Red Hat Enterprise Linux 8

Implementando o Red Hat Enterprise Linux 8 em plataformas de nuvem pública

Criação de imagens personalizadas do Red Hat Enterprise Linux e configuração de um cluster Red Hat High Availability para plataformas de nuvem pública

Last Updated: 2021-03-07

Red Hat Enterprise Linux 8 Implementando o Red Hat Enterprise Linux 8 em plataformas de nuvem pública

Criação de imagens personalizadas do Red Hat Enterprise Linux e configuração de um cluster Red Hat High Availability para plataformas de nuvem 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.

Nota Legal

Copyright © 2021 | You need to change the HOLDER entity in the en-US/Deploying_Red_Hat_Enterprise_Linux_8_on_public_cloud_platforms.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Resumo

Você pode criar e implementar imagens personalizadas do Red Hat Enterprise Linux para várias plataformas de nuvem, incluindo Microsoft Azure, Amazon Web Services (AWS), e Google Cloud Platform (GCP). Você também pode criar e configurar um cluster Red Hat High Availability em cada plataforma em nuvem. Este documento inclui procedimentos para a criação de clusters HA, incluindo a instalação de pacotes e agentes necessários, a configuração de cercas e a instalação de agentes de recursos de rede. Cada fornecedor de nuvens tem seu próprio capítulo que descreve a criação e implantação de uma imagem personalizada. Há também um capítulo separado para a configuração de clusters de HA para cada fornecedor de nuvens.

Índice

TORNANDO O CÓDIGO ABERTO MAIS INCLUSIVO

A Red Hat tem o compromisso de substituir a linguagem problemática em nosso código, documentação e propriedades da web. Estamos começando com estes quatro termos: master, slave, blacklist e whitelist. Por causa da enormidade deste esforço, estas mudanças serão implementadas gradualmente ao longo de vários lançamentos futuros. Para mais detalhes, veja a mensagem de nosso CTO Chris Wright.

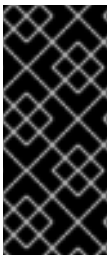
FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT

Agradecemos sua contribuição em nossa documentação. Por favor, diga-nos como podemos melhorá-la. Para fazer isso:

- Para comentários simples sobre passagens específicas:
  1. Certifique-se de que você está visualizando a documentação no formato *Multi-page HTML*. Além disso, certifique-se de ver o botão **Feedback** no canto superior direito do documento.
  2. Use o cursor do mouse para destacar a parte do texto que você deseja comentar.
  3. Clique no pop-up **Add Feedback** que aparece abaixo do texto destacado.
  4. Siga as instruções apresentadas.
- Para enviar comentários mais complexos, crie um bilhete Bugzilla:
  1. Ir para o site da Bugzilla.
  2. Como Componente, use **Documentation**.
  3. Preencha o campo **Description** com sua sugestão de melhoria. Inclua um link para a(s) parte(s) relevante(s) da documentação.
  4. Clique em **Submit Bug**.

CAPÍTULO 1. IMPLANTANDO UMA IMAGEM DO RED HAT ENTERPRISE LINUX 8 COMO UMA MÁQUINA VIRTUAL NO MICROSOFT AZURE

Você tem várias opções para implantar uma imagem do Red Hat Enterprise Linux (RHEL) 8 no Azure. Este capítulo discute suas opções para escolher uma imagem e lista ou se refere aos requisitos do sistema para seu sistema host e máquina virtual (VM). Este capítulo também fornece procedimentos para criar uma VM personalizada a partir de uma imagem ISO, carregando-a para o Azure, e lançando uma VM Azure.



IMPORTANTE

Enquanto você pode criar uma VM personalizada a partir de uma imagem ISO, a Red Hat recomenda que você use o produto Red Hat Image Builder para criar imagens personalizadas para uso em provedores de nuvem específicos. Com o Image Builder, você pode criar e carregar uma imagem Azure Disk Image (formato VHD). Veja Composição de uma imagem personalizada do sistema RHEL para mais informações.

Este capítulo se refere à documentação Azure em vários lugares. Para muitos procedimentos, consulte a documentação Azure referenciada para obter detalhes adicionais.

NOTA

Para uma lista de produtos Red Hat que você pode usar com segurança no Azure, consulte o Red Hat no Microsoft Azure.

Pré-requisitos

- Cadastre-se para uma conta no Portal do Cliente Red Hat .
- Inscreva-se em uma conta Microsoft Azure.
- Habilite suas assinaturas no programa Red Hat Cloud Access . O programa Red Hat Cloud Access permite que você transfira suas assinaturas da Red Hat de sistemas físicos ou locais para o Azure com total suporte da Red Hat.

Recursos adicionais

- Red Hat na Nuvem Pública
- Guia de Referência de Acesso à Nuvem da Red Hat
- Perguntas freqüentes e práticas recomendadas para o Microsoft Azure

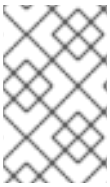
1.1. OPÇÕES DE IMAGEM DO RED HAT ENTERPRISE LINUX NO AZURE

A tabela a seguir lista as opções de imagem e anota as diferenças nas opções de imagem.

Tabela 1.1. Opções de imagem

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações
Opte por implantar uma Red Hat Gold Image.	Aproveite suas assinaturas de Red Hat existentes.	Habilite assinaturas através do programa Red Hat Cloud Access, e depois escolha uma Red Hat Gold Image no Azure. Veja o Guia de Referência de Acesso à Nuvem da Red Hat para detalhes sobre imagens douradas e como acessá-las no Azure.	A assinatura inclui o custo do produto Red Hat; você paga a Microsoft por todos os outros custos de instância. As imagens Gold da Red Hat são chamadas de imagens "Cloud Access" porque você aproveita suas assinaturas existentes da Red Hat. A Red Hat fornece suporte diretamente para as imagens de Cloud Access.
Opte por implantar uma imagem personalizada que você transfira para o Azure.	Aproveite suas assinaturas de Red Hat existentes.	Habilite as assinaturas através do programa Red Hat Cloud Access, faça o upload de sua imagem personalizada e anexe suas assinaturas.	A assinatura inclui o custo do produto Red Hat; você paga a Microsoft por todos os outros custos de instância. As imagens personalizadas que você move para o Azure são imagens "Cloud Access" porque você aproveita suas assinaturas Red Hat existentes. A Red Hat fornece suporte diretamente para imagens de Cloud Access.

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações
Opte por implantar uma imagem Azure existente que inclua a RHEL.	As imagens do Azure incluem um produto Red Hat.	Escolha uma imagem RHEL quando você criar uma VM usando o console Azure, ou escolha uma VM do Mercado Azure.	Você paga a Microsoft por hora em um modelo pay-as-you-go. Tais imagens são chamadas de "on-demand.\i Azure fornece suporte para imagens sob demanda através de um acordo de suporte. A Red Hat fornece atualizações das imagens. Azure disponibiliza as atualizações através da Infra-estrutura de Atualização da Red Hat (RHUI).



NOTA

Você pode criar uma imagem personalizada para o Azure usando o Red Hat Image Builder. Veja Composição de uma imagem personalizada do sistema RHEL para mais informações.

O restante deste capítulo inclui informações e procedimentos relativos às imagens personalizadas do Red Hat Enterprise Linux.

Recursos adicionais

- Imagens de ouro Red Hat em Microsoft Azure
- Programa Red Hat Cloud Access
- Mercado Azure
- Opções de faturamento no Mercado Azure
- Red Hat Enterprise Linux traz imagens douradas com inscrição em Azure

1.2. ENTENDENDO AS IMAGENS DE BASE

Esta seção inclui informações sobre o uso de imagens de base pré-configuradas e suas configurações.

1.2.1. Usando uma imagem de base personalizada

Para configurar manualmente uma VM, você começa com uma imagem VM de base (starter). Uma vez criada a imagem base da VM, você pode modificar as configurações e adicionar os pacotes que a VM requer para operar na nuvem. Você pode fazer alterações de configuração adicionais para sua aplicação específica depois de carregar a imagem.

Para preparar uma imagem da RHEL em nuvem, siga as instruções abaixo. Para preparar uma imagem de nuvem Hyper-V da RHEL, veja a seção Prepare uma máquina virtual baseada na Red Hat do Gerente Hyper-V.

Recursos adicionais

Red Hat Enterprise Linux

1.2.2. Pacotes de sistemas requeridos

Os procedimentos neste capítulo assumem que você está usando um sistema host rodando o Red Hat Enterprise Linux. Para completar os procedimentos com sucesso, seu sistema hospedeiro deve ter os seguintes pacotes instalados.

Tabela 1.2. Pacotes de sistemas

Pacote	Repositório	Descrição
libvirt	rhel-8-for-x86_64-appstream-rpms	API de código aberto, daemon e ferramenta de gerenciamento para gerenciar a virtualização da plataforma
virt-install	rhel-8-for-x86_64-appstream-rpms	Um utilitário de linha de comando para a construção de VMs
libguestfs	rhel-8-for-x86_64-appstream-rpms	Uma biblioteca para acesso e modificação de sistemas de arquivos VM
libguestfs-tools	rhel-8-for-x86_64-appstream-rpms	Ferramentas de administração do sistema para VMs; inclui o utilitário guestfish

1.2.3. Configurações de configuração da VM Azure

As VMs Azure devem ter as seguintes configurações. Algumas dessas configurações são ativadas durante a criação inicial da VM. Outras configurações são definidas ao provisionar a imagem da VM para o Azure. Mantenha estas configurações em mente à medida que você se move através dos procedimentos. Consulte-as conforme necessário.

Tabela 1.3. Configurações de configuração da VM

Configuração	Recomendação
ssh	ssh deve estar habilitado para fornecer acesso remoto aos seus VMs Azure.
dhcp	O adaptador virtual primário deve ser configurado para dhcp (somente IPv4).

Configuração	Recomendação
Troca de espaço	Não criar um arquivo swap dedicado ou partição swap. Você pode configurar o espaço swap com o Agente Linux Windows Azure (WALinuxAgent).
NIC	Escolha **virtio** para o adaptador de rede virtual principal.
criptografia	Para imagens personalizadas, use Network Bound Disk Encryption (NBDE) para criptografia completa de disco no Azure.

1.2.4. Criação de uma imagem de base a partir de uma imagem ISO

O procedimento a seguir lista as etapas e requisitos de configuração inicial para a criação de uma imagem ISO personalizada. Uma vez que você tenha configurado a imagem, você pode usar a imagem como modelo para criar instâncias VM adicionais.

Procedimento

1. Baixe a última imagem ISO do DVD Binário Red Hat Enterprise Linux 8 no Portal do Cliente Red Hat.
2. Certifique-se de ter habilitado sua máquina host para virtualização. Veja Habilitação de virtualização no RHEL 8 para informações e procedimentos.
3. Criar e iniciar um Red Hat Enterprise Linux VM básico. Veja Criando máquinas virtuais para instruções.
    a. Se você usar a linha de comando para criar sua VM, certifique-se de definir a memória padrão e as CPUs para a capacidade que você deseja para a VM. Defina sua interface de rede virtual para **virtio**.
    Segue uma amostra básica da linha de comando.

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

    b. Se você usar o console web para criar sua VM, siga o procedimento em Criar máquinas virtuais usando o console web, com estas advertências:
        - Não confira **Immediately Start VM**
        - Mude seu **Memory** e **Storage Size** para as configurações de sua preferência.
        - Antes de iniciar a instalação, certifique-se de ter alterado **Model** sob **Virtual Network Interface Settings** para **virtio** e altere seu **vCPUs** para as configurações de capacidade que deseja para a VM.
4. Reveja a seguinte seleção e modificações adicionais de instalação.

- Selecione **Minimal Install** com a opção **standard RHEL**.
- Para **Installation Destination**, selecione **Custom Storage Configuration**. Use as seguintes informações de configuração para fazer suas seleções.
  - Verificar pelo menos 500 MB para **/boot**.
  - Para sistema de arquivo, use xfs, ext4, ou ext3 tanto para partições **boot** como para **root**.
  - Remover o espaço de troca. O espaço de troca é configurado no servidor físico de lâminas em Azure pelo WALinuxAgent.
- Na tela **Installation Summary**, selecione **Network and Host Name**. Mude **Ethernet** para **On**.

5. Quando a instalação começa:
   - Crie uma senha **root**.
   - Criar uma conta de usuário administrativa.
6. Quando a instalação estiver completa, reinicie a VM e faça o login na conta raiz.
7. Uma vez logado como **root**, você pode configurar a imagem.

1.3. CONFIGURANDO A IMAGEM BASE PARA O MICROSOFT AZURE

A imagem base requer mudanças de configuração para servir como sua imagem RHEL 8 VM no Azure. As seções seguintes fornecem as mudanças adicionais de configuração que o Azure requer.

1.3.1. Instalação de drivers de dispositivos Hyper-V

A Microsoft fornece drivers de rede e dispositivos de armazenamento como parte de seus Serviços de Integração Linux (LIS) para o pacote Hyper-V. Talvez seja necessário instalar drivers de dispositivos Hyper-V na imagem da VM antes de provisioná-la como uma VM Azure. Use o comando **lsinitrd | grep hv** para verificar se os drivers estão instalados.

Procedimento

1. Digite o seguinte comando **grep** para determinar se os drivers do dispositivo Hyper-V necessários estão instalados.

```
# lsinitrd | grep hv
```

No exemplo abaixo, todos os drivers necessários estão 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
```

Se todos os motoristas não estiverem instalados, complete as demais etapas.

NOTA

Um motorista **hv_vmbus** pode existir no ambiente. Mesmo que este motorista esteja presente, complete os seguintes passos.

2. Crie um arquivo chamado **hv.conf** em **/etc/dracut.conf.d**.
3. Adicione os seguintes parâmetros de driver ao arquivo **hv.conf**.

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

NOTA

Observe os espaços antes e depois das citações, por exemplo, **add_drivers =" hv_vmbus "**. Isto garante que condutores únicos sejam carregados no caso de outros condutores Hyper-V já existirem no ambiente.

4. Regenerar a imagem **initramfs**.

```
# dracut -f -v --regenerar-tudo
```

Etapas de verificação

1. Reinicialize a máquina.
2. Execute o comando **lsinitrd | grep hv** para verificar se os drivers estão instalados.

1.3.2. Fazendo mudanças de configuração adicionais

A VM requer outras mudanças de configuração para operar no Azure. Execute o seguinte procedimento para fazer as mudanças adicionais.

Procedimento

1. Se necessário, potência sobre a VM.
2. Registre o VM e habilite o repositório do Red Hat Enterprise Linux 8.

```
# registro de gerenciador de assinaturas --auto-attach
```

Parar e remover as nuvens -init

1. Parar o serviço **cloud-init** (se presente).

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

2. Remova o software **cloud-init**.

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

Concluindo outras mudanças na VM

1. Edite o arquivo **/etc/ssh/sshd_config** e habilite a autenticação da senha.

```
SenhaAutenticação sim
```

2. Defina um nome genérico de anfitrião.

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

3. Editar (ou criar) o arquivo **/etc/sysconfig/network-scripts/ifcfg-eth0**. Use somente os parâmetros listados abaixo.

NOTA

O arquivo **ifcfg-eth0** não existe na imagem ISO do DVD RHEL 8 e deve ser criado.

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

4. Remover todas as regras persistentes de dispositivos de rede, se 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. Defina **ssh** para iniciar automaticamente.

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

6. Modificar os parâmetros de inicialização do kernel.

   a. Adicione **crashkernel=256M** ao início da linha **GRUB_CMDLINE_LINUX** no arquivo **/etc/default/grub**. Se **crashkernel=auto** estiver presente, mude-o para **crashkernel=256M**.

   b. Adicione as seguintes linhas ao final da linha **GRUB_CMDLINE_LINUX**, se não estiver presente.

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

c. Remova as seguintes opções, se presentes.

```
rhgb
quiet
```

7. Regenerar o arquivo **grub.cfg**.

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

8. Instalar e habilitar o Agente Linux Windows Azure (WALinuxAgent). O Red Hat Enterprise Linux 8 Application Stream (AppStream) inclui o WALinuxAgent. Veja Usando o AppStream para mais informações.

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

9. Edite as seguintes linhas no arquivo **/etc/waagent.conf** para configurar o espaço swap para VMs provisionadas. Configure espaço swap para o que for apropriado para suas VMs provisionadas.

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

Preparação para o fornecimento

1. Desregistrar o VM do Gerente de Assinaturas da Red Hat.

```
# não-registo do gerenciador de assinaturas
```

2. Preparar o VM para o provisionamento do Azure, limpando os detalhes de provisionamento existentes. O Azure reprovisa o VM em Azure. Este comando gera avisos, o que é esperado.

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

3. Limpe o histórico da casca e desligue a VM.

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

1.4. CONVERTENDO A IMAGEM PARA UM FORMATO VHD FIXO

Todas as imagens do Microsoft Azure VM devem estar em um formato fixo **VHD**. A imagem deve ser alinhada em um limite de 1 MB antes de ser convertida para VHD. Esta seção descreve como converter a imagem de **qcow2** para um formato **VHD** fixo e alinhar a imagem, se necessário. Uma vez convertida a imagem, você pode carregá-la para o Azure.

Procedimento

1. Converta a imagem de **qcow2** para o formato **raw**.

```
qemu-img converter -f qcow2 -O bruto <image-name>.qcow2 <image-name>.raw
```

2. Crie um roteiro de shell usando o conteúdo abaixo.

```
#!/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. Execute o roteiro. Este exemplo usa o nome **align.sh**.

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

- Se a mensagem *"Your image is already aligned. You do not need to resize."* for exibida, siga para o seguinte passo.
- Se um valor for exibido, sua imagem não está alinhada.

4. Use o seguinte comando para converter o arquivo para um formato **VHD** fixo.
The sample uses qemu-img version 2.12.0.

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

Uma vez convertido, o arquivo **VHD** está pronto para ser carregado no Azure.

Aligning the image

Complete os seguintes passos somente se o arquivo **raw** não estiver alinhado.

1. Redimensione o arquivo **raw** usando o valor arredondado exibido quando você executou o roteiro de verificação.

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

2. Converta o arquivo de imagem **raw** para um formato **VHD**.
The sample uses qemu-img version 2.12.0.

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

Uma vez convertido, o arquivo **VHD** está pronto para ser carregado no Azure.

1.5. INSTALANDO A CLI AZURE

Complete os seguintes passos para instalar a interface de linha de comando Azure (Azure CLI 2.1). Azure CLI 2.1 é um utilitário baseado em Python que cria e gerencia as VMs no Azure.

Pré-requisitos

- Você precisa ter uma conta no Microsoft Azure antes de poder usar o CLI Azure.
- A instalação do Azure CLI requer o Python 3.x.

Procedimento

1. Importar a chave do repositório Microsoft.

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

2. Criar uma entrada local no repositório Azure CLI.

```
sudo sh -c 'echo -e"[azure-cli]|Azure CLI=https://packages.microsoft.com/yumrepos/azure-
cli=https://packages.microsoft.com/keys/microsoft.asc===1ngpgcheck=1ngpgkey=https://packa
es.microsoft.com/keys/microsoft.asc=" > /etc/yum.repos.d/azure-cli.repo'
```

3. Atualizar o índice do pacote **yum**.

```
Data do check-up de $ yum
```

4. Verifique sua versão Python (**python --version**) e instale o Python 3.x, se necessário.

```
$ sudo yum instalar python3
```

5. Instale a CLI Azure.

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

6. Dirija a CLI Azure.

```
$ az
```

Recursos adicionais

- Azure CLI
- Referência de comando Azure CLI

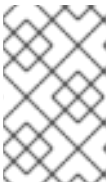
1.6. CRIANDO RECURSOS EM AZURE

Complete o seguinte procedimento para criar os recursos Azure de que você precisa antes de poder carregar o arquivo **VHD** e criar a imagem Azure.

Procedimento

1. Digite o seguinte comando para autenticar seu sistema com o Azure e faça o login.

```
$ az login
```



NOTA

Se um navegador estiver disponível em seu ambiente, o CLI abre seu navegador para a página de login no Azure. Veja Entrar com a CLI Azure para mais informações e opções.

2. Criar um grupo de recursos em uma região Azure.

```
Grupo az criar --nome <recurso grupo> --localização <azure-região>
```

Exemplo:

```
[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. Criar uma conta de armazenamento. Consulte Tipos de SKU para obter mais informações sobre valores válidos de SKU.

```
Conta de armazenamento az criar -l <azure-region> -n <storage-account-namee> -g
<resource-group> --sku <sku_type>
```

Exemplo:

```
[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/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. Obtenha o cordão de conexão da conta de armazenamento.

```
Conta de armazenamento az mostrar-conexão-corda -n <storage-conta-nomee> -g
<recurso-grupo>
```

Exemplo:

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

5. Exportar a cadeia de conexão copiando a cadeia de conexão e colando-a no seguinte comando. Esta cadeia de conexão conecta seu sistema à conta de armazenamento.

```
$ exportação AZURE_STORAGE_CONNECTION_STRING="<storage-connect-string>"
```

Exemplo:

```
export
AZURE_STORAGE_CONNECTION_STRING="DefaultEndpointsProtocol=https;EndpointSuffi
x=core.windows.net;AccountName=azrhelclistact;AccountKey=NreGk...=="
```

6. Criar o recipiente de armazenagem.

```
Container de armazenamento de $ az criar -n <container-nome >
```

Exemplo:

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

7. Criar uma rede virtual.

```
$ rede az vnet criar -g -YRFFGUNA grupo de recursos> --nome <vnet-nome -
terNGREGUNA- --subnet-nome <subnet-nome -terNGREGUNA-
```

Exemplo:

```
[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
  }
}
```

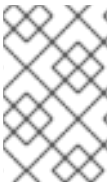
Recursos adicionais

- Visão geral dos discos administrados em Azure

- Tipos de unidades para estocagem

1.7. CARREGANDO E CRIANDO UMA IMAGEM AZURE

Complete os seguintes passos para carregar o arquivo **VHD** em seu container e criar uma imagem personalizada Azure.



NOTA

O fio de conexão de armazenamento exportado não persiste após um reinício do sistema. Se algum dos comandos nas etapas seguintes falhar, exportar a cadeia de conexão novamente.

Procedimento

1. Carregue o arquivo **VHD** para o recipiente de armazenamento. Pode levar vários minutos. Para obter uma lista de contêineres de armazenamento, digite o comando **az storage container list**.

```
$ az storage blob upload -- nome da conta <storage-nome da conta > -nome do recipiente <container-nome da conta > -- página tipo -- arquivo <path-to-vhd> -nome <image-nome da conta >.vhd
```

   Exemplo:

```
[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. Obtenha a URL para o arquivo **VHD** carregado para usar na etapa seguinte.

```
$ az storage blob url -c <container-name> -n <image-name>.vhd
```

   Exemplo:

```
[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. Criar a imagem personalizada Azure.

```
$ imagem az criar -n <image-nome > -g <recurso grupo> -l <azure-região> --source <URL> --os-type linux
```

NOTA

A geração padrão do hipervisor da VM é V1. Você pode opcionalmente especificar uma geração de hipervisor V2, incluindo a opção **--hyper-v-generation V2**. As VMs da Geração 2 utilizam uma arquitetura de inicialização baseada em UEFI. Veja Suporte para geração 2 VMs no Azure para informações sobre a geração 2 VMs.

O comando pode retornar o erro "Somente blobs formatados como VHDs podem ser importados." Este erro pode significar que a imagem não estava alinhada com o limite de 1 MB mais próximo antes de ser convertida para **VHD**.

Exemplo:

```
[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. CRIANDO E INICIANDO O VM EM AZURE

Os passos seguintes fornecem as opções mínimas de comando para criar uma VM de disco gerenciado Azure a partir da imagem. Veja az vm criar para opções adicionais.

Procedimento

1. Digite o seguinte comando para criar a VM.

NOTA

A opção **--generate-ssh-keys** cria um par de chaves públicas/privadas. Os arquivos de chave privada e pública são criados em ~/**.ssh** em seu sistema. A chave pública é adicionada ao arquivo **authorized_keys** no VM para o usuário especificado pela opção **--admin-username**. Veja Outros métodos de autenticação para informações adicionais.

```
az vm criar -g <recurso-grupo> -l <azure-região> -n <vm-nome_TERNGREGUNA- --vnet-
nome_YRFFGUNA-vnet-nome_TERNGREGUNA- --subrede <subrede-
nome_TERNGREGUNA- --size Standard_A2 --os-disk-name <simple-name > --admin-nome
de usuário <administrator-nome > --generate-ssh-keys --image <path-to-image>
```

Exemplo:

```
[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"
```

Note o **publicIpAddress**. Você precisa deste endereço para fazer o login no VM no passo seguinte.

2. Inicie uma sessão SSH e faça o login na 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 ~]$
```

Se você vir uma solicitação de usuário, você implantou com sucesso sua VM Azure.

Agora você pode ir até o portal Microsoft Azure e verificar os logs de auditoria e as propriedades de seus recursos. Você pode gerenciar suas VMs diretamente neste portal. Se você estiver gerenciando várias VMs, você deve usar o CLI Azure. A CLI Azure fornece uma interface poderosa para seus recursos no Azure. Entre **az --help** na CLI ou veja a referência do comando da CLI Azure para saber mais sobre os comandos que você usa para gerenciar suas VMs no Microsoft Azure.

1.9. OUTROS MÉTODOS DE AUTENTICAÇÃO

Embora recomendado para aumentar a segurança, o uso do par de chaves geradas pelo Azure não é necessário. Os exemplos a seguir mostram dois métodos para autenticação SSH.

Example 1: Estas opções de comando fornecem uma nova VM sem gerar um arquivo de chave pública. Elas permitem a autenticação SSH usando uma senha.

```
az vm criar -g <recurso-grupo> -l <azure-região> -n <vm-nome_TERNGREGUNA- --vnet-nome_YRFFGUNA-vnet-nome_TERNGREGUNA- --subrede <subrede-nome_TERNGREGUNA- -tamanho Standard_A2 --os-disk-name <simple-name> -authentication-type password --admin-username <administrator-name> --admin-password <ssh-password> --image <path-to-image>
```

```
$ ssh <admin-username>@<public-ip-address>
```

Example 2: Estas opções de comando fornecem uma nova VM Azure e permitem a autenticação SSH usando um arquivo de chave pública existente.

```
az vm criar -g <recurso-grupo> -l <azure-região> -n <vm-nome_TERNGREGUNA- --vnet-nome_YRFFGUNA-vnet-nome_TERNGREGUNA- --subrede <subrede-nome_TERNGREGUNA- --tamanho Standard_A2 --os-disk-name <simple-name> --admin-nome de usuário <administrator-name> --ssh-key-value <pato-a-existente-- -image <pato-a-imagem>
```

```
$ ssh -i <pato-a-existir-e-terNGREGUNA- <admin-username>@<public-ip-address>
```

1.10. ANEXANDO ASSINATURAS DA RED HAT

Complete os seguintes passos para anexar as assinaturas que você ativou anteriormente através do programa Red Hat Cloud Access.

Pré-requisitos

Você deve ter habilitado suas assinaturas.

Procedimento

1. Registre seu sistema.

```
registro de gerenciador de assinaturas --auto-attach
```

2. Anexe suas assinaturas.

   - Você pode usar uma chave de ativação para anexar as assinaturas. Consulte Criando Chaves de Ativação do Portal do Cliente Red Hat para mais informações.
   - Alternativamente, você pode anexar manualmente uma assinatura usando o ID do pool de assinaturas (Pool ID). Veja Anexar e remover assinaturas através da Linha de Comando .

Recursos adicionais

- Criando as chaves de ativação do Portal do Cliente Red Hat
- Anexar e remover assinaturas através da linha de comando
- Uso e configuração do Red Hat Subscription Manager

CAPÍTULO 2. CONFIGURAÇÃO DE UM CLUSTER RED HAT HIGH AVAILABILITY NO MICROSOFT AZURE

Este capítulo inclui informações e procedimentos para configurar um cluster Red Hat High Availability (HA) no Azure usando instâncias da máquina virtual Azure (VM) como nós de cluster. Os procedimentos neste capítulo assumem que você está criando uma imagem personalizada para o Azure. Você tem uma série de opções para obter as imagens RHEL 8 que você utiliza para seu cluster. Consulte Opções de Imagem do Red Hat Enterprise Linux no Azure para obter informações sobre as opções de imagem para o Azure.

Este capítulo inclui procedimentos prévios para a criação de seu ambiente para o Azure. Uma vez que você tenha configurado seu ambiente, você pode criar e configurar instâncias do Azure VM.

O capítulo também inclui procedimentos específicos para a criação de clusters de HA, que transformam nós individuais em um cluster de nós HA em Azure. Estes incluem procedimentos para instalação dos pacotes e agentes de alta disponibilidade em cada nó de cluster, configuração de cercas e instalação de agentes de recursos de rede Azure.

O capítulo se refere à documentação Azure em vários lugares. Para muitos procedimentos, consulte a documentação Azure referenciada para mais informações.

Pré-requisitos

- Cadastre-se para uma conta no Portal do Cliente Red Hat .
- Inscreva-se em uma conta Microsoft Azure com privilégios de administrador.
- Você precisa instalar a interface de linha de comando Azure (CLI). Para mais informações, consulte Seção 1.5, “Instalando a CLI Azure” .
- Habilite suas assinaturas no programa Red Hat Cloud Access . O programa Red Hat Cloud Access permite que você transfira suas assinaturas da Red Hat de sistemas físicos ou locais para o Azure com total suporte da Red Hat.

Recursos adicionais

- Políticas de apoio aos Clusters de Alta Disponibilidade RHEL - Máquinas Virtuais Microsoft Azure como Membros do Cluster
- Configuração e Gerenciamento de Aglomerados de Alta Disponibilidade

2.1. CRIANDO RECURSOS EM AZURE

Complete o seguinte procedimento para criar uma região, grupo de recursos, conta de armazenamento, rede virtual e conjunto de disponibilidade. Você precisa destes recursos para completar as tarefas subseqüentes neste capítulo.

Procedimento

1. Autentique seu sistema com Azure e faça o login.

```
$ az login
```

NOTA

Se um navegador estiver disponível em seu ambiente, o CLI abre seu navegador para a página de login no Azure.

Exemplo:

```
[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. Criar um grupo de recursos em uma região Azure.

```
Grupo az criar --nome resource-group --local azure-region
```

Exemplo:

```
[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. Criar uma conta de armazenamento.

```
$ az criar conta de armazenamento -l azure-region -n storage-account-name -g resource-
group --sku sku_type --kind StorageV2
```

Exemplo:

```
[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. Obtenha o cordão de conexão da conta de armazenamento.

```
Conta de armazenamento az mostrar-conexão de fio -n storage-account-name -g resource-
group
```

Exemplo:


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


5. Exportar a cadeia de conexão copiando a cadeia de conexão e colando-a no seguinte comando. Esta cadeia de conexão conecta seu sistema à conta de armazenamento.

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

Exemplo:

```
export
AZURE_STORAGE_CONNECTION_STRING="DefaultEndpointsProtocol=https;EndpointSuffi
x=core.windows.net;AccountName=azrhelclistact;AccountKey=NreGk...=="
```

6. Criar o recipiente de armazenagem.

```
Container de armazenamento $ az criar -n container-name
```

Exemplo:

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

7. Criar uma rede virtual. Todos os nós de cluster devem estar na mesma rede virtual.

```
$ az rede vnet criar -g resource group --nome vnet-name --subnet-nome subnet-name
```

Exemplo:

```
[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. Criar um conjunto de disponibilidade. Todos os nós de cluster devem estar no mesmo conjunto de disponibilidade.

```
$ az vm-disponibilidade -conjunto criar --nome MyAvailabilitySet --recurso-grupo
MyResourceGroup
```

Exemplo:

```
[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 adicionais

- Assine com o Azure CLI
- Tipos de unidades para estocagem
- Visão geral dos discos administrados em Azure

2.2. PACOTES DE SISTEMA NECESSÁRIOS PARA ALTA DISPONIBILIDADE

O procedimento assume que você está criando uma imagem VM para o Azure HA usando o Red Hat Enterprise Linux. Para completar o procedimento com sucesso, os seguintes pacotes devem ser instalados.

Tabela 2.1. Pacotes de sistemas

Pacote	Repositório	Descrição

Pacote	Repositório	Descrição
libvirt	rhel-8-for-x86_64-appstream-rpms	API de código aberto, daemon e ferramenta de gerenciamento para gerenciar a virtualização da plataforma
virt-install	rhel-8-for-x86_64-appstream-rpms	Um utilitário de linha de comando para a construção de VMs
libguestfs	rhel-8-for-x86_64-appstream-rpms	Uma biblioteca para acesso e modificação de sistemas de arquivos VM
libguestfs-tools	rhel-8-for-x86_64-appstream-rpms	Ferramentas de administração do sistema para VMs; inclui o utilitário guestfish

2.3. CONFIGURAÇÕES DE CONFIGURAÇÃO DA VM AZURE

As VMs Azure devem ter as seguintes configurações. Algumas dessas configurações são ativadas durante a criação inicial da VM. Outras configurações são definidas ao provisionar a imagem da VM para o Azure. Mantenha estas configurações em mente à medida que você se move através dos procedimentos. Consulte-as conforme necessário.

Tabela 2.2. Configurações de configuração da VM

Configuração	Recomendação
ssh	ssh deve estar habilitado para fornecer acesso remoto aos seus VMs Azure.
dhcp	O adaptador virtual primário deve ser configurado para dhcp (somente IPv4).
Troca de espaço	Não criar um arquivo swap dedicado ou partição swap. Você pode configurar o espaço swap com o Agente Linux Windows Azure (WALinuxAgent).
NIC	Escolha **virtio** para o adaptador de rede virtual principal.
criptografia	Para imagens personalizadas, use Network Bound Disk Encryption (NBDE) para criptografia completa de disco no Azure.

2.4. INSTALAÇÃO DE DRIVERS DE DISPOSITIVOS HYPER-V

A Microsoft fornece drivers de rede e dispositivos de armazenamento como parte de seus Serviços de

Integração Linux (LIS) para o pacote Hyper-V. Talvez seja necessário instalar drivers de dispositivos Hyper-V na imagem da VM antes de provisioná-la como uma VM Azure. Use o comando **lsinitrd | grep hv** para verificar se os drivers estão instalados.

Procedimento

1. Digite o seguinte comando **grep** para determinar se os drivers do dispositivo Hyper-V necessários estão instalados.

```
# lsinitrd | grep hv
```

No exemplo abaixo, todos os drivers necessários estão 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
```

Se todos os motoristas não estiverem instalados, complete as demais etapas.

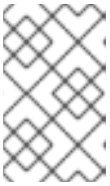
NOTA

Um motorista **hv_vmbus** pode existir no ambiente. Mesmo que este motorista esteja presente, complete os seguintes passos.

2. Crie um arquivo chamado **hv.conf** em **/etc/dracut.conf.d**.

3. Adicione os seguintes parâmetros de driver ao arquivo **hv.conf**.

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



NOTA

Observe os espaços antes e depois das citações, por exemplo, **add_drivers =" hv_vmbus "**. Isto garante que condutores únicos sejam carregados no caso de outros condutores Hyper-V já existirem no ambiente.

4. Regenerar a imagem **initramfs**.

```
# dracut -f -v --regenerar-tudo
```

Etapas de verificação

1. Reinicialize a máquina.

2. Execute o comando **lsinitrd | grep hv** para verificar se os drivers estão instalados.

2.5. FAZENDO MUDANÇAS DE CONFIGURAÇÃO ADICIONAIS

A VM requer outras mudanças de configuração para operar no Azure. Execute o seguinte procedimento para fazer as mudanças adicionais.

Procedimento

1. Se necessário, potência sobre a VM.
2. Registre o VM e habilite o repositório do Red Hat Enterprise Linux 8.

```
# registro de gerenciador de assinaturas --auto-attach
```

Parar e remover as nuvens -init

1. Parar o serviço **cloud-init** (se presente).

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

2. Remova o software **cloud-init**.

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

Concluindo outras mudanças na VM

1. Edite o arquivo **/etc/ssh/sshd_config** e habilite a autenticação da senha.

```
SenhaAutenticação sim
```

2. Defina um nome genérico de anfitrião.

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

3. Editar (ou criar) o arquivo **/etc/sysconfig/network-scripts/ifcfg-eth0**. Use somente os parâmetros listados abaixo.

NOTA

O arquivo **ifcfg-eth0** não existe na imagem ISO do DVD RHEL 8 e deve ser criado.

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

4. Remover todas as regras persistentes de dispositivos de rede, se 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. Defina **ssh** para iniciar automaticamente.

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

6. Modificar os parâmetros de inicialização do kernel.

   a. Adicione **crashkernel=256M** ao início da linha **GRUB_CMDLINE_LINUX** no arquivo **/etc/default/grub**. Se **crashkernel=auto** estiver presente, mude-o para **crashkernel=256M**.

   b. Adicione as seguintes linhas ao final da linha **GRUB_CMDLINE_LINUX**, se não estiver presente.

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

   c. Remova as seguintes opções, se presentes.

```
rhgb
quiet
```

7. Regenerar o arquivo **grub.cfg**.

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

8. Instalar e habilitar o Agente Linux Windows Azure (WALinuxAgent). O Red Hat Enterprise Linux 8 Application Stream (AppStream) inclui o WALinuxAgent. Veja Usando o AppStream para mais informações.

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

9. Edite as seguintes linhas no arquivo **/etc/waagent.conf** para configurar o espaço swap para VMs provisionadas. Configure espaço swap para o que for apropriado para suas VMs provisionadas.

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

Preparação para o fornecimento

1. Desregistrar o VM do Gerente de Assinaturas da Red Hat.

```
# não-registo do gerenciador de assinaturas
```

2. Preparar o VM para o provisionamento do Azure, limpando os detalhes de provisionamento existentes. O Azure reprovisa o VM em Azure. Este comando gera avisos, o que é esperado.

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

3. Limpe o histórico da casca e desligue a VM.

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

2.6. CRIANDO UMA APLICAÇÃO DO AZURE ACTIVE DIRECTORY

Complete o seguinte procedimento para criar uma Aplicação Azure AD. A Aplicação Azure AD autoriza e automatiza o acesso para operações HA para todos os nós do cluster.

Pré-requisitos

Instalar a Interface de Linha de Comando Azure (CLI) .

Procedimento

1. Certifique-se de ser um Administrador ou Proprietário para a assinatura do Microsoft Azure. Você precisa desta autorização para criar um aplicativo Azure AD.

2. Faça o login em sua conta Azure.

```
$ az login
```

3. Digite o seguinte comando para criar a Aplicação Azure AD. Para usar sua própria senha, adicione a opção **--password** ao comando. Assegure-se de criar uma senha forte.

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

Exemplo:

```
[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. Salve as seguintes informações antes de prosseguir. Você precisa destas informações para montar o agente de esgrima.

   - Azure AD ID de aplicação
   - Senha de aplicação Azure AD
   - Identificação do locatário

- ID de Assinatura Microsoft Azure

Recursos adicionais

Veja o acesso que um usuário tem aos recursos Azure

2.7. CONVERTENDO A IMAGEM PARA UM FORMATO VHD FIXO

Todas as imagens do Microsoft Azure VM devem estar em um formato fixo **VHD**. A imagem deve ser alinhada em um limite de 1 MB antes de ser convertida para VHD. Esta seção descreve como converter a imagem de **qcow2** para um formato **VHD** fixo e alinhar a imagem, se necessário. Uma vez convertida a imagem, você pode carregá-la para o Azure.

Procedimento

1. Converta a imagem de **qcow2** para o formato **raw**.

```
qemu-img converter -f qcow2 -O bruto <image-name>.qcow2 <image-name>.raw
```

2. Crie um roteiro de shell usando o conteúdo abaixo.

```
#!/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. Execute o roteiro. Este exemplo usa o nome **align.sh**.

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

- Se a mensagem *"Your image is already aligned. You do not need to resize."* for exibida, siga para o seguinte passo.

- Se um valor for exibido, sua imagem não está alinhada.

4. Use o seguinte comando para converter o arquivo para um formato **VHD** fixo.
The sample uses qemu-img version 2.12.0.

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

Uma vez convertido, o arquivo **VHD** está pronto para ser carregado no Azure.

Aligning the image

Complete os seguintes passos somente se o arquivo **raw** não estiver alinhado.

1. Redimensione o arquivo **raw** usando o valor arredondado exibido quando você executou o roteiro de verificação.

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

2. Converta o arquivo de imagem **raw** para um formato **VHD**.
The sample uses qemu-img version 2.12.0.

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

Uma vez convertido, o arquivo **VHD** está pronto para ser carregado no Azure.

2.8. CARREGANDO E CRIANDO UMA IMAGEM AZURE

Complete os seguintes passos para carregar o arquivo **VHD** em seu container e criar uma imagem personalizada Azure.

NOTA

O fio de conexão de armazenamento exportado não persiste após um reinício do sistema. Se algum dos comandos nas etapas seguintes falhar, exportar a cadeia de conexão novamente.

Procedimento

1. Carregue o arquivo **VHD** para o recipiente de armazenamento. Pode levar vários minutos. Para obter uma lista de contêineres de armazenamento, digite o comando **az storage container list**.

```
$ az storage blob upload -- nome da conta <storage-nome da conta > -nome do recipiente
<container-nome da conta > -- página tipo -- arquivo <path-to-vhd> -nome <image-nome da
conta >.vhd
```

Exemplo:

```
[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. Obtenha a URL para o arquivo **VHD** carregado para usar na etapa seguinte.

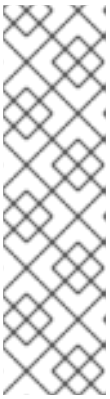
```
$ az storage blob url -c <container-name> -n <image-name>.vhd
```

Exemplo:

```
[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. Criar a imagem personalizada Azure.

```
$ imagem az criar -n <image-nome > -g <recurso grupo> -l <azure-região> --source <URL> -
-os-type linux
```



NOTA

A geração padrão do hipervisor da VM é V1. Você pode opcionalmente especificar uma geração de hipervisor V2, incluindo a opção **--hyper-v-generation V2**. As VMs da Geração 2 utilizam uma arquitetura de inicialização baseada em UEFI. Veja Suporte para geração 2 VMs no Azure para informações sobre a geração 2 VMs.

O comando pode retornar o erro "Somente blobs formatados como VHDs podem ser importados." Este erro pode significar que a imagem não estava alinhada com o limite de 1 MB mais próximo antes de ser convertida para **VHD**.

Exemplo:

```
[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. INSTALAÇÃO DE PACOTES E AGENTES RED HAT HA

Complete os seguintes passos em todos os nós.

Procedimento

1. Iniciar uma sessão terminal SSH e conectar-se à VM usando o nome do administrador e o endereço IP público.

```
$ ssh administrador@PublicIP
```

Para obter o endereço IP público de uma VM Azure, abra as propriedades da VM no Portal Azure ou digite o seguinte comando da CLI Azure.

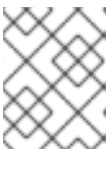
```
$ az vm lista -g <recursos- grupo> -d -- tabela de saída
```

Exemplo:

```
[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. Registrar a VM com o Red Hat.

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



NOTA

Se o comando **--auto-attach** falhar, registre manualmente o VM em sua assinatura.

3. Desativar todos os repositórios.

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

4. Habilitar os repositórios RHEL 8 Server e RHEL 8 Server HA.

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

5. Atualizar todos os pacotes.

```
# yum update -y
```

6. Instale os pacotes de software Red Hat High Availability Add-On, junto com todos os agentes de cercas disponíveis no canal High Availability.

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

7. O usuário **hacluster** foi criado durante a instalação de pcs e marcapassos na etapa anterior. Crie uma senha para **hacluster** em todos os nós de cluster. Use a mesma senha para todos os nós.

```
# hacluster da senha
```

8. Adicione o serviço **high availability** ao Firewall RHEL se **firewalld.service** estiver instalado.

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

9. Inicie o serviço **pcs** e habilite-o a começar na inicialização.

```
# 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.
```

Etapa de verificação

Certifique-se de que o serviço **pcs** esteja 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. CRIAÇÃO DE UM CLUSTER

Complete os seguintes passos para criar o conjunto de nós.

Procedimento

1. Em um dos nós, digite o seguinte comando para autenticar o usuário do pcs **hacluster**. No comando, especifique o nome de cada nó do cluster.

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

   Exemplo:

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

2. Criar o conjunto.

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

   Exemplo:

```
[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
```

Etapas de verificação

1. Habilite o conjunto.

```
[root@node01 clouduser]# pcs cluster enable --tudo
```

2. Comece o agrupamento.

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

   Exemplo:

```
[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. VISÃO GERAL DA VEDAÇÃO

Se a comunicação com um único nó do cluster falhar, então outros nós do cluster devem ser capazes de restringir ou liberar o acesso a recursos aos quais o nó de cluster falhado possa ter acesso. Isto não pode ser feito contatando o próprio nó de cluster, pois o nó de cluster pode não ser responsivo. Ao invés disso, deve-se fornecer um método externo, que é chamado de vedação com um agente de vedação.

Um nó que não responde ainda pode estar acessando dados. A única maneira de ter certeza de que seus dados estão seguros é cercando o nó usando STONITH. STONITH é um acrônimo para "Shoot The Other Node In The Head" e protege seus dados de serem corrompidos por nós desonestos ou acessos simultâneos. Usando STONITH, você pode ter certeza de que um nó está verdadeiramente offline antes de permitir que os dados sejam acessados de outro nó.

Recursos adicionais

Esgrima no grupo de alta disponibilidade da Red Hat

2.12. CRIANDO UM DISPOSITIVO DE ESGRIMA

Complete os seguintes passos para configurar a vedação. Complete estes comandos a partir de qualquer nó do agrupamento

Pré-requisitos

Você precisa definir a propriedade do cluster **stonith-enabled** para **true**.

Procedimento

1. Identificar o nome do nó Azure para cada RHEL VM. Você usa os nomes dos nós Azure para configurar o dispositivo de cerca.

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

   Exemplo:

   ```
   [root@node01 clouduser]# fence_azure_arm -l e04a6a49-9f00-xxxx-xxxx-a8bdda4af447 -p
   z/a05AwCN0IzAjVwXXXXXXXXEWIoeVp0xg7QT//JE= --resourceGroup azrhelclirsgrp --
   tenantId 77ecefb6-cff0-XXXX-XXXX-757XXXX9485 --subscriptionId XXXXXXXX-38b4-4527-
   XXXX-012d49dfc02c -o list
   node01,
   node02,
   node03,
   ```

2. Veja as opções para o agente Azure ARM STONITH.

```
pcs stonith descrevem o braço_de_armação
```

Exemplo:

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

ATENÇÃO

Para agentes de cerca que fornecem uma opção de método, não especifique um valor de ciclo, pois não é suportado e pode causar corrupção de dados.

Alguns dispositivos de cerca podem cercar apenas um único nó, enquanto outros dispositivos podem cercar vários nós. Os parâmetros que você especifica ao criar um dispositivo de cerca dependem do que seu dispositivo de cerca suporta e requer.

Você pode usar o parâmetro **pcmk_host_list** ao criar um dispositivo de esgrima para especificar todas as máquinas que são controladas por esse dispositivo de esgrima.

Você pode usar o parâmetro **pcmk_host_map** ao criar um dispositivo de cercas para mapear os nomes dos anfitriões de acordo com as especificações que compreendem o dispositivo de cercas.

3. Criar um dispositivo de cercas.

```
# pcs stonith criar clusterfence fence_azure_arm
```

4. Teste o agente de esgrima para um dos outros nós.

```
# pcs cerca de pedra azurenodename
```

Exemplo:

```
[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. Iniciar o nó que foi cercado na etapa anterior.

```
# pcs cluster start hostname
```

6. Verifique o status para verificar o nó iniciado.

```
# pcs status
```

Exemplo:

```
[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 adicionais

- Esgrima em um grupo de alta disponibilidade de chapéu vermelho
- Propriedades Gerais dos Dispositivos de Esgrima

2.13. CRIAÇÃO DE UM EQUILIBRADOR DE CARGA INTERNO AZURE

O equilibrador de carga interno Azure remove os nós de cluster que não respondem aos pedidos de sondas de saúde.

Realizar o seguinte procedimento para criar um equilibrador de carga interno Azure. Cada passo faz referência a um procedimento específico da Microsoft e inclui as configurações para personalizar o equilibrador de carga para HA.

Pré-requisitos

Painel de controle Azure

Procedimento

1. Criar um equilibrador de carga básico . Selecione **Internal load balancer**, o **Basic SKU**, e **Dynamic** para o tipo de atribuição de endereço IP.

2. Criar um grupo de endereços back-end . Associar o grupo de endereços back-end ao conjunto de disponibilidade criado durante a criação dos recursos Azure no HA. Não defina nenhuma configuração IP de rede alvo.

3. Criar uma sonda de saúde . Para a sonda de saúde, selecione **TCP** e entre na porta **61000**. Você pode usar o número da porta TCP que não interfira com outro serviço. Para certas aplicações de produtos HA (por exemplo, SAP HANA e SQL Server), você pode precisar trabalhar com a Microsoft para identificar a porta correta a ser utilizada.

4. Criar uma regra de balanceamento de carga . Para criar a regra de balanceamento de carga, os valores padrão são pré-populados. Certifique-se de definir **Floating IP (direct server return)** para **Enabled**.

2.14. CONFIGURAÇÃO DO AGENTE EQUILIBRADOR DE RECURSOS DE CARGA

Após ter criado a sonda de saúde, você deve configurar o agente de recursos **load balancer**. Este agente de recursos executa um serviço que responde aos pedidos de sonda de saúde do equilibrador de carga Azure e remove os nós de cluster que não respondem aos pedidos.

Procedimento

1. Instale os agentes de recursos **nmap-ncat** em todos os nós.

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

   Execute as seguintes etapas em um único nó.

2. Crie os recursos e o grupo **pcs**. Use seu balanceador de carga FrontendIP para o endereço IPaddr2.

```
# pcs resource create resource-name IPaddr2 ip=\i10.0.0.7\i1 -- grupo cluster-resources-group
```

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

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

Etapa de verificação

Corra **pcs status** para ver os resultados.

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

Exemplo:

```
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. CONFIGURAÇÃO DE ARMAZENAMENTO EM BLOCO COMPARTILHADO

Esta seção fornece um procedimento opcional para configurar o armazenamento em bloco compartilhado para um cluster Red Hat High Availability com discos compartilhados Microsoft Azure. O procedimento assume três VMs Azure (um cluster de três nós) com um disco compartilhado de 1 TB.

NOTA

Este é um procedimento de amostra autônomo para configurar o armazenamento em bloco. O procedimento pressupõe que você ainda não tenha criado seu agrupamento.

Pré-requisitos

- Você deve ter instalado o Azure CLI em seu sistema host e criado sua(s) chave(s) SSH.
- Você deve ter criado seu ambiente de cluster no Azure, o que inclui a criação dos seguintes recursos. Os links são para a documentação do Microsoft Azure.
  - Grupo de recursos
  - Rede virtual
  - Grupo(s) de segurança de rede
  - Regras do grupo de segurança de rede
  - Sub-rede(s)
  - Balanceador de carga (opcional)

- Conta de armazenamento
- Grupo de colocação de proximidade
- Conjunto de disponibilidade

Procedimento

1. Criar um volume de blocos compartilhados usando o 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 exemplo, o seguinte comando cria um volume de blocos compartilhados chamado **shared-block-volume.vhd** no grupo de recursos **sharedblock** dentro da Zona de Disponibilidade do 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. Verifique se você criou o volume de blocos compartilhados usando o comando Azure **az disk show**.

```
Az disk show -g <resource_group> -n <shared_block_volume_name>
```

Por exemplo, o seguinte comando mostra detalhes do volume do bloco compartilhado **shared-block-volume.vhd** dentro do 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. Criar três interfaces de rede usando o comando Azure **az network nic create**. Execute o seguinte comando três vezes usando um diferente **<nic_name>** para cada um.

```
az rede nic criar -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 exemplo, o seguinte comando cria uma interface de rede com o nome **shareblock-nodea-vm-nic-protected**.

```
az rede nic criar -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-adersion IPv4
```

4. Criar três VMs e anexar o volume do bloco compartilhado usando o comando Azure **az vm create**. Os valores das opções são os mesmos para cada VM, exceto que cada VM tem seu próprio **<vm_name>**, **<new_vm_disk_name>**, e **<nic_name>**.

```
az vm create -n <vm_name> -g <resource_group> --attach-data-discos <shared_block_volume_name> --data-disk-caching Nenhum --os-disk-caching ReadWrite --os-disk-name <new-vm-disk-name> --os-disk-size-gb <disk_size> --location <location> --tamanho <virtual_machine_size> --imagem <imagem_nome_da_imagem> --admin-nome_de_utilizador <vm_username> -autenticação-tipo ssh --ssh-valores-chave <ssh_key> --nics <nic_name> --availability-set <availability_set> --ppg <proximity_placement_group>
```

Por exemplo, o seguinte comando cria uma VM chamada **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": ""
}
```

Etapas de verificação

1. Para cada VM de seu cluster, verifique se o dispositivo de bloco está disponível usando o comando **ssh** com seu VM **<ip_address>**.

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

Por exemplo, o seguinte comando lista detalhes incluindo o nome do host e o dispositivo de bloco para o IP da VM **198.51.100.3**.

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

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

2. Use o comando **ssh** para verificar se cada VM em seu cluster usa o mesmo disco compartilhado.

```
# ssh <ip_address>"hostname ; lsblk -d | grep ' 1T ' | awk '{print \\i1}' | xargs -i udevadm info -
-query=all --name=/dev/{} | grep '^E: ID_SERIAL='"
```

Por exemplo, o seguinte comando lista detalhes incluindo o nome do host e o ID do volume do disco compartilhado para o endereço IP por exemplo **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
```

Depois de ter verificado que o disco compartilhado está anexado a cada VM, você pode configurar um armazenamento resiliente para o cluster. Para informações sobre como configurar o armazenamento resiliente para um cluster Red Hat High Availability, veja Configurando um sistema de arquivos GFS2 em um cluster. Para informações gerais sobre o sistema de arquivos GFS2, veja Configurando os sistemas de arquivos GFS2.

CAPÍTULO 3. IMPLANTANDO UMA IMAGEM DO RED HAT ENTERPRISE LINUX COMO UMA INSTÂNCIA DO EC2 NOS SERVIÇOS WEB DA AMAZON

Você tem várias opções para implantar uma imagem do Red Hat Enterprise Linux (RHEL) 8 como uma instância EC2 no Amazon Web Services (AWS). Este capítulo discute suas opções para escolher uma imagem e lista ou refere-se aos requisitos do sistema para seu sistema host e máquina virtual (VM). Este capítulo também fornece procedimentos para criar uma VM personalizada a partir de uma imagem ISO, carregando-a para o EC2, e lançando uma instância EC2.

IMPORTANTE

Enquanto você pode criar uma VM personalizada a partir de uma imagem ISO, a Red Hat recomenda que você use o produto Red Hat Image Builder para criar imagens personalizadas para uso em provedores de nuvem específicos. Com o Image Builder, você pode criar e carregar uma imagem de máquina Amazon (AMI) no formato **ami**. Consulte Composição de uma Imagem Personalizada do Sistema RHEL para mais informações.

Este capítulo se refere à documentação da Amazônia em vários lugares. Para muitos procedimentos, consulte a documentação amazônica referenciada para obter detalhes adicionais.

NOTA

Para uma lista de produtos Red Hat que você pode usar com segurança no AWS, veja Red Hat on Amazon Web Services.

Pré-requisitos

- Cadastre-se para uma conta no Portal do Cliente Red Hat.
- Inscreva-se na AWS e configure seus recursos AWS. Veja Configurando com o Amazon EC2 para mais informações.
- Habilite suas assinaturas no programa Red Hat Cloud Access. O programa Red Hat Cloud Access permite que você transfira suas assinaturas da Red Hat de sistemas físicos ou locais para AWS com total suporte da Red Hat.

Recursos adicionais

- Guia de Referência de Acesso à Nuvem da Red Hat
- Red Hat na Nuvem Pública
- Red Hat Enterprise Linux na Amazon EC2 - FAQs
- Instalação com o EC2 da Amazon
- Red Hat on Amazon Web Services

3.1. OPÇÕES DE IMAGEM DO RED HAT ENTERPRISE LINUX NA AWS

A tabela a seguir lista as opções de imagem e anota as diferenças nas opções de imagem.

Tabela 3.1. Opções de imagem

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações
Opte por implantar uma Red Hat Gold Image.	Aproveite suas assinaturas de Red Hat existentes.	Habilite assinaturas através do programa Red Hat Cloud Access, e depois escolha uma Red Hat Gold Image na AWS.	A assinatura inclui o custo do produto Red Hat; você paga a Amazon por todos os outros custos de instância. As imagens Gold da Red Hat são chamadas de imagens "Cloud Access" porque você aproveita suas assinaturas existentes da Red Hat. A Red Hat fornece suporte diretamente para as imagens de Cloud Access.
Opte por implantar uma imagem personalizada que você transfira para AWS.	Aproveite suas assinaturas de Red Hat existentes.	Habilite as assinaturas através do programa Red Hat Cloud Access, faça o upload de sua imagem personalizada e anexe suas assinaturas.	A assinatura inclui o custo do produto Red Hat; você paga a Amazon por todos os outros custos de instância. As imagens personalizadas que você muda para AWS são imagens "Cloud Access" porque você aproveita suas assinaturas Red Hat existentes. A Red Hat fornece suporte diretamente para as imagens de Cloud Access.

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações
Escolha a implantação de uma imagem amazônica existente que inclua a RHEL.	As imagens AWS EC2 incluem um produto da Red Hat.	Escolha uma imagem RHEL ao lançar uma instância no Console de Gestão AWS, ou escolha uma imagem do AWS Marketplace.	Você paga à Amazon por hora em um modelo pay-as-you-go. Tais imagens são chamadas de imagens "on-demand". A Amazon fornece suporte para imagens sob demanda. A Red Hat fornece atualizações das imagens. AWS disponibiliza as atualizações através da Infra-estrutura de Atualização da Red Hat (RHUI).

NOTA

Você pode criar uma imagem personalizada para AWS usando o Red Hat Image Builder. Consulte Composição de uma imagem personalizada do sistema RHEL para obter mais informações.

IMPORTANTE

Você não pode converter uma instância sob demanda para uma instância de Red Hat Cloud Access. Para mudar de uma imagem on-demand para uma imagem do Red Hat Cloud Access bring-your-own-subscription (BYOS), crie uma nova instância do Red Hat Cloud Access e migre os dados de sua instância on-demand. Cancele sua instância on-demand depois de migrar seus dados para evitar a dupla cobrança.

O restante deste capítulo inclui informações e procedimentos relativos às imagens personalizadas.

Recursos adicionais

- Programa Red Hat Cloud Access
- Composição de uma imagem personalizada do sistema RHEL
- Console de gestão AWS
- AWS Marketplace

3.2. ENTENDENDO AS IMAGENS DE BASE

Esta seção inclui informações sobre o uso de imagens de base pré-configuradas e suas configurações.

3.2.1. Usando uma imagem de base personalizada

Para configurar manualmente uma VM, você começa com uma imagem VM de base (starter). Uma vez criada a imagem base da VM, você pode modificar as configurações e adicionar os pacotes que a VM requer para operar na nuvem. Você pode fazer alterações de configuração adicionais para sua aplicação específica depois de carregar a imagem.

Recursos adicionais

Red Hat Enterprise Linux

3.2.2. Configurações da máquina virtual

As VMs em nuvem devem ter as seguintes configurações.

Tabela 3.2. Configurações de configuração da VM

Configuração	Recomendação
ssh	ssh deve estar habilitado para fornecer acesso remoto a seus VMs.
dhcp	O adaptador virtual primário deve ser configurado para a dhcp.

3.3. CRIAÇÃO DE UMA VM BASE A PARTIR DE UMA IMAGEM ISO

Siga os procedimentos desta seção para criar uma imagem de base a partir de uma imagem ISO.

Pré-requisitos

Habilite a virtualização para sua máquina host Red Hat Enterprise Linux 8.

3.3.1. Baixando a imagem ISO

Procedimento

1. Faça o download da última imagem ISO do Red Hat Enterprise Linux no Portal do Cliente Red Hat.
2. Mova a imagem para **/var/lib/libvirt/images**.

3.3.2. Criação de uma VM a partir da imagem ISO

Procedimento

1. Certifique-se de ter habilitado sua máquina host para virtualização. Veja Habilitação de virtualização no RHEL 8 para informações e procedimentos.
2. Criar e iniciar um Red Hat Enterprise Linux VM básico. Veja Criando máquinas virtuais para instruções.
    a. Se você usar a linha de comando para criar sua VM, certifique-se de definir a memória padrão e as CPUs para a capacidade que você deseja para a VM. Defina sua interface de rede virtual para **virtio**.

Segue uma amostra básica da linha de comando.

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

b. Se você usar o console web para criar sua VM, siga o procedimento em Criar máquinas virtuais usando o console web, com estas advertências:

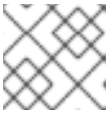
- Não confira **Immediately Start VM**.
- Mude seu **Memory** e **Storage Size** para as configurações de sua preferência.
- Antes de iniciar a instalação, certifique-se de ter alterado **Model** sob **Virtual Network Interface Settings** para **virtio** e altere seu **vCPUs** para as configurações de capacidade que deseja para a VM.

3.3.3. Conclusão da instalação da RHEL

Execute os seguintes passos para completar a instalação e permitir o acesso root uma vez que a VM seja lançada.

Procedimento

1. Escolha o idioma que você deseja usar durante o processo de instalação.
2. Na visualização do site **Installation Summary**:
   a. Clique em **Software Selection** e confira **Minimal Install**.
   b. Clique em **Done**.
   c. Clique **Installation Destination** e confira **Custom** em **Storage Configuration**.
      - Verificar pelo menos 500 MB para **/boot**. Você pode usar o espaço restante para a raiz /.
      - As partições padrão são recomendadas, mas você pode usar o Logical Volume Management (LVM).
      - Você pode usar xfs, ext4, ou ext3 para o sistema de arquivo.
      - Clique em **Done** quando você terminar com as mudanças.
3. Clique em **Begin Installation**.
4. Definir um **Root Password**. Criar outros usuários, conforme o caso.
5. Reinicie a VM e faça o login como **root** quando a instalação estiver concluída.
6. Configurar a imagem.



NOTA

Certifique-se de que o pacote **cloud-init** esteja instalado e habilitado.

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

a. Para os x86 VMs, instale os drivers **nvme**, **xen-netfront**, e **xen-blkfront**.

```
# dracut -f --add-drivers {\i1}"nvme xen-netfront xen-blkfront
```

b. Para aarch64 VMs, instale o driver **nvme**.

```
# dracut -f --add-drivers {\i1}"nvme}"
```

A inclusão desses motoristas elimina a possibilidade de um tempo limite de tração.

Alternativamente, você pode adicionar os motoristas a **/etc/dracut.conf.d/** e depois entrar **dracut -f** para sobrescrever o arquivo **initramfs** existente.

8. Desligue a VM.

3.4. CARREGANDO A IMAGEM DO RED HAT ENTERPRISE LINUX PARA AWS

Siga os procedimentos desta seção para carregar sua imagem na AWS.

3.4.1. Instalando o AWS CLI

Muitos dos procedimentos deste capítulo incluem o uso do AWS CLI. Complete os seguintes passos para instalar o AWS CLI.

Pré-requisitos

Você precisa ter criado e ter acesso a uma AWS Access Key ID e a uma AWS Secret Access Key. Consulte Configuração rápida da AWS CLI para obter informações e instruções.

Procedimento

1. Instale o Python 3 e a ferramenta **pip**.

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

2. Instale as ferramentas de linha de comando AWS com o comando **pip**.

```
# pip3 instalar awscli
```

3. Execute o comando **aws --version** para verificar se você instalou o AWS CLI.

```
$ 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 o cliente de linha de comando AWS de acordo com seus detalhes de acesso AWS.

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

Recursos adicionais

- Configurando rapidamente o AWS CLI
- Ferramentas de linha de comando AWS

3.4.2. Criação de um balde S3

A importação para AWS requer um balde Amazon S3. Um balde Amazon S3 é um recurso amazônico onde você armazena objetos. Como parte do processo de carregamento de sua imagem, você cria um balde S3 e depois move sua imagem para o balde. Complete os seguintes passos para criar um balde.

Procedimento

1. Lançar a Consola S3 da Amazônia.
2. Clique em **Create Bucket**. O diálogo **Create Bucket** aparece.
3. Na visão **Name and region**:
   a. Entre em um **Bucket name**.
   b. Entre em um **Region**.
   c. Clique em **Next**.
4. Na visualização de **Configure options**, selecione as opções desejadas e clique em **Next**.
5. Na visualização **Set permissions**, altere ou aceite as opções padrão e clique em **Next**.
6. Revise a configuração de sua caçamba.
7. Clique em **Create bucket**.

NOTA

Alternativamente, você pode usar o AWS CLI para criar um balde. Por exemplo, o comando **aws s3 mb s3://my-new-bucket** cria um balde S3 chamado **my-new-bucket**. Veja o comando AWS CLI Command Reference para mais informações sobre o comando **mb**.

Recursos adicionais

- Console S3 da Amazônia
- AWS CLI Referência de Comando

3.4.3. Criação da função vmimport

Realizar o seguinte procedimento para criar a função **vmimport**, que é exigida pela importação de VM. Veja a documentação sobre a função do Serviço de Importação da VM na Amazônia para maiores informações.

Procedimento

1. Crie um arquivo chamado **trust-policy.json** e inclua a seguinte política. Salve o arquivo em seu sistema e anote sua localização.

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

2. Use o comando **create role** para criar a função **vmimport**. Especifique o caminho completo para a localização do arquivo **trust-policy.json**. Prefixo **file:**// para o caminho. Segue um exemplo.

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

3. Crie um arquivo chamado **role-policy.json** e inclua a seguinte política. Substitua **s3-bucket-name** pelo nome do seu balde 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. Use o comando **put-role-policy** para anexar a política ao papel que você criou. Especifique o caminho completo do arquivo **role-policy.json**. Segue um exemplo.

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

Recursos adicionais

- Função do serviço de importação da VM
- Função de serviço requerida

3.4.4. Convertendo e empurrando sua imagem para S3

Complete o seguinte procedimento para converter e empurrar sua imagem para S3. As amostras são representativas; elas convertem uma imagem formatada no formato de arquivo **qcow2** para o formato **raw**. A Amazon aceita imagens nos formatos **OVA**, **VHD**, **VHDX**, **VMDK**, e **raw**. Veja Como funciona o VM Import/Export para mais informações sobre os formatos de imagem que a Amazon aceita.

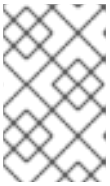
Procedimento

1. Execute o comando **qemu-img** para converter sua imagem. Segue uma amostra.

```
qemu-img converter -f qcow2 -O bruto rel-8.2-sample.qcow2 rel-8.2-sample.raw
```

2. Empurrar a imagem para S3.

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



NOTA

Este procedimento pode levar alguns minutos. Após a conclusão, você pode verificar se sua imagem foi transferida com sucesso para seu balde S3 usando o Console AWS S3.

Recursos adicionais

- Como funciona a importação/exportação de VM
- Console AWS S3

3.4.5. Importando sua imagem como um instantâneo

Realize o seguinte procedimento para importar uma imagem como um instantâneo.

Procedimento

1. Crie um arquivo para especificar um balde e um caminho para sua imagem. Nomeie o arquivo **containers.json**. Na amostra que se segue, substitua **s3-bucket-name** pelo nome de seu balde e **s3-key** pela chave. Você pode obter a chave para a imagem usando o Console S3 da Amazon.

```
{
    "Description": "rhel-8.2-sample.raw",
```

```
    "Format": "raw",
    "UserBucket": {
        "S3Bucket": "s3-bucket-name",
        "S3Key": "s3-key"
    }
}
```

2. Importar a imagem como um instantâneo. Este exemplo usa um arquivo público Amazon S3; você pode usar o Console Amazon S3 para alterar as configurações de permissões em seu balde.

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

O terminal exibe uma mensagem como a seguinte. Observe o **ImportTaskID** dentro da mensagem.

```
{
    "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. Acompanhe o progresso da importação usando o comando **describe-import-snapshot-tasks**. Incluir o **ImportTaskID**.

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

A mensagem de retorno mostra o status atual da tarefa. Quando concluída, **Status** mostra **completed**. Dentro do status, anote a identificação da instancia.

Recursos adicionais

- Console S3 da Amazônia
- Importação de um disco como um instantâneo usando a importação/exportação de VM

3.4.6. Criação de um AMI a partir da foto carregada

Dentro do EC2, você deve escolher uma Máquina Imagem da Amazônia (AMI) ao lançar uma instância. Execute o seguinte procedimento para criar uma AMI a partir de sua foto carregada.

Procedimento

1. Ir para o painel de controle AWS EC2.

2. Em **Elastic Block Store**, selecione **Snapshots**.
3. Pesquise sua identificação instantânea (por exemplo, **snap-0e718930bd72bcda0**).
4. Clique com o botão direito do mouse no instantâneo e selecione **Create image**.
5. Dê um nome à sua imagem.
6. Em **Virtualization type**, escolha **Hardware-assisted virtualization**.
7. Clique em **Create**. Na nota referente à criação da imagem, há um link para sua imagem.
8. Clique no link da imagem. Sua imagem aparece em **Images>AMIs**.

NOTA

Alternativamente, você pode usar o comando AWS CLI **register-image** para criar um AMI a partir de um instantâneo. Veja register-image para mais informações. Segue um exemplo.

```
$ 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
```

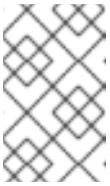
Você deve especificar o volume do dispositivo raiz **/dev/sda1** como seu **root-device-name**. Para informações conceituais sobre o mapeamento de dispositivos para AWS, veja Exemplo de mapeamento de dispositivo de bloco .

3.4.7. Lançamento de uma instância da AMI

Execute o seguinte procedimento para lançar e configurar uma instância da AMI.

Procedimento

1. No Painel de Controle AWS EC2, selecione **Images** e depois **AMIs**.
2. Clique com o botão direito do mouse sobre sua imagem e selecione **Launch**.
3. Escolha um **Instance Type** que atenda ou exceda as exigências de sua carga de trabalho. Ver Amazon EC2 Instance Types para informações sobre os tipos de instância.
4. Clique em **Next: Configure Instance Details**.
   a. Entre no site **Number of instances** que você deseja criar.
   b. Para **Network**, selecione o VPC que você criou ao configurar seu ambiente AWS. Selecione uma sub-rede, por exemplo, ou crie uma nova sub-rede.
   c. Selecione **Enable** para Auto-atribuir IP Público.



NOTA

Estas são as opções mínimas de configuração necessárias para criar uma instância básica. Revise opções adicionais com base nas exigências de sua aplicação.

5. Clique em **Next: Add Storage**. Verifique se o armazenamento padrão é suficiente.
6. Clique em **Next: Add Tags**.

NOTA

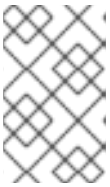
As etiquetas podem ajudá-lo a gerenciar seus recursos AWS. Veja Tagging Your Amazon EC2 Resources para informações sobre tagging.

7. Clique em **Next: Configure Security Group**. Selecione o grupo de segurança que você criou ao configurar seu ambiente AWS.
8. Clique em **Review and Launch**. Verifique suas seleções.
9. Clique em **Launch**. Você é solicitado a selecionar um par de chaves existente ou a criar um novo par de chaves. Selecione o par de chaves que você criou ao configurar seu ambiente AWS.

NOTA

Verifique se as permissões para sua chave privada estão corretas. Use as opções de comando **chmod 400 <keyname>.pem** para alterar as permissões, se necessário.

10. Clique em **Launch Instances**.
11. Clique em **View Instances**. Você pode citar a(s) instância(s).
Agora você pode lançar uma sessão SSH para sua(s) instância(s), selecionando uma instância e clicando em **Connect**. Use o exemplo fornecido para **A standalone SSH client**.



NOTA

Alternativamente, você pode lançar uma instância usando o AWS CLI. Veja Lançamento, Listagem e Encerramento das Instâncias EC2 da Amazon na documentação da Amazon para mais informações.

Recursos adicionais

- Console de gestão AWS
- Instalação com o EC2 da Amazon
- Instâncias EC2 da Amazônia
- Tipos de instâncias EC2 da Amazônia

3.4.8. Anexando assinaturas da Red Hat

Complete os seguintes passos para anexar as assinaturas que você ativou anteriormente através do programa Red Hat Cloud Access.

Pré-requisitos

Você deve ter habilitado suas assinaturas.

Procedimento

1. Registre seu sistema.

```
registro de gerenciador de assinaturas --auto-attach
```

2. Anexe suas assinaturas.

   - Você pode usar uma chave de ativação para anexar as assinaturas. Consulte Criando Chaves de Ativação do Portal do Cliente Red Hat para mais informações.
   - Alternativamente, você pode anexar manualmente uma assinatura usando o ID do pool de assinaturas (Pool ID). Veja Anexar e remover assinaturas através da Linha de Comando .

Recursos adicionais

- Criando as chaves de ativação do Portal do Cliente Red Hat
- Anexar e remover assinaturas através da linha de comando
- Uso e configuração do Red Hat Subscription Manager

CAPÍTULO 4. CONFIGURAÇÃO DE UM CLUSTER RED HAT HIGH AVAILABILITY NO AWS

Este capítulo inclui informações e procedimentos para a configuração de um cluster Red Hat High Availability (HA) em Amazon Web Services (AWS) usando instâncias EC2 como nós de cluster. Note que você tem várias opções para obter as imagens do Red Hat Enterprise Linux (RHEL) que você usa para seu cluster. Para informações sobre as opções de imagem para AWS, consulte Opções de imagem do Red Hat Enterprise Linux no AWS.

Este capítulo inclui procedimentos prévios para a criação de seu ambiente para AWS. Uma vez que você tenha configurado seu ambiente, você pode criar e configurar instâncias EC2.

Este capítulo também inclui procedimentos específicos para a criação de clusters de HA, que transformam nós individuais em um cluster de nós HA no AWS. Estes incluem procedimentos para instalação dos pacotes e agentes de alta disponibilidade em cada nó de cluster, configuração de cercas e instalação de agentes de recursos de rede AWS.

O capítulo se refere à documentação da Amazônia em vários lugares. Para muitos procedimentos, consulte a documentação amazônica referenciada para mais informações.

Pré-requisitos

- Cadastre-se para uma conta no Portal do Cliente Red Hat .
- Inscreva-se na AWS e configure seus recursos AWS. Veja Configurando com o Amazon EC2 para mais informações.
- Habilite suas assinaturas no programa Red Hat Cloud Access . O programa Red Hat Cloud Access permite que você transfira suas assinaturas da Red Hat de sistemas físicos ou locais para AWS com total suporte da Red Hat.

Recursos adicionais

- Guia de Referência de Acesso à Nuvem da Red Hat
- Red Hat na Nuvem Pública
- Red Hat Enterprise Linux na Amazon EC2 - FAQs
- Instalação com o EC2 da Amazon
- Red Hat on Amazon Web Services

4.1. CRIAÇÃO DA CHAVE DE ACESSO AWS E DA CHAVE DE ACESSO SECRETA AWS

Você precisa criar uma AWS Access Key e uma AWS Secret Access Key antes de instalar a AWS CLI. As APIs de esgrima e agente de recursos usam a AWS Access Key e a Secret Access Key para se conectar a cada nó do cluster.

Complete os seguintes passos para criar estas chaves.

Pré-requisitos

Sua conta de usuário do IAM deve ter acesso programático. Veja Configurando o ambiente AWS para mais informações.

Procedimento

1. Lançar o AWS Console.
2. Clique em seu ID de conta AWS para exibir o menu suspenso e selecione **My Security Credentials**.
3. Clique em **Users**.
4. Selecione o usuário e abra a tela **Summary**.
5. Clique na guia **Security credentials**.
6. Clique em **Create access key**.
7. Baixe o arquivo **.csv** (ou salve ambas as chaves). Você precisa digitar estas chaves ao criar o dispositivo de esgrima.

4.2. INSTALANDO O AWS CLI

Muitos dos procedimentos deste capítulo incluem o uso do AWS CLI. Complete os seguintes passos para instalar o AWS CLI.

Pré-requisitos

Você precisa ter criado e ter acesso a uma AWS Access Key ID e a uma AWS Secret Access Key. Consulte Configuração rápida da AWS CLI para obter informações e instruções.

Procedimento

1. Instale o Python 3 e a ferramenta **pip**.

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

2. Instale as ferramentas de linha de comando AWS com o comando **pip**.

```
# pip3 instalar awscli
```

3. Execute o comando **aws --version** para verificar se você instalou o AWS CLI.

```
$ 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 o cliente de linha de comando AWS de acordo com seus detalhes de acesso AWS.

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

Recursos adicionais

- Configurando rapidamente o AWS CLI
- Ferramentas de linha de comando AWS

4.3. CRIAÇÃO DE UMA INSTÂNCIA HA EC2

Complete os seguintes passos para criar as instâncias que você utiliza como seus nós de cluster HA. Observe que você tem uma série de opções para obter as imagens RHEL que você utiliza para seu cluster. Consulte as Opções de Imagem do Red Hat Enterprise Linux em AWS para obter informações sobre as opções de imagem para AWS.

Você pode criar e carregar uma imagem personalizada que você usa para seus nós de cluster, ou você pode escolher uma imagem Gold (imagem de acesso à nuvem) ou uma imagem on-demand.

Pré-requisitos

Você precisa ter criado um ambiente AWS. Veja Configurando com o Amazon EC2 para mais informações.

Procedimento

1. No Painel de Controle AWS EC2, selecione **Images** e depois **AMIs**.
2. Clique com o botão direito do mouse sobre sua imagem e selecione **Launch**.
3. Escolha um **Instance Type** que atenda ou exceda as exigências de sua carga de trabalho. Dependendo de sua aplicação HA, cada instância pode precisar ter maior capacidade.

Ver Amazon EC2 Instance Types para informações sobre os tipos de instância.

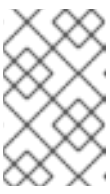
1. Clique em **Next: Configure Instance Details**.
   a. Entre no site **Number of instances** que você deseja criar para o cluster. Os exemplos neste capítulo utilizam três nós de agrupamento.

NOTA

Não se lançar em um Grupo de Escala de Automóveis.

   b. Para **Network**, selecione o VPC que você criou em Configurar o ambiente AWS. Selecione a sub-rede, por exemplo, para criar uma nova sub-rede.

   c. Selecione **Enable** para Auto-atribuir IP Público. Estas são as seleções mínimas que você precisa fazer para **Configure Instance Details**. Dependendo de sua aplicação HA específica, você pode precisar fazer seleções adicionais.



NOTA

Estas são as opções mínimas de configuração necessárias para criar uma instância básica. Reveja opções adicionais com base em seus requisitos de aplicação HA.

2. Clique em **Next: Add Storage** e verifique se o armazenamento padrão é suficiente. Você não precisa modificar estas configurações, a menos que sua aplicação HA exija outras opções de armazenamento.

3. Clique em **Next: Add Tags**.

NOTA

As etiquetas podem ajudá-lo a gerenciar seus recursos AWS. Veja Tagging Your Amazon EC2 Resources para informações sobre tagging.

4. Clique em **Next: Configure Security Group**. Selecione o grupo de segurança existente que você criou em Configurar o ambiente AWS.

5. Clique em **Review and Launch** e verifique suas seleções.

6. Clique em **Launch**. Você é solicitado a selecionar um par de chaves existente ou a criar um novo par de chaves. Selecione o par de chaves que você criou ao configurar o ambiente AWS.

7. Clique em **Launch Instances**.

8. Clique em **View Instances**. Você pode citar a(s) instância(s).

NOTA

Alternativamente, você pode lançar instâncias usando o AWS CLI. Veja Lançamento, Listagem e Encerramento de Instâncias EC2 da Amazon na documentação da Amazon para mais informações.

Recursos adicionais

- Console de gestão AWS
- Instalação com o EC2 da Amazon
- Instâncias EC2 da Amazônia
- Tipos de instâncias EC2 da Amazônia

4.4. CONFIGURANDO A CHAVE PRIVADA

Complete as seguintes tarefas de configuração para usar o arquivo chave SSH privado (**.pem**) antes que ele possa ser usado em uma sessão SSH.

Procedimento

1. Mova o arquivo chave do diretório **Downloads** para seu diretório **Home** ou para seu **~/.ssh directory**.

2. Digite o seguinte comando para alterar as permissões do arquivo chave para que somente o usuário root possa lê-lo.

```
# chmod 400 KeyName.pem
```

4.5. CONECTANDO-SE A UMA INSTÂNCIA

Complete os seguintes passos em todos os nós para se conectar a uma instância.

Procedimento

1. Inicie a AWS Console e selecione a instância EC2.
2. Clique em **Connect** e selecione **A standalone SSH client**.
3. A partir de sua sessão terminal SSH, conecte-se à instância usando o exemplo AWS fornecido na janela pop-up. Adicione o caminho correto ao seu arquivo **KeyName.pem** se o caminho não for mostrado no exemplo.

4.6. INSTALANDO OS PACOTES E AGENTES DE ALTA DISPONIBILIDADE

Complete os seguintes passos em todos os nós para instalar os pacotes e agentes de Alta Disponibilidade.

Procedimento

1. Digite o seguinte comando para remover o cliente AWS Red Hat Update Infrastructure (RHUI). Como você vai usar uma assinatura Red Hat Cloud Access, você não deve usar AWS RHUI além de sua assinatura.

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

2. Registrar a VM com o Red Hat.

```
# registro de gerenciador de assinaturas --auto-attach
```

3. Desativar todos os repositórios.

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

4. Habilitar os repositórios RHEL 8 Server e RHEL 8 Server HA.

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

5. Atualize a instância da RHEL AWS.

```
# yum update -y
```

6. Instale os pacotes de software Red Hat High Availability Add-On, junto com todos os agentes de cercas disponíveis no canal High Availability.

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

7. O usuário **hacluster** foi criado durante a instalação de **pcs** e **pacemaker** na etapa anterior. Criar uma senha para **hacluster** em todos os nós de cluster. Use a mesma senha para todos os nós.

```
# hacluster da senha
```

8. Adicione o serviço **high availability** ao Firewall RHEL se **firewalld.service** estiver instalado.

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

9. Inicie o serviço **pcs** e habilite-o a começar na inicialização.

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

10. Edite **/etc/hosts** e adicione nomes de hosts RHEL e endereços IP internos. Veja Como o arquivo /etc/hosts deve ser configurado nos nós de cluster RHEL? para maiores detalhes.

Etapa de verificação

Certifique-se de que o serviço **pcs** esteja 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. CRIAÇÃO DE UM CLUSTER

Complete os seguintes passos para criar o conjunto de nós.

Procedimento

1. Em um dos nós, digite o seguinte comando para autenticar o usuário do pcs **hacluster**. No comando, especifique o nome de cada nó do cluster.

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

Exemplo:

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

2. Criar o conjunto.

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

Exemplo:

```
[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
```

Etapas de verificação

1. Habilite o conjunto.

```
[root@node01 clouduser]# pcs cluster enable --tudo
```

2. Comece o agrupamento.

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

Exemplo:

```
[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. CONFIGURAÇÃO DE CERCAS

Complete os seguintes passos para configurar a vedação.

Procedimento

1. Digite a seguinte consulta de metadados AWS para obter a identificação de instância para cada nó. Você precisa dessas identificações para configurar o dispositivo de cerca. Consulte Metadados de Instância e Dados de Usuário para obter informações adicionais.

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

Exemplo:

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

2. Digite o seguinte comando para configurar o dispositivo de cerca. Use o comando **pcmk_host_map** para mapear o nome do host RHEL para o ID da Instância. Use a chave de acesso AWS e a chave de acesso secreta AWS que você configurou anteriormente.

```
# pcs stonith create name fence_aws access_key=access-key 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
```

Exemplo:

```
[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. Teste o agente de esgrima para um dos outros nós.

```
# pcs cerca de pedra awsnodename
```

NOTA

A resposta do comando pode levar vários minutos para ser exibida. Se você assistir à sessão terminal ativa para o nó sendo cercado, você verá que a conexão terminal é imediatamente terminada após você entrar no comando de cercado.

Exemplo:

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

Etapas de verificação

1. Verifique o status para verificar se o nó está cercado.

```
# pcs status
```

Exemplo:

```
[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. Iniciar o nó que foi cercado na etapa anterior.

```
# pcs cluster start awshostname
```

3. Verifique o status para verificar o nó iniciado.

```
# pcs status
```

Exemplo:

```
[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. INSTALANDO O AWS CLI EM NÓS DE CLUSTER

Anteriormente, você instalou o AWS CLI em seu sistema host. Você precisa instalar o AWS CLI nos nós de cluster antes de configurar os agentes de recursos da rede.

Complete o seguinte procedimento em cada nó de agrupamento.

Pré-requisitos

Você deve ter criado uma chave de acesso AWS e uma chave de acesso secreta AWS. Consulte Criando a chave de acesso AWS e a chave de acesso secreta AWS para mais informações.

Procedimento

1. Realizar o procedimento de instalação do AWS CLI.
2. Digite o seguinte comando para verificar se o AWS CLI está configurado corretamente. As identificações das instâncias e os nomes das instâncias devem ser exibidos.
   Exemplo:

```
[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. INSTALAÇÃO DE AGENTES DE RECURSOS DE REDE

Para que as operações HA funcionem, o cluster utiliza agentes de recursos de rede AWS para permitir a funcionalidade de failover. Se um nó não responder a uma verificação de batimento cardíaco em um determinado período de tempo, o nó é cercado e as operações falham para um nó adicional no cluster. Os agentes de recursos de rede precisam ser configurados para que isso funcione.

Acrescentar os dois recursos ao mesmo grupo para fazer cumprir as restrições de **order** e **colocation**.

Create a secondary private IP resource and virtual IP resource

Complete o seguinte procedimento para adicionar um endereço IP privado secundário e criar um IP virtual. Você pode completar este procedimento a partir de qualquer nó do cluster.

Procedimento

1. Digite o seguinte comando para ver a descrição do agente de recursos (awsvip) **AWS Secondary Private IP Address**. Isto mostra as opções e operações padrão para este agente.

```
# pcs resource descrever awsvip
```

2. Digite o seguinte comando para criar o endereço IP privado secundário usando um endereço IP privado não utilizado no bloco **VPC CIDR**.

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

Exemplo:

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

3. Criar um recurso IP virtual. Este é um endereço IP VPC que pode ser rapidamente refazido do nó cercado para o nó de failover, mascarando a falha do nó cercado dentro da sub-rede.

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

Exemplo:

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

Etapa de verificação

Digite o comando **pcs status** para verificar se os recursos estão funcionando.

```
# pcs status
```

Exemplo:

```
[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

Um endereço IP elástico é um endereço IP público que pode ser rapidamente refazido do nó cercado para o nó de falha, mascarando a falha do nó cercado.

Note que isto é diferente do recurso de PI virtual criado anteriormente. O endereço IP elástico é usado para conexões de Internet voltadas para o público, ao invés de conexões de sub-rede.

1. Acrescentar os dois recursos ao mesmo grupo que foi criado anteriormente para fazer cumprir as restrições de **order** e **colocation**.

2. Digite o seguinte comando AWS CLI para criar um endereço IP elástico.

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

3. Digite o seguinte comando para ver a descrição do agente de recursos de endereço IP secundário elástico AWS (awseip). Isto mostra as opções e operações padrão para este agente.

```
# pcs resource descrever awseip
```

4. Criar o recurso de endereço IP secundário elástico utilizando o endereço IP alocado criado na Etapa 1.

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

Exemplo:

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

Etapa de verificação

Digite o comando **pcs status** para verificar se o recurso está funcionando.

```
# pcs status
```

Exemplo:

```
[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

Digite os seguintes comandos para verificar se os recursos de IP virtual (awsvip) e de IP elástico (awseip) estão funcionando.

Procedimento

1. Lance uma sessão SSH de sua estação de trabalho local para o endereço IP elástico previamente criado.

   ```
   $ ssh -l ec2-user -i ~/.ssh/<KeyName>.pem elástico-IP
   ```

   Exemplo:

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

2. Verifique se o host ao qual você se conectou via SSH é o host associado com o recurso elástico criado.

Recursos adicionais

- Visão geral do Add-On de alta disponibilidade
- Administração de Suplementos de Alta Disponibilidade
- Referência de alta disponibilidade adicional

4.11. CONFIGURAÇÃO DE ARMAZENAMENTO EM BLOCO COMPARTILHADO

Esta seção fornece um procedimento opcional para configurar o armazenamento em bloco compartilhado para um cluster Red Hat High Availability com volumes Amazon EBS Multi-Attach. O procedimento assume três instâncias (um cluster de três nós) com um disco compartilhado de 1 TB.

Procedimento

1. Criar um volume de blocos compartilhados usando o comando create-volume AWS.

   ```
   $ aws ec2 criar-volume --disponibilidade-zona<disponibilidade_zona> -- sem encriptação -tamanho 1024 --volume tipo io1 --iops 51200 --multi-attach
   ```

   Por exemplo, o seguinte comando cria um volume na zona de disponibilidade **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

Você precisa do **VolumeId** na próxima etapa.

2. Para cada instância em seu cluster, anexe um volume de bloco compartilhado usando o volume de bloco de comando AWS. Use seu **<instance_id>** e **<volume_id>**.

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

Por exemplo, o seguinte comando anexa um volume de blocos compartilhados **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"
}
```

Etapas de verificação

1. Para cada instância em seu agrupamento, verifique se o dispositivo de bloco está disponível usando o comando **ssh** com sua instância **<ip_address>**.

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

Por exemplo, o seguinte comando lista detalhes incluindo o nome do host e o dispositivo de bloco para o IP por exemplo **198.51.100.3**.

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

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

2. Use o comando **ssh** para verificar se cada instância em seu cluster usa o mesmo disco compartilhado.

```
# ssh <ip_address>"hostname ; lsblk -d | grep ' 1T ' | awk '{print \\i1}' | xargs -i udevadm info --query=all --name=/dev/{} | grep '^E: ID_SERIAL='"
```

Por exemplo, o seguinte comando lista detalhes incluindo o nome do host e o ID do volume do disco compartilhado para o endereço IP por exemplo **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
```

Após verificar que o disco compartilhado está anexado a cada instância, você pode configurar um armazenamento resiliente para o cluster. Para informações sobre como configurar o armazenamento resiliente para um cluster Red Hat High Availability, consulte Configurando um sistema de arquivos GFS2 em um cluster. Para informações gerais sobre o sistema de arquivos GFS2, veja Configurando os sistemas de arquivos GFS2.

CAPÍTULO 5. IMPLEMENTANDO UMA IMAGEM DO RED HAT ENTERPRISE LINUX COMO UMA INSTÂNCIA DO GOOGLE COMPUTE ENGINE NA PLATAFORMA GOOGLE CLOUD

Você tem várias opções para implantar uma imagem do Red Hat Enterprise Linux (RHEL) 8 como uma instância do Google Compute Engine (GCE) na plataforma Google Cloud Platform (GCP). Este capítulo discute suas opções para escolher uma imagem e lista ou refere-se aos requisitos do sistema para seu sistema host e máquina virtual (VM). O capítulo fornece procedimentos para criar uma VM personalizada a partir de uma imagem ISO, fazer o upload para GCE e lançar uma instância.

Este capítulo se refere à documentação do Google em vários lugares. Para muitos procedimentos, consulte a documentação referenciada do Google para obter detalhes adicionais.

NOTA

Para uma lista de certificações de produtos Red Hat para GCP, veja Red Hat na plataforma Google Cloud.

Pré-requisitos

- Você precisa de uma conta no Portal do Cliente da Red Hat para completar os procedimentos deste capítulo.
- Criar uma conta com GCP para acessar o Console da Plataforma Google Cloud. Consulte o Google Cloud para mais informações.
- Habilite suas assinaturas da Red Hat através do programa Red Hat Cloud Access . O programa Red Hat Cloud Access permite que você transfira suas assinaturas Red Hat de sistemas físicos ou locais para o GCP com total suporte da Red Hat.

Recursos adicionais

- Red Hat na Nuvem Pública
- Nuvem Google

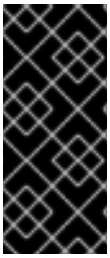
5.1. OPÇÕES DE IMAGEM DO RED HAT ENTERPRISE LINUX NO GCP

A tabela a seguir lista as opções de imagem e as diferenças nas opções de imagem.

Tabela 5.1. Opções de imagem

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações
Opte por implantar uma imagem personalizada que você transfira para GCP.	Aproveite suas assinaturas de Red Hat existentes.	Habilite as assinaturas através do programa Red Hat Cloud Access, faça o upload de sua imagem personalizada e anexe suas assinaturas.	A assinatura inclui o custo do produto Red Hat; você paga todos os outros custos de instância. As imagens personalizadas que você move para o GCP são chamadas de imagens "Cloud Access" porque você aproveita suas assinaturas Red Hat existentes. A Red Hat fornece suporte diretamente para imagens de Cloud Access.
Escolha a implantação de uma imagem GCP existente que inclua a RHEL.	As imagens do GCP incluem um produto Red Hat.	Escolha uma imagem RHEL quando você lança uma instância no GCP Compute Engine, ou escolha uma imagem do Google Cloud Platform Marketplace.	Você paga GCP por hora em um modelo pay-as-you-go. Tais imagens são chamadas de imagens "on-demand". A GCP oferece suporte para imagens sob demanda através de um contrato de suporte.



IMPORTANTE

Você não pode converter uma instância sob demanda para uma instância de Red Hat Cloud Access. Para mudar de uma imagem on-demand para uma imagem do Red Hat Cloud Access bring-your-own-subscription (BYOS), crie uma nova instância do Red Hat Cloud Access e migre os dados de sua instância on-demand. Cancele sua instância on-demand depois de migrar seus dados para evitar a dupla cobrança.

O restante deste capítulo inclui informações e procedimentos relativos às imagens personalizadas.

Recursos adicionais

- Red Hat na Nuvem Pública
- Imagens
- Guia de Referência de Acesso à Nuvem da Red Hat
- Criação de uma instância a partir de uma imagem personalizada

5.2. ENTENDENDO AS IMAGENS DE BASE

Esta seção inclui informações sobre o uso de imagens de base pré-configuradas e suas configurações.

5.2.1. Usando uma imagem de base personalizada

Para configurar manualmente uma VM, você começa com uma imagem VM de base (starter). Uma vez criada a imagem base da VM, você pode modificar as configurações e adicionar os pacotes que a VM requer para operar na nuvem. Você pode fazer alterações de configuração adicionais para sua aplicação específica depois de carregar a imagem.

Recursos adicionais

Red Hat Enterprise Linux

5.2.2. Configurações da máquina virtual

As VMs em nuvem devem ter as seguintes configurações.

Tabela 5.2. Configurações de configuração da VM

Configuração	Recomendação
ssh	ssh deve estar habilitado para fornecer acesso remoto a seus VMs.
dhcp	O adaptador virtual primário deve ser configurado para a dhcp.

5.3. CRIAÇÃO DE UMA VM BASE A PARTIR DE UMA IMAGEM ISO

Siga os procedimentos desta seção para criar uma imagem de base a partir de uma imagem ISO.

Pré-requisitos

Habilite a virtualização para sua máquina host Red Hat Enterprise Linux 8.

5.3.1. Baixando a imagem ISO

Procedimento

1. Faça o download da última imagem ISO do Red Hat Enterprise Linux no Portal do Cliente Red Hat.
2. Mova a imagem para **/var/lib/libvirt/images**.

5.3.2. Criação de uma VM a partir da imagem ISO

Procedimento

1. Certifique-se de ter habilitado sua máquina host para virtualização. Veja Habilitação de virtualização no RHEL 8 para informações e procedimentos.
2. Criar e iniciar um Red Hat Enterprise Linux VM básico. Veja Criando máquinas virtuais para instruções.

a. Se você usar a linha de comando para criar sua VM, certifique-se de definir a memória padrão e as CPUs para a capacidade que você deseja para a VM. Defina sua interface de rede virtual para **virtio**.
Segue uma amostra básica da linha de comando.

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

b. Se você usar o console web para criar sua VM, siga o procedimento em Criar máquinas virtuais usando o console web, com estas advertências:

- Não confira **Immediately Start VM**.
- Mude seu **Memory** e **Storage Size** para as configurações de sua preferência.
- Antes de iniciar a instalação, certifique-se de ter alterado **Model** sob **Virtual Network Interface Settings** para **virtio** e altere seu **vCPUs** para as configurações de capacidade que deseja para a VM.

5.3.3. Conclusão da instalação da RHEL

Execute os seguintes passos para completar a instalação e permitir o acesso root uma vez que a VM seja lançada.

Procedimento

1. Escolha o idioma que você deseja usar durante o processo de instalação.
2. Na visualização do site **Installation Summary**:
   a. Clique em **Software Selection** e confira **Minimal Install**.
   b. Clique em **Done**.
   c. Clique **Installation Destination** e confira **Custom** em **Storage Configuration**.
      - Verificar pelo menos 500 MB para **/boot**. Você pode usar o espaço restante para a raiz /.
      - As partições padrão são recomendadas, mas você pode usar o Logical Volume Management (LVM).
      - Você pode usar xfs, ext4, ou ext3 para o sistema de arquivo.
      - Clique em **Done** quando você terminar com as mudanças.
3. Clique em **Begin Installation**.
4. Definir um **Root Password**. Criar outros usuários, conforme o caso.
5. Reinicie a VM e faça o login como **root** quando a instalação estiver concluída.
6. Configurar a imagem.

NOTA

Certifique-se de que o pacote **cloud-init** esteja instalado e habilitado.

7. Desligue a VM.

5.4. CARREGANDO A IMAGEM RHEL PARA GCP

Siga os procedimentos desta seção para carregar sua imagem no GCP.

5.4.1. Criando um novo projeto sobre GCP

Complete os seguintes passos para criar um novo projeto sobre GCP.

Pré-requisitos

Você deve ter criado uma conta com GCP. Caso não tenha, consulte o Google Cloud para mais informações.

Procedimento

1. Lançar o Console GCP.
2. Clique no menu suspenso à direita de **Google Cloud Platform**.
3. A partir do menu pop-up, clique **NEW PROJECT**.
4. Da janela **New Project**, digite um nome para seu novo projeto.
5. Verifique o site **Organization**. Clique no menu suspenso para mudar a organização, se necessário.
6. Confirme o **Location** de sua organização mãe ou pasta. Clique em **Browse** para pesquisar e alterar este valor, se necessário.
7. Clique em **CREATE** para criar seu novo projeto GCP.

NOTA

Uma vez instalado o Google Cloud SDK, você pode usar o comando **gcloud projects create** CLI para criar um projeto. Segue um exemplo simples.

```
projetos gcloud criam o my-gcp-projeto3 --nome projeto3
```

O exemplo cria um projeto com o ID do projeto **my-gcp-project3** e o nome do projeto **project3**. Veja gcloud project create para mais informações.

Recursos adicionais

Criação e gerenciamento de recursos

5.4.2. Instalando o Google Cloud SDK

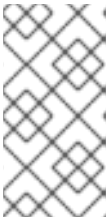
Complete os seguintes passos para instalar o Google Cloud SDK.

Pré-requisitos

- Crie um projeto sobre o GCP, caso ainda não o tenha feito. Veja Criar um novo projeto na plataforma Google Cloud para mais informações.
- Certifique-se de que seu sistema hospedeiro inclua Python 2.7. Se não incluir, instale o Python 2.7.

Procedimento

1. Siga as instruções GCP para baixar e extrair o arquivo do Google Cloud SDK. Veja o documento GCP Quickstart para Linux para maiores detalhes.
2. Siga as mesmas instruções para inicializar o Google Cloud SDK.



NOTA

Uma vez inicializado o Google Cloud SDK, você pode usar os comandos **gcloud** CLI para realizar tarefas e obter informações sobre seu projeto e instâncias. Por exemplo, você pode exibir informações sobre o projeto com o comando **gcloud compute project-info describe --project <project-name>**.

Recursos adicionais

- Início rápido para Linux
- referência de comando gcloud
- visão geral da ferramenta de linha de comando gcloud

5.4.3. Criando chaves SSH para Google Compute Engine

Execute o seguinte procedimento para gerar e registrar chaves SSH com GCE para que você possa SSH diretamente em uma instância usando seu endereço IP público.

Procedimento

1. Use o comando **ssh-keygen** para gerar um par de chaves SSH para uso com GCE.

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

2. A partir da página Painel de Controle do Console GCP , clique no menu **Navigation** à esquerda do Google **Cloud Console banner** e selecione **Compute Engine** e depois selecione **Metadata**.
3. Clique em **SSH Keys** e depois clique em **Edit**.
4. Digite a saída gerada a partir do arquivo **~/.ssh/google_compute_engine.pub** e clique em **Save**.
   Agora você pode se conectar à sua instância usando SSH padrão.

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

NOTA

Você pode executar o comando **gcloud compute config-ssh** para preencher seu arquivo de configuração com pseudônimos para suas instâncias. Os pseudônimos permitem conexões SSH simples por nome de instância. Para informações sobre o comando **gcloud compute config-ssh**, veja gcloud compute config-ssh.

Recursos adicionais

- gcloud compute config-ssh
- Conexão com instâncias

5.4.4. Criação de um balde de armazenamento em GCP Storage

A importação para GCP requer um balde de armazenamento GCP. Complete os seguintes passos para criar uma caçamba.

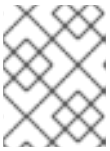
Procedimento

1. Se você ainda não está logado no GCP, faça o log in com o seguinte comando.

```
# gcloud auth login
```

2. Criar um balde de armazenamento.

```
# gsutil mb gs://bucket_name
```



NOTA

Alternativamente, você pode usar o Console do Google Cloud para criar um balde. Veja Criar um balde para informações.

Recursos adicionais

Criar um balde

5.4.5. Convertendo e carregando sua imagem para seu balde GCP

Complete o seguinte procedimento para converter e carregar sua imagem para seu balde GCP. As amostras são representativas; elas convertem uma imagem **qcow2** para o formato **raw** e, em seguida, tar essa imagem para upload.

Procedimento

1. Execute o comando **qemu-img** para converter sua imagem. A imagem convertida deve ter o nome **disk.raw**.

```
# qemu-img converter -f qcow2 -O bruto rel-8.2-sample.qcow2 disk.raw
```

2. Tar a imagem.

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

3. Carregue a imagem para o balde que você criou anteriormente. O upload pode demorar alguns minutos.

```
# gsutil cp disk.raw.tar.gz gs://bucket_name
```

4. A partir da tela inicial **Google Cloud Platform**, clique no ícone do menu colapsado e selecione **Storage** e depois selecione **Browser**.

5. Clique no nome do seu balde.
A imagem asfaltada está listada sob o nome de seu balde.

NOTA

Você também pode carregar sua imagem usando o site **GCP Console**. Para fazer isso, clique no nome do seu balde e depois clique em **Upload files**.

Recursos adicionais

- Importação manual de discos virtuais
- Escolhendo um método de importação

5.4.6. Criar uma imagem a partir do objeto no balde GCP

Realize o seguinte procedimento para criar uma imagem a partir do objeto em seu balde GCP.

Procedimento

1. Execute o seguinte comando para criar uma imagem para GCE. Especifique o nome da imagem que você está criando, o nome do balde e o nome da imagem asfaltada.

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

NOTA

Alternativamente, você pode usar o Console do Google Cloud para criar uma imagem. Consulte Criando, apagando e depreciando imagens personalizadas para obter mais informações.

2. Opcionalmente, encontre a imagem no Console GCP.
   a. Clique no menu **Navigation** à esquerda do banner **Google Cloud Console**.
   b. Selecione **Compute Engine** e depois **Images**.

Recursos adicionais

- Criando, apagando e depreciando imagens personalizadas
- imagens de computação em nuvem criam

5.4.7. Criando uma instância do Google Compute Engine a partir de uma imagem

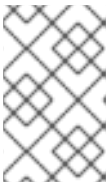
Complete os seguintes passos para configurar uma instância GCE VM usando o GCP Console.

NOTA

O procedimento a seguir fornece instruções para criar uma instância básica de VM usando o Console GCP. Veja Criando e iniciando uma instância VM para mais informações sobre instâncias VM GCE e suas opções de configuração.

Procedimento

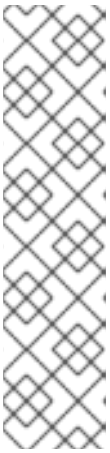
1. A partir da página Painel de Controle do Console GCP , clique no menu **Navigation** à esquerda do Google **Cloud Console banner** e selecione **Compute Engine** e depois selecione **Images**.
2. Selecione sua imagem.
3. Clique em **Create Instance**.
4. Na página **Create an instance**, digite um **Name** para seu exemplo.
5. Escolha um **Region** e **Zone**.
6. Escolha um **Machine configuration** que atenda ou exceda as exigências de sua carga de trabalho.
7. Certifique-se de que **Boot disk** especifique o nome de sua imagem.
8. Opcionalmente, em **Firewall**, selecione **Allow HTTP traffic** ou **Allow HTTPS traffic**.
9. Clique em **Create**.



NOTA

Estas são as opções mínimas de configuração necessárias para criar uma instância básica. Revise opções adicionais com base nas exigências de sua aplicação.

10. Encontre sua imagem em **VM instances**.
11. No Painel de Controle do Console GCP, clique no menu **Navigation** à esquerda do Google **Cloud Console banner** e selecione **Compute Engine** e depois selecione **VM instances**.



NOTA

Alternativamente, você pode usar o comando **gcloud compute instances create** CLI para criar uma instância GCE VM a partir de uma imagem. Segue um exemplo simples.

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

O exemplo cria uma instância VM chamada **myinstance3** na zona **us-central1-a** com base na imagem existente **test-iso2-image**. Veja a criação de instâncias gcloud compute para mais informações.

5.4.8. Conectando-se à sua instância

Execute o seguinte procedimento para conectar-se à sua instância GCE usando seu endereço IP público.

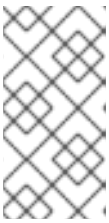
Procedimento

1. Execute o seguinte comando para garantir que sua instância esteja funcionando. O comando lista informações sobre sua instância GCE, incluindo se a instância está rodando e, em caso afirmativo, o endereço IP público da instância em execução.

```
# lista de instâncias de computação em gcloud
```

2. Conecte-se à sua instância usando SSH padrão. O exemplo utiliza a chave **google_compute_engine** criada anteriormente.

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



NOTA

A GCP oferece uma série de formas de SSH em sua instância. Consulte Conectando-se às instâncias para obter mais informações. Você também pode se conectar à sua instância usando a conta raiz e a senha que você definiu anteriormente.

Recursos adicionais

- lista de instâncias de computação em nuvem
- Conexão com instâncias

5.4.9. Anexando assinaturas da Red Hat

Complete os seguintes passos para anexar as assinaturas que você ativou anteriormente através do programa Red Hat Cloud Access.

Pré-requisitos

Você deve ter habilitado suas assinaturas.

Procedimento

1. Registre seu sistema.

```
registro de gerenciador de assinaturas --auto-attach
```

2. Anexe suas assinaturas.
   - Você pode usar uma chave de ativação para anexar as assinaturas. Consulte Criando Chaves de Ativação do Portal do Cliente Red Hat para mais informações.
   - Alternativamente, você pode anexar manualmente uma assinatura usando o ID do pool de assinaturas (Pool ID). Veja Anexar e remover assinaturas através da Linha de Comando .

Recursos adicionais

- Criando as chaves de ativação do Portal do Cliente Red Hat
- Anexar e remover assinaturas através da linha de comando
- Uso e configuração do Red Hat Subscription Manager

CAPÍTULO 6. CONFIGURANDO O RED HAT HIGH AVAILABILITY CLUSTER NA PLATAFORMA GOOGLE CLOUD

Este capítulo inclui informações e procedimentos para configurar um cluster Red Hat High Availability (HA) na plataforma Google Cloud Platform (GCP) usando as instâncias da máquina virtual (VM) do Google Compute Engine (GCE) como nós de cluster.

Este capítulo inclui procedimentos prévios para a criação de seu ambiente para GCP. Uma vez que você tenha configurado seu ambiente, você pode criar e configurar instâncias VM.

Este capítulo também inclui procedimentos específicos para a criação de clusters de HA, que transformam os nós individuais em um cluster de nós de HA sobre GCP. Estes incluem procedimentos para instalação dos pacotes e agentes de Alta Disponibilidade em cada nó de cluster, configuração de cercas, e instalação de agentes de recursos de rede.

Pré-requisitos

- Você deve estar matriculado no programa Red Hat Cloud Access e ter assinaturas RHEL não utilizadas. A assinatura anexa deve incluir acesso aos seguintes repositórios para cada instância GCP.
  - Red Hat Enterprise Linux 8 Server: rhel-8-server-rpms/8Server/x86_64
  - Red Hat Enterprise Linux 8 Server (Alta Disponibilidade): rhel-8-server-ha-rpms/8Server/x86_64
- Você deve pertencer a um projeto GCP ativo e ter permissões suficientes para criar recursos no projeto.
- Seu projeto deve ter uma conta de serviço que pertença a uma instância da VM e não a um usuário individual. Consulte Utilizando a Conta de Serviço Padrão do Motor de Computação para obter informações sobre o uso da conta de serviço padrão em vez de criar uma conta de serviço separada.

Se você ou seu administrador de projeto criar uma conta de serviço personalizada, a conta de serviço deve ser configurada para as seguintes funções.

- Agente de traços de nuvens
- Administração do cálculo
- Cálculo de Administração de Rede
- Usuário do Cloud Datastore
- Administração de Logging
- Editor de monitoramento
- Monitoramento do Escritor de Métricas
- Administrador de conta de serviço
- Administração de armazenamento

Recursos adicionais

- Políticas de apoio aos clusters RHEL de alta disponibilidade - Protocolos de transporte
- Visão geral da rede VPC
- Explorando os componentes, conceitos e características da RHEL High Availability - Visão geral dos protocolos de transporte
- Orientação de Projeto para os Clusters de Alta Disponibilidade RHEL - Seleção do Protocolo de Transporte

6.1. PACOTES DE SISTEMAS REQUERIDOS

Os procedimentos neste capítulo assumem que você está usando um sistema host rodando o Red Hat Enterprise Linux. Para completar os procedimentos com sucesso, seu sistema hospedeiro deve ter os seguintes pacotes instalados.

Tabela 6.1. Pacotes de sistemas

Pacote	Repositório	Descrição
libvirt	rhel-8-for-x86_64-appstream-rpms	API de código aberto, daemon e ferramenta de gerenciamento para gerenciar a virtualização da plataforma
virt-install	rhel-8-for-x86_64-appstream-rpms	Um utilitário de linha de comando para a construção de VMs
libguestfs	rhel-8-for-x86_64-appstream-rpms	Uma biblioteca para acesso e modificação de sistemas de arquivos VM
libguestfs-tools	rhel-8-for-x86_64-appstream-rpms	Ferramentas de administração do sistema para VMs; inclui o utilitário guestfish

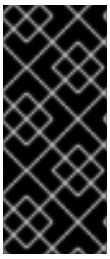
6.2. OPÇÕES DE IMAGEM DO RED HAT ENTERPRISE LINUX NO GCP

A tabela a seguir lista as opções de imagem e as diferenças nas opções de imagem.

Tabela 6.2. Opções de imagem

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações

Opção de imagem	Assinaturas	Exemplo de cenário	Considerações
Opte por implantar uma imagem personalizada que você transfira para GCP.	Aproveite suas assinaturas de Red Hat existentes.	Habilite as assinaturas através do programa Red Hat Cloud Access, faça o upload de sua imagem personalizada e anexe suas assinaturas.	A assinatura inclui o custo do produto Red Hat; você paga todos os outros custos de instância. As imagens personalizadas que você move para o GCP são chamadas de imagens "Cloud Access" porque você aproveita suas assinaturas Red Hat existentes. A Red Hat fornece suporte diretamente para imagens de Cloud Access.
Escolha a implantação de uma imagem GCP existente que inclua a RHEL.	As imagens do GCP incluem um produto Red Hat.	Escolha uma imagem RHEL quando você lança uma instância no GCP Compute Engine, ou escolha uma imagem do Google Cloud Platform Marketplace.	Você paga GCP por hora em um modelo pay-as-you-go. Tais imagens são chamadas de imagens "on-demand". A GCP oferece suporte para imagens sob demanda através de um contrato de suporte.



IMPORTANTE

Você não pode converter uma instância sob demanda para uma instância de Red Hat Cloud Access. Para mudar de uma imagem on-demand para uma imagem do Red Hat Cloud Access bring-your-own-subscription (BYOS), crie uma nova instância do Red Hat Cloud Access e migre os dados de sua instância on-demand. Cancele sua instância on-demand depois de migrar seus dados para evitar a dupla cobrança.

O restante deste capítulo inclui informações e procedimentos relativos às imagens personalizadas.

Recursos adicionais

- Red Hat na Nuvem Pública
- Imagens
- Guia de Referência de Acesso à Nuvem da Red Hat
- Criação de uma instância a partir de uma imagem personalizada

6.3. INSTALANDO O GOOGLE CLOUD SDK

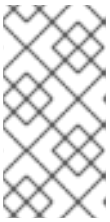
Complete os seguintes passos para instalar o Google Cloud SDK.

Pré-requisitos

- Crie um projeto sobre o GCP, caso ainda não o tenha feito. Veja Criar um novo projeto na plataforma Google Cloud para mais informações.
- Certifique-se de que seu sistema hospedeiro inclua Python 2.7. Se não incluir, instale o Python 2.7.

Procedimento

1. Siga as instruções GCP para baixar e extrair o arquivo do Google Cloud SDK. Veja o documento GCP Quickstart para Linux para maiores detalhes.
2. Siga as mesmas instruções para inicializar o Google Cloud SDK.



NOTA

Uma vez inicializado o Google Cloud SDK, você pode usar os comandos **gcloud** CLI para realizar tarefas e obter informações sobre seu projeto e instâncias. Por exemplo, você pode exibir informações sobre o projeto com o comando **gcloud compute project-info describe --project <project-name>**.

Recursos adicionais

- Início rápido para Linux
- referência de comando gcloud
- visão geral da ferramenta de linha de comando gcloud

6.4. CRIAÇÃO DE UM BALDE DE IMAGEM GCP

O documento a seguir inclui os requisitos mínimos para a criação de um balde multi-regional em seu local padrão.

Pré-requisitos

Utilitário de armazenamento GCP (gsutil)

Procedimento

1. Se você ainda não está logado na plataforma Google Cloud, faça o login com o seguinte comando.

```
# gcloud auth login
```

2. Criar um balde de armazenamento.

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

Exemplo:

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

Recursos adicionais

Fazer baldes

6.5. CRIAÇÃO DE UMA REDE E SUB-REDE PRIVADA VIRTUAL PERSONALIZADA DE NUVENS

Complete os seguintes passos para criar uma rede e sub-rede personalizada de nuvem privada virtual (VPC).

Procedimento

1. Lançar o Console GCP.
2. Selecione **VPC networks** em **Networking** no painel de navegação à esquerda.
3. Clique em **Create VPC Network**
4. Digite um nome para a rede VPC.
5. Sob o **New subnet**, crie um **Custom subnet** na região onde você deseja criar o agrupamento.
6. Clique em **Create**.

6.6. PREPARAÇÃO E IMPORTAÇÃO DE UMA IMAGEM GCP DE BASE

Complete os seguintes passos para preparar a imagem para GCP.

Procedimento

1. Digite o seguinte comando para converter o arquivo. As imagens carregadas no GCP devem estar no formato **raw** e nomeadas **disk.raw**.

```
$ qemu-img converter -f qcow2 ImageName.qcow2 -O disco.raw
```

2. Digite o seguinte comando para comprimir o arquivo **raw**. As imagens carregadas no GCP devem ser comprimidas.

```
$ alcatrão -Sczf ImageName.tar.gz disk.raw
```

3. Importar a imagem comprimida para o balde criado anteriormente.

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

6.7. CRIAÇÃO E CONFIGURAÇÃO DE UMA INSTÂNCIA BASE GCP

Complete os seguintes passos para criar e configurar uma instância GCP que esteja em conformidade com os requisitos operacionais e de segurança da GCP.

Procedimento

1. Insira o seguinte comando para criar uma imagem a partir do arquivo comprimido no balde.

```
$ gcloud criar imagens de computação BaseImageName --source-uri
gs://BucketName/BaseImageName.tar.gz
```

Exemplo:

```
[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. Insira o seguinte comando para criar uma instância modelo a partir da imagem. O tamanho mínimo requerido para uma instância base RHEL é n1-standard-2. Veja gcloud compute instances create para opções adicionais de configuração.

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

Exemplo:

```
[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. Conecte-se à instância com uma sessão terminal SSH.

```
$ ssh root@PublicIPaddress
```

4. Atualizar o software RHEL.

   a. Cadastre-se no Red Hat Subscription Manager (RHSM).

   b. Habilitar um ID de Pool de Assinaturas (ou usar o comando **--auto-attach**).

   c. Desativar todos os repositórios.

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

   d. Habilite o seguinte repositório.

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

   e. Execute o comando **yum update**.

```
# yum update -y
```

5. Instale o Ambiente Convidado GCP Linux na instância em execução (instalação no local). Veja Instalar o ambiente do hóspede no local para instruções.

6. Selecione a opção **CentOS/RHEL**.

7. Copie o roteiro de comando e cole-o no prompt de comando para executar o roteiro imediatamente.

8. Faça as seguintes mudanças de configuração na instância. Estas mudanças são baseadas nas recomendações do GCP para imagens personalizadas. Veja a lista de imagens gcloudcompute para mais informações.

   a. Edite o arquivo **/etc/chrony.conf** e remova todos os servidores NTP.

   b. Adicione o seguinte servidor NTP.

   ```
   metadados.google.internal iburst Google NTP server
   ```

   c. Remover quaisquer regras persistentes de dispositivos de rede.

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

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

   d. Configurar o serviço de rede para iniciar automaticamente.

   ```
   # rede chkconfig em
   ```

   e. Defina o **sshd service** para iniciar automaticamente.

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

   f. Digite o seguinte comando para definir o fuso horário como UTC.

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

   g. (Opcional) Edite o arquivo **/etc/ssh/ssh_config** e adicione as seguintes linhas ao final do arquivo. Isto mantém sua sessão SSH ativa durante períodos mais longos de inatividade.

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

   h. Edite o arquivo **/etc/ssh/sshd_config** e faça as seguintes mudanças, se necessário. A configuração **ClientAliveInterval 420** é opcional; isto mantém sua sessão SSH ativa durante períodos mais longos de inatividade.

   ```
   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. Digite o seguinte comando para desativar o acesso por senha. Edite o arquivo **/etc/cloud/cloud.cfg**.

```
ssh_pwauth from 1 to 0.
ssh_pwauth: 0
```

IMPORTANTE

Anteriormente, você habilitava o acesso por senha para permitir o acesso à sessão SSH para configurar a instância. Você deve desativar o acesso com senha. Todo acesso à sessão SSH deve ser sem senhas.

10. Digite o seguinte comando para desregistrar a instância do gerente da assinatura.

```
# não-registo do gerenciador de assinaturas
```

11. Digite o seguinte comando para limpar o histórico da casca. Mantenha a instância funcionando para o próximo procedimento.

```
# exportação HISTSIZE=0
```

6.8. CRIANDO UMA IMAGEM INSTANTÂNEA

Complete os seguintes passos para preservar as configurações da instância e criar um instantâneo.

Procedimento

1. Na instância em execução, digite o seguinte comando para sincronizar os dados com o disco.

```
# Sincronia
```

2. Em seu sistema hospedeiro, digite o seguinte comando para criar o instantâneo.

```
$ gcloud compute disks snapshot InstanceName --snapshot-nomes SnapshotName
```

3. Em seu sistema host, digite o seguinte comando para criar a imagem configurada a partir do instantâneo.

```
Imagens de computação em nuvem criam ConfiguredImageFromSnapshot --source-
snapshot SnapshotName
```

Recursos adicionais

Criando Instantâneos Persistentes de Disco

6.9. CRIAÇÃO DE UMA INSTÂNCIA DE MODELO DE NÓ HA E NÓS HA

Uma vez que você tenha configurado uma imagem a partir do instantâneo, você pode criar um modelo de nó. Use este modelo para criar todos os nós HA. Complete os seguintes passos para criar o modelo e os nós HA.

Procedimento

1. Digite o seguinte comando para criar um modelo de instância.

```
$ gcloud compute instance-templates create InstanceTemplateName --can-ip-forward --
machine-type n1-standard-2  --image ConfiguredImageFromSnapshot --service-account
ServiceAccountEmailAddress
```

   Exemplo:

```
[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. Digite o seguinte comando para criar vários nós em uma zona.

```
# instâncias de computação gcloud criar NodeName01 NodeName02 --source-instance-
template InstanceTemplateName --zone RegionZone --network=NetworkName --
subnet=SubnetName
```

   Exemplo:

```
[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. INSTALAÇÃO DE PACOTES E AGENTES HA

Complete os seguintes passos em todos os nós.

Procedimento

1. No Console do Google Cloud, selecione **Compute Engine** e depois **VM instances**.
2. Selecione a instância, clique na seta ao lado de **SSH**, e selecione a opção de comando **View gcloud**.
3. Cole este comando em um prompt de comando para acesso sem senhas à instância.
4. Permitir o acesso à conta sudo e o registro junto ao Gerente de Assinaturas da Red Hat.
5. Habilitar um ID de Pool de Assinaturas (ou usar o comando **--auto-attach**).
6. Desativar todos os repositórios.

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

7. Habilitar os seguintes repositórios.

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

8. Instale **pcs pacemaker**, os agentes de vedação e os agentes de recursos.

```
# yum install -y pcs pacemaker fence-agents-gce resource-agents-gcp
```

9. Atualizar todos os pacotes.

```
# yum update -y
```

6.11. CONFIGURAÇÃO DOS SERVIÇOS HA

Complete os seguintes passos em todos os nós para configurar os serviços HA.

Procedimento

1. O usuário **hacluster** foi criado durante a instalação de **pcs** e **pacemaker** na etapa anterior. Criar uma senha para o usuário **hacluster** em todos os nós de cluster. Use a mesma senha para todos os nós.

```
# hacluster da senha
```

2. Se o serviço **firewalld** estiver instalado, digite o seguinte comando para adicionar o serviço HA.

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

# firewall-cmd --reload
```

3. Digite o seguinte comando para iniciar o serviço **pcs** e habilite-o para iniciar na inicialização.

```
# 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.
```

Etapas de verificação

1. Certifique-se de que o serviço **pcsd** esteja 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 o arquivo **/etc/hosts**. Adicionar nomes de hosts RHEL e endereços IP internos para todos os nós.

Recursos adicionais

Como o arquivo /etc/hosts deve ser configurado nos nós de cluster RHEL?

6.12. CRIAÇÃO DE UM CLUSTER

Complete os seguintes passos para criar o conjunto de nós.

Procedimento

1. Em um dos nós, digite o seguinte comando para autenticar o usuário do pcs. Especifique o nome de cada nó do cluster no comando.

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

2. Digite o seguinte comando para criar o agrupamento.

```
# pcs cluster setup cluster-name hostname1 hostname2 _hostname3-
```

Etapas de verificação

1. Execute o seguinte comando para permitir que os nós se juntem ao cluster automaticamente quando iniciado.

```
# pcs cluster enable --tudo
```

2. Digite o seguinte comando para iniciar o agrupamento.

```
# pcs cluster start --tudo
```

6.13. CRIANDO UM DISPOSITIVO DE ESGRIMA

Para a maioria das configurações padrão, os nomes das instâncias GCP e os nomes dos anfitriões RHEL são idênticos.

Complete os seguintes passos para criar um dispositivo de esgrima.

Procedimento

1. Digite o seguinte comando para obter nomes de instâncias GCP. Note que a saída também mostra a identificação interna da instância.

```
# fence_gce --zone us-west1-b --project=rhel-ha-on-gcp -o list
```

Exemplo:

```
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. Digite o seguinte comando para criar um dispositivo de cerca.

```
# pcs stonith create _FenceDeviceName_ fence_gce zone=_Region-Zone_
project=_MyProject_
```

Etapa de verificação

Verificar se os dispositivos da cerca começaram.

```
# pcs status
```

Exemplo:

```
[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. CONFIGURAÇÃO DA AUTORIZAÇÃO DO NÓ GCP

Configure as ferramentas SDK da nuvem para usar suas credenciais de conta para acessar o GCP.

Procedimento

Insira o seguinte comando em cada nó para inicializar cada nó com seu ID de projeto e credenciais de conta.

```
# gcloud-ra init
```

6.15. CONFIGURAÇÃO DO AGENTE DE RECURSOS GCP-VCP-MOVE-VIP

O agente de recursos **gcp-vpc-move-vip** anexa um endereço IP secundário (alias IP) a uma instância em execução. Este é um endereço IP flutuante que pode ser passado entre os diferentes nós do cluster.

Digite o seguinte comando para mostrar mais informações sobre este recurso.

```
# Recursos pcs descrever gcp-vpc-move-vip
```

Você pode configurar o agente de recursos para usar uma faixa de endereços de sub-rede primária ou uma faixa de endereços de sub-rede secundária. Esta seção inclui procedimentos para ambas as faixas.

Primary subnet address range

Complete os seguintes passos para configurar o recurso para a subrede VPC primária.

Procedimento

1. Digite o seguinte comando para criar o recurso **aliasip**. Inclua um endereço IP interno não utilizado. Inclua o bloco CIDR no comando.

   ```
   # pcs resource create aliasip gcp-vpc-move-vip  alias_ip=UnusedIPaddress/CIDRblock
   ```

   Exemplo:

   ```
   [root@rhel81-node-01 ~]# pcs resource create aliasip gcp-vpc-move-vip
   alias_ip=10.10.10.200/32
   ```

2. Digite o seguinte comando para criar um recurso **IPaddr2** para gerenciar o IP no nó.

   ```
   # pcs resource create vip IPaddr2 nic=interface ip=AliasIPaddress cidr_netmask=32
   ```

   Exemplo:

```
[root@rhel81-node-01 ~]# pcs resource create vip IPaddr2 nic=eth0 ip=10.10.10.200
cidr_netmask=32
```

3. Digite o seguinte comando para agrupar os recursos da rede em **vipgrp**.

```
# grupo de recursos pcs adicionar vipgrp aliasip vip
```

Etapas de verificação

1. Digite o seguinte comando para verificar se os recursos começaram e estão agrupados sob **vipgrp**.

```
[root@rhel81-node-01 ~]# pcs status
```

2. Digite o seguinte comando para verificar se o recurso pode se mover para um nó diferente.

```
# pcs resource move vip _Node_
```

Exemplo:

```
[root@rhel81-node-01 ~]# pcs resource move vip rhel81-node-03
```

3. Digite o seguinte comando para verificar se o **vip** começou com sucesso em um nó diferente.

```
[root@rhel81-node-01 ~]# pcs status
```

Secondary subnet address range

Complete os seguintes passos para configurar o recurso para uma faixa de endereços de sub-rede secundária.

Pré-requisitos

Criar uma rede e sub-rede personalizada

Procedimento

1. Digite o seguinte comando para criar uma faixa de endereços de sub-rede secundária.

```
# atualização das sub-redes de redes de computação gcloud-ra SubnetName --região
RegionName --add-secondary-ranges SecondarySubnetName=SecondarySubnetRange
```

Exemplo:

```
# rede de computação gcloud-ra faixa de atualização das sub-redes0 --região us-west1 --
add-secundário faixa1=10.10.20.0/24
```

2. Digite o seguinte comando para criar o recurso **aliasip**. Crie um endereço IP interno não utilizado na faixa de endereços de sub-rede secundária. Inclua o bloco CIDR no comando.

```
# pcs resource create aliasip gcp-vpc-move-vip alias_ip=UnusedIPaddress/CIDRblock
```

Exemplo:

```
[root@rhel81-node-01 ~]# pcs resource create aliasip gcp-vpc-move-vip
alias_ip=10.10.20.200/32
```

3. Digite o seguinte comando para criar um recurso **IPaddr2** para gerenciar o IP no nó.

```
# pcs resource create vip IPaddr2 nic=interface ip=AliasIPaddress cidr_netmask=32
```

Exemplo:

```
[root@rhel81-node-01 ~]# pcs resource create vip IPaddr2 nic=eth0 ip=10.10.20.200
cidr_netmask=32
```

4. Agrupar os recursos da rede em **vipgrp**.

```
# grupo de recursos pcs adicionar vipgrp aliasip vip
```

Etapas de verificação

1. Digite o seguinte comando para verificar se os recursos começaram e estão agrupados sob **vipgrp**.

```
[root@rhel81-node-01 ~]# pcs status
```

2. Digite o seguinte comando para verificar se o recurso pode se mover para um nó diferente.

```
# pcs resource move vip _Node_
```

Exemplo:

```
[root@rhel81-node-01 ~]# pcs resource move vip rhel81-node-03
```

3. Digite o seguinte comando para verificar se o **vip** começou com sucesso em um nó diferente.

```
[root@rhel81-node-01 ~]# pcs status
```