machine-type n1-standard-2 --image rhel-81-gcp-image --service-account
account@project-name-on-gcp.iam.gserviceaccount.com
Created [https://www.googleapis.com/compute/v1/projects/project-name-on-
gcp/global/instanceTemplates/rhel-81-instance-template].
NAME  MACHINE_TYPE   PREEMPTIBLE  CREATION_TIMESTAMP
rhel-81-instance-template   n1-standard-2          2018-07-25T11:09:30.506-07:00
```

2. Introduzca el siguiente comando para crear varios nodos en una zona.

```
# gcloud compute instances create NodeName01 NodeName02 --source-instance-template
InstanceTemplateName --zone RegionZone --network=NetworkName --
subnet=SubnetName
```

Ejemplo:

```
[admin@localhost ~] $ gcloud compute instances create rhel81-node-01 rhel81-node-02
rhel81-node-03 --source-instance-template rhel-81-instance-template --zone us-west1-b --
network=projectVPC --subnet=range0
Created [https://www.googleapis.com/compute/v1/projects/project-name-on-gcp/zones/us-
west1-b/instances/rhel81-node-01].
Created [https://www.googleapis.com/compute/v1/projects/project-name-on-gcp/zones/us-
west1-b/instances/rhel81-node-02].
Created [https://www.googleapis.com/compute/v1/projects/project-name-on-gcp/zones/us-
west1-b/instances/rhel81-node-03].
NAME          ZONE        MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP
STATUS
rhel81-node-01  us-west1-b  n1-standard-2            10.10.10.4   192.230.25.81   RUNNING
rhel81-node-02  us-west1-b  n1-standard-2            10.10.10.5   192.230.81.253  RUNNING
rhel81-node-03  us-east1-b  n1-standard-2            10.10.10.6   192.230.102.15  RUNNING
```

6.10. INSTALACIÓN DE PAQUETES Y AGENTES DE HA

Complete los siguientes pasos en todos los nodos.

Procedimiento

1. En la consola de Google Cloud, seleccione **Compute Engine** y, a continuación, seleccione **VM instances**.
2. Seleccione la instancia, haga clic en la flecha junto a **SSH**, y seleccione la opción de comando **View** gcloud.
3. Pegue este comando en una línea de comandos para acceder sin contraseña a la instancia.
4. Habilite el acceso a la cuenta sudo y regístrese en Red Hat Subscription Manager.
5. Habilitar un ID de grupo de suscripción (o utilizar el comando **--auto-attach**).
6. Desactivar todos los repositorios.

```
# subscription-manager repos --disable=*
```

7. Habilite los siguientes repositorios.

```
# subscription-manager repos --enable=rhel-8-server-rpms
# subscription-manager repos --enable=rhel-ha-for-rhel-8-server-rpms
```

8. Instale **pcs pacemaker**, los agentes de la valla y los agentes de los recursos.

```
# yum install -y pcs pacemaker fence-agents-gce resource-agents-gcp
```

9. Actualice todos los paquetes.

```
# yum update -y
```

6.11. CONFIGURACIÓN DE LOS SERVICIOS DE HA

Complete los siguientes pasos en todos los nodos para configurar los servicios de HA.

Procedimiento

1. El usuario **hacluster** fue creado durante la instalación de **pcs** y **pacemaker** en el paso anterior. Cree una contraseña para el usuario **hacluster** en todos los nodos del clúster. Utilice la misma contraseña para todos los nodos.

```
# passwd hacluster
```

2. Si el servicio **firewalld** está instalado, introduzca el siguiente comando para añadir el servicio HA.

```
# firewall-cmd --permanent --add-service=high-availability

# firewall-cmd --reload
```

3. Introduzca el siguiente comando para iniciar el servicio **pcs** y permitir que se inicie en el arranque.

```
# systemctl start pcsd.service

# systemctl enable pcsd.service

Created symlink from /etc/systemd/system/multi-user.target.wants/pcsd.service to
/usr/lib/systemd/system/pcsd.service.
```

Pasos de verificación

1. Asegúrese de que el servicio **pcsd** está funcionando.

```
# systemctl status pcsd.service

pcsd.service - PCS GUI and remote configuration interface
Loaded: loaded (/usr/lib/systemd/system/pcsd.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2018-06-25 19:21:42 UTC; 15s ago
Docs: man:pcsd(8)
man:pcs(8)
Main PID: 5901 (pcsd)
CGroup: /system.slice/pcsd.service
└─5901 /usr/bin/ruby /usr/lib/pcsd/pcsd > /dev/null &
```

2. Edite el archivo **/etc/hosts**. Añade los nombres de host RHEL y las direcciones IP internas de todos los nodos.

Recursos adicionales

¿Cómo debe configurarse el archivo /etc/hosts en los nodos del cluster RHEL?

6.12. CREACIÓN DE UN CLÚSTER

Complete los siguientes pasos para crear el cluster de nodos.

Procedimiento

1. En uno de los nodos, introduzca el siguiente comando para autenticar al usuario pcs. Especifique el nombre de cada nodo del clúster en el comando.

```
# pcs host auth  hostname1 hostname2 hostname3
Username: hacluster
Password:
hostname1: Authorized
hostname2: Authorized
hostname3: Authorized
```

2. Introduzca el siguiente comando para crear el cluster.

```
# pcs cluster setup cluster-name hostname1 hostname2 _hostname3-
```

Pasos de verificación

1. Ejecute el siguiente comando para permitir que los nodos se unan al clúster automáticamente cuando se inicie.

```
# pcs cluster enable --all
```

2. Introduzca el siguiente comando para iniciar el clúster.

```
# pcs cluster start --all
```

6.13. CREACIÓN DE UN DISPOSITIVO DE ESGRIMA

En la mayoría de las configuraciones por defecto, los nombres de las instancias de GCP y los nombres de los hosts de RHEL son idénticos.

Complete los siguientes pasos para crear un dispositivo de cercado.

Procedimiento

1. Introduzca el siguiente comando para obtener los nombres de las instancias de GCP. Tenga en cuenta que la salida también muestra el ID interno de la instancia.

```
# fence_gce --zone us-west1-b --project=rhel-ha-on-gcp -o list
```

Ejemplo:

```
Example:
[root@rhel81-node-01 ~]# fence_gce --zone us-west1-b --project=rhel-ha-testing-on-gcp -o
list
44358**********3181,InstanceName-3
40819**********6811,InstanceName-1
71736**********3341,InstanceName-2
```

2. Introduzca el siguiente comando para crear un dispositivo de valla.

```
# pcs stonith create _FenceDeviceName_ fence_gce zone=_Region-Zone_
project=_MyProject_
```

Paso de verificación

Compruebe que los dispositivos de la valla se han puesto en marcha.

```
# estado de las pcs
```

Ejemplo:

```
[root@rhel81-node-01 ~]# pcs status
Cluster name: gcp-cluster
Stack: corosync
Current DC: rhel81-node-02 (version 1.1.18-11.el7_5.3-2b07d5c5a9) - partition with quorum
Last updated: Fri Jul 27 12:53:25 2018
Last change: Fri Jul 27 12:51:43 2018 by root via cibadmin on rhel81-node-01

3 nodes configured
3 resources configured

Online: [ rhel81-node-01 rhel81-node-02 rhel81-node-03 ]
```

```
Full list of resources:

us-west1-b-fence    (stonith:fence_gce):    Started rhel81-node-01

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

6.14. CONFIGURACIÓN DE LA AUTORIZACIÓN DEL NODO GCP

Configure las herramientas del SDK de la nube para utilizar las credenciales de su cuenta para acceder a GCP.

Procedimiento

Introduzca el siguiente comando en cada nodo para inicializar cada nodo con su ID de proyecto y las credenciales de la cuenta.

```
# gcloud-ra init
```

6.15. CONFIGURACIÓN DEL AGENTE DE RECURSOS GCP-VCP-MOVE-VIP

El agente de recursos **gcp-vpc-move-vip** adjunta una dirección IP secundaria (alias IP) a una instancia en ejecución. Se trata de una dirección IP flotante que puede pasar entre diferentes nodos del clúster.

Introduzca el siguiente comando para mostrar más información sobre este recurso.

```
# pcs resource describe gcp-vpc-move-vip
```

Puede configurar el agente de recursos para que utilice un rango de direcciones de subred primario o un rango de direcciones de subred secundario. Esta sección incluye procedimientos para ambos rangos.

Primary subnet address range

Complete los siguientes pasos para configurar el recurso para la subred primaria de la VPC.

Procedimiento

1. Introduzca el siguiente comando para crear el recurso **aliasip**. Incluya una dirección IP interna no utilizada. Incluya el bloque CIDR en el comando.

   ```
   # pcs resource create aliasip gcp-vpc-move-vip  alias_ip=UnusedIPaddress/CIDRblock
   ```

   Ejemplo:

   ```
   root@rhel81-node-01 ~]# pcs resource create aliasip gcp-vpc-move-vip
   alias_ip=10.10.10.200/32
   ```

2. Introduzca el siguiente comando para crear un recurso **IPaddr2** para gestionar la IP en el nodo.

```
# pcs resource create vip IPaddr2 nic=interface ip=AliasIPaddress cidr_netmask=32
```

Ejemplo:

```
root@rhel81-node-01 ~]# pcs resource create vip IPaddr2 nic=eth0 ip=10.10.10.200
cidr_netmask=32
```

3. Introduzca el siguiente comando para agrupar los recursos de red en **vipgrp**.

```
# pcs resource group add vipgrp aliasip vip
```

Pasos de verificación

1. Introduzca el siguiente comando para verificar que los recursos se han iniciado y están agrupados en **vipgrp**.

```
[root@rhel81-node-01 ~]# pcs status
```

2. Introduzca el siguiente comando para verificar que el recurso puede moverse a un nodo diferente.

```
# pcs resource move vip _Node_
```

Ejemplo:

```
[root@rhel81-node-01 ~]# pcs resource move vip rhel81-node-03
```

3. Introduzca el siguiente comando para verificar que el **vip** se ha iniciado con éxito en un nodo diferente.

```
[root@rhel81-node-01 ~]# pcs status
```

Secondary subnet address range

Complete los siguientes pasos para configurar el recurso para un rango de direcciones de subred secundario.

Requisitos previos

Crear una red y una subred personalizadas

Procedimiento

1. Introduzca el siguiente comando para crear un rango de direcciones de subred secundario.

```
# gcloud-ra compute networks subnets update SubnetName --region RegionName --add-
second-ranges SecondarySubnetName=SecondarySubnetRange
```

Ejemplo:

```
# gcloud-ra compute networks subnets update range0 --region us-west1 --add-second-
ranges range1=10.10.20.0/24
```

2. Introduzca el siguiente comando para crear el recurso **aliasip**. Cree una dirección IP interna no utilizada en el rango de direcciones de la subred secundaria. Incluya el bloque CIDR en el comando.

```
# pcs resource create aliasip gcp-vpc-move-vip alias_ip=UnusedIPaddress/CIDRblock
```

Ejemplo:

```
root@rhel81-node-01 ~]# pcs resource create aliasip gcp-vpc-move-vip
alias_ip=10.10.20.200/32
```

3. Introduzca el siguiente comando para crear un recurso **IPaddr2** para gestionar la IP en el nodo.

```
# pcs resource create vip IPaddr2 nic=interface ip=AliasIPaddress cidr_netmask=32
```

Ejemplo:

```
root@rhel81-node-01 ~]# pcs resource create vip IPaddr2 nic=eth0 ip=10.10.20.200
cidr_netmask=32
```

4. Agrupe los recursos de red en **vipgrp**.

```
# pcs resource group add vipgrp aliasip vip
```

Pasos de verificación

1. Introduzca el siguiente comando para verificar que los recursos se han iniciado y están agrupados en **vipgrp**.

```
[root@rhel81-node-01 ~]# pcs status
```

2. Introduzca el siguiente comando para verificar que el recurso puede moverse a un nodo diferente.

```
# pcs resource move vip _Node_
```

Ejemplo:

```
[root@rhel81-node-01 ~]# pcs resource move vip rhel81-node-03
```

3. Introduzca el siguiente comando para verificar que el **vip** se ha iniciado con éxito en un nodo diferente.

```
[root@rhel81-node-01 ~]# pcs status
```