Red Hat Enterprise Linux 9

Déploiement de RHEL 9 sur Microsoft Azure

Obtenir des images système RHEL et créer des instances RHEL sur Azure

Last Updated: 2024-02-22

Red Hat Enterprise Linux 9 Déploiement de RHEL 9 sur Microsoft Azure

Obtenir des images système RHEL et créer des instances RHEL sur Azure

Notice légale

Résumé

Pour utiliser Red Hat Enterprise Linux (RHEL) dans un environnement de cloud public, vous pouvez créer et déployer des images système RHEL sur diverses plateformes de cloud, y compris Microsoft Azure. Vous pouvez également créer et configurer un cluster Red Hat High Availability (HA) sur Azure. Les chapitres suivants fournissent des instructions pour créer des instances RHEL en nuage et des clusters HA sur Azure. Ces processus comprennent l'installation des paquets et des agents requis, la configuration de la clôture et l'installation des agents de ressources réseau.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

CHAPITRE 1. PRÉSENTATION DE RHEL SUR LES PLATES-FORMES DE CLOUD PUBLIC

Les plateformes de cloud public fournissent des ressources informatiques en tant que service. Au lieu d'utiliser du matériel sur site, vous pouvez exécuter vos charges de travail informatiques, y compris les systèmes Red Hat Enterprise Linux (RHEL), en tant qu'instances de cloud public.

Pour en savoir plus sur RHEL sur les plates-formes de cloud public, voir :

- Avantages de l'utilisation de RHEL dans un nuage public
- Cas d'utilisation de RHEL dans les nuages publics
- Problèmes fréquents lors de la migration vers un nuage public
- Obtenir RHEL pour les déploiements dans les nuages publics
- Méthodes de création d'instances de cloud RHEL

1.1. AVANTAGES DE L'UTILISATION DE RHEL DANS UN NUAGE PUBLIC

RHEL en tant qu'instance cloud située sur une plateforme cloud publique présente les avantages suivants par rapport à RHEL sur des systèmes physiques ou des machines virtuelles (VM) sur site :

- **Flexible and fine-grained allocation of resources**
  Une instance cloud de RHEL s'exécute en tant que VM sur une plateforme cloud, ce qui signifie généralement une grappe de serveurs distants gérée par le fournisseur du service cloud. Par conséquent, l'attribution de ressources matérielles à l'instance, telles qu'un type spécifique d'unité centrale ou de stockage, se fait au niveau du logiciel et est facilement personnalisable.

  Par rapport à un système RHEL local, vous n'êtes pas non plus limité par les capacités de votre hôte physique. Au lieu de cela, vous pouvez choisir parmi une variété de fonctionnalités, sur la base de la sélection proposée par le fournisseur de services en nuage.

- **Space and cost efficiency**
  Vous n'avez pas besoin de posséder des serveurs sur site pour héberger vos charges de travail en nuage. Vous n'avez donc pas besoin de l'espace, de l'énergie et de la maintenance associés au matériel physique.

  En revanche, sur les plateformes de cloud public, vous payez directement le fournisseur de cloud pour l'utilisation d'une instance de cloud. Le coût est généralement basé sur le matériel alloué à l'instance et sur le temps que vous passez à l'utiliser. Vous pouvez donc optimiser vos coûts en fonction de vos besoins.

- **Software-controlled configurations**
  L'ensemble de la configuration d'une instance en nuage est sauvegardé sous forme de données sur la plateforme en nuage et est contrôlé par un logiciel. Vous pouvez donc facilement créer, supprimer, cloner ou migrer l'instance. Une instance en nuage est également gérée à distance dans une console du fournisseur de nuage et est connectée par défaut à un stockage à distance.

  En outre, vous pouvez à tout moment sauvegarder l'état actuel d'une instance cloud sous la forme d'un instantané. Ensuite, vous pouvez charger l'instantané pour restaurer l'instance à l'état sauvegardé.

- **Separation from the host and software compatibility**

Comme pour une VM locale, le système d'exploitation invité RHEL sur une instance cloud s'exécute sur un noyau virtualisé. Ce noyau est distinct du système d'exploitation hôte et du système *client* que vous utilisez pour vous connecter à l'instance.

Par conséquent, n'importe quel système d'exploitation peut être installé sur l'instance de cloud. Cela signifie que sur une instance de cloud public RHEL, vous pouvez exécuter des applications spécifiques à RHEL qui ne peuvent pas être utilisées sur votre système d'exploitation local.

En outre, même si le système d'exploitation de l'instance devient instable ou est compromis, votre système client n'est en aucun cas affecté.

Ressources supplémentaires

- Qu'est-ce que l'informatique dématérialisée ?
- Qu'est-ce qu'un hyperscaler ?
- Types d'informatique en nuage
- Cas d'utilisation de RHEL dans les nuages publics
- Obtenir RHEL pour les déploiements dans les nuages publics

1.2. CAS D'UTILISATION DE RHEL DANS LES NUAGES PUBLICS

Le déploiement sur un cloud public présente de nombreux avantages, mais n'est pas forcément la solution la plus efficace dans tous les cas de figure. Si vous envisagez de migrer vos déploiements RHEL vers le cloud public, demandez-vous si votre cas d'utilisation bénéficiera des avantages du cloud public.

Beneficial use cases

- Le déploiement d'instances de cloud public est très efficace pour augmenter et réduire de manière flexible la puissance informatique active de vos déploiements, également connue sous les noms de *scaling up* et *scaling down*. Par conséquent, l'utilisation de RHEL sur le cloud public est recommandée dans les scénarios suivants :
  - Clusters avec des charges de travail de pointe élevées et de faibles exigences de performance générale. La mise à l'échelle en fonction de vos besoins peut s'avérer très efficace en termes de coûts de ressources.
  - Mise en place ou extension rapide de vos clusters. Cela permet d'éviter les coûts initiaux élevés liés à la mise en place de serveurs locaux.
- Les instances en nuage ne sont pas affectées par ce qui se passe dans votre environnement local. Vous pouvez donc les utiliser pour la sauvegarde et la reprise après sinistre.

Potentially problematic use cases

- Vous utilisez un environnement existant qui ne peut pas être adapté. La personnalisation d'une instance en nuage pour répondre aux besoins spécifiques d'un déploiement existant peut ne pas être rentable par rapport à votre plateforme hôte actuelle.
- Votre budget est limité. Le maintien de votre déploiement dans un centre de données local offre généralement moins de flexibilité mais plus de contrôle sur les coûts maximaux des ressources que le nuage public.

Prochaines étapes

- Obtenir RHEL pour les déploiements dans les nuages publics

Ressources supplémentaires

- Dois-je migrer mon application vers l'informatique dématérialisée ? Voici comment décider.

1.3. PROBLÈMES FRÉQUENTS LORS DE LA MIGRATION VERS UN NUAGE PUBLIC

Le transfert de vos charges de travail RHEL d'un environnement local vers une plateforme de cloud public peut susciter des inquiétudes quant aux changements qu'il implique. Voici les questions les plus fréquemment posées.

Will my RHEL work differently as a cloud instance than as a local virtual machine?

À la plupart des égards, les instances RHEL sur une plateforme de cloud public fonctionnent de la même manière que les machines virtuelles RHEL sur un hôte local, tel qu'un serveur sur site. Les exceptions notables sont les suivantes :

- Au lieu d'interfaces d'orchestration privées, les instances de cloud public utilisent des interfaces de console spécifiques au fournisseur pour gérer vos ressources de cloud.
- Certaines fonctionnalités, telles que la virtualisation imbriquée, peuvent ne pas fonctionner correctement. Si une fonctionnalité spécifique est essentielle pour votre déploiement, vérifiez au préalable sa compatibilité avec le fournisseur de cloud public que vous avez choisi.

Will my data stay safe in a public cloud as opposed to a local server?

Les données de vos instances de cloud RHEL sont votre propriété et votre fournisseur de cloud public n'y a pas accès. En outre, les principaux fournisseurs de cloud prennent en charge le cryptage des données en transit, ce qui améliore la sécurité des données lors de la migration de vos machines virtuelles vers le cloud public.

La sécurité générale de vos instances de cloud public RHEL est gérée comme suit :

- Votre fournisseur de cloud public est responsable de la sécurité de l'hyperviseur du cloud
- Red Hat fournit les fonctions de sécurité des systèmes d'exploitation invités RHEL dans vos instances
- Vous gérez les paramètres et les pratiques de sécurité spécifiques de votre infrastructure en nuage

What effect does my geographic region have on the functionality of RHEL public cloud instances?

Vous pouvez utiliser des instances RHEL sur une plateforme de cloud public quelle que soit votre situation géographique. Par conséquent, vous pouvez exécuter vos instances dans la même région que votre serveur sur site.

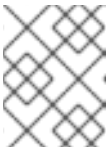
Toutefois, l'hébergement de vos instances dans une région physiquement éloignée peut entraîner une latence élevée lors de leur fonctionnement. En outre, selon le fournisseur de cloud public, certaines régions peuvent offrir des fonctionnalités supplémentaires ou être plus rentables. Avant de créer vos instances RHEL, examinez les propriétés des régions d'hébergement disponibles pour le fournisseur de cloud choisi.

1.4. OBTENIR RHEL POUR LES DÉPLOIEMENTS DANS LES NUAGES PUBLICS

Pour déployer un système RHEL dans un environnement de cloud public :

1. Sélectionnez le fournisseur de services en nuage optimal pour votre cas d'utilisation, en fonction de vos besoins et de l'offre actuelle sur le marché.
   Les fournisseurs de services en nuage actuellement certifiés pour l'exécution d'instances RHEL sont les suivants :

   - Amazon Web Services (AWS)
   - Google Cloud Platform (GCP)
   - Microsoft Azure

   NOTE

   Ce document traite spécifiquement du déploiement de RHEL sur Microsoft Azure.

2. Créez une instance de cloud RHEL sur la plateforme de cloud choisie. Pour plus d'informations, voir Méthodes de création d'instances de cloud RHEL .
3. Pour maintenir votre déploiement RHEL à jour, utilisez Red Hat Update Infrastructure (RHUI).

Ressources supplémentaires

- Documentation RHUI
- Red Hat Open Hybrid Cloud

1.5. MÉTHODES DE CRÉATION D'INSTANCES DE CLOUD RHEL

Pour déployer une instance RHEL sur une plateforme de cloud public, vous pouvez utiliser l'une des méthodes suivantes :

Create a system image of RHEL and import it to the cloud platform.

- Pour créer l'image système, vous pouvez utiliser le générateur d'images RHEL ou construire l'image manuellement.
- Cette méthode utilise votre abonnement RHEL existant et est également appelée *bring your own subscription* (BYOS).
- Vous payez à l'avance un abonnement annuel et vous pouvez utiliser votre réduction client Red Hat.
- Votre service clientèle est assuré par Red Hat.
- Pour créer plusieurs images de manière efficace, vous pouvez utiliser l'outil **cloud-init**.

Purchase a RHEL instance directly from the cloud provider marketplace.

- Vous post-payez un taux horaire pour l'utilisation du service. Cette méthode est donc également appelée *pay as you go* (PAYG).
- Votre service clientèle est assuré par le fournisseur de la plateforme en nuage.

NOTE

Pour des instructions détaillées sur l'utilisation de différentes méthodes pour déployer des instances RHEL sur Microsoft Azure, voir les chapitres suivants de ce document.

Ressources supplémentaires

- Qu'est-ce qu'une image en or ?
- Configurer et gérer cloud-init pour RHEL 9

CHAPITRE 2. POUSSER DES IMAGES VHD VERS LE NUAGE MICROSOFT AZURE

Vous pouvez créer des images **.vhd** à l'aide de l'outil de création d'images. Ensuite, vous pouvez pousser les images **.vhd** vers un stockage Blob du fournisseur de services Microsoft Azure Cloud.

Conditions préalables

- Vous avez un accès root au système.
- Vous avez accès à l'interface de construction d'images de la console web RHEL.
- Vous avez créé un modèle. Voir Création d'un modèle de constructeur d'images dans l'interface de la console web.
- Vous avez créé un compte de stockage Microsoft .
- Vous avez préparé un stockage Blob accessible en écriture.

Procédure

1. Dans le tableau de bord du constructeur d'images, sélectionnez le modèle que vous souhaitez utiliser.
2. Cliquez sur l'onglet **Images**.
3. Cliquez sur **Créer une image** pour créer votre image **.vhd** personnalisée.
   L'assistant **Create image** s'ouvre.
   a. Sélectionnez **Microsoft Azure (.vhd)** dans la liste du menu déroulant **Type**.
   b. Cochez la case **Upload to Azure** pour télécharger votre image dans le nuage Microsoft Azure.
   c. Saisissez le site **Image Size** et cliquez sur **Next.**
4. Sur la page **Upload to Azure**, saisissez les informations suivantes :
   a. Sur la page Authentification, entrez :
      i. Votre nom **Storage account**. Vous le trouverez sur la page **Storage account**, dans le portail Microsoft Azure.
      ii. Votre **Storage access key**. Vous pouvez le trouver sur la page **Access Key** Storage.
      iii. Cliquez sur **Suivant**.
   b. Sur la page **Authentication**, entrez :
      i. Le nom de l'image.
      ii. Le **Storage container** est le conteneur blob dans lequel vous allez télécharger l'image. Vous le trouverez sous la section **Blob service**, dans le portail Microsoft Azure.
      iii. Cliquez sur **Suivant**.

5. Sur la page **Review**, cliquez sur **Créer**. Les processus de construction et de téléchargement de l'image démarrent.

Prochaines étapes

1. Pour accéder à l'image que vous avez transférée sur **Microsoft Azure Cloud**, accédez au portail Microsoft Azure.
2. Dans la barre de recherche, tapez "compte de stockage" et cliquez sur **Storage accounts** dans la liste.
3. Dans la barre de recherche, tapez "Images" et sélectionnez la première entrée sous **Services**. Vous êtes redirigé vers le site **Image dashboard**.
4. Dans le panneau de navigation, cliquez sur **Containers**.
5. Trouvez le conteneur que vous avez créé. Dans le conteneur se trouve le fichier ***your_image_name*.vhd** que vous avez créé et poussé.

Vérification

Vérifiez que vous pouvez créer une image de VM et la lancer.

1. Dans la barre de recherche, tapez compte images et cliquez sur **Images** dans la liste.
2. Cliquez sur **Créer**.
3. Dans la liste déroulante, choisissez le groupe de ressources que vous avez utilisé précédemment.
4. Entrez un nom pour l'image.
5. Pour le site **OS type**, sélectionnez **Linux**.
6. Pour le site **VM generation**, sélectionnez **Gen 2**.
7. Sous **Storage Blob**, cliquez sur **Parcourir** et cliquez sur les comptes de stockage et les conteneurs jusqu'à ce que vous atteigniez votre fichier VHD.
8. Cliquez sur **Select** à la fin de la page.
9. Choisissez un type de compte, par exemple, **Standard SSD**.
10. Cliquez sur **Réviser créer**, puis sur **Créer**. Attendez quelques instants pour la création de l'image.

Pour lancer la VM, procédez comme suit :

1. Cliquez sur **Aller à la ressource**.
2. Cliquez sur **Créer une VM** dans la barre de menu de l'en-tête.
3. Entrez un nom pour votre machine virtuelle.
4. Complétez les sections **Size** et **Administrator account**.
5. Cliquez sur **Examiner la création**, puis sur **Créer**. Vous pouvez voir la progression du déploiement.

Une fois le déploiement terminé, cliquez sur le nom de la machine virtuelle pour récupérer l'adresse IP publique de l'instance afin de vous connecter à l'aide de SSH.

6. Ouvrez un terminal pour créer une connexion SSH afin de vous connecter à la VM.

Ressources supplémentaires

- Documentation sur le stockage Microsoft Azure .
- Créez un compte Microsoft Azure Storage.
- Ouvrez un dossier sur le portail client de Red Hat .
- Aide à l'assistance.
- Contacter Red Hat.

CHAPITRE 3. DÉPLOYER UNE IMAGE RED HAT ENTERPRISE LINUX EN TANT QUE MACHINE VIRTUELLE SUR MICROSOFT AZURE

Pour déployer une image Red Hat Enterprise Linux 9 (RHEL 9) sur Microsoft Azure, suivez les informations ci-dessous. Ce chapitre :

- Examine les options qui s'offrent à vous pour le choix d'une image
- Liste ou fait référence à la configuration requise pour votre système hôte et votre machine virtuelle (VM)
- Fournit des procédures pour créer une VM personnalisée à partir d'une image ISO, la télécharger vers Azure et lancer une instance de VM Azure

IMPORTANT

Vous pouvez créer une VM personnalisée à partir d'une image ISO, mais Red Hat vous recommande d'utiliser le produit *Red Hat Image Builder* pour créer des images personnalisées à utiliser sur des fournisseurs de cloud spécifiques. Avec Image Builder, vous pouvez créer et télécharger une image disque Azure (format VHD). Voir Composer une image système RHEL personnalisée pour plus d'informations.

Pour obtenir une liste des produits Red Hat que vous pouvez utiliser en toute sécurité sur Azure, reportez-vous à Red Hat sur Microsoft Azure .

Conditions préalables

- Créez un compte sur le portail client de Red Hat .
- Créez un compte Microsoft Azure.

3.1. OPTIONS D'IMAGES RED HAT ENTERPRISE LINUX SUR AZURE

Le tableau suivant répertorie les choix d'images pour RHEL 9 sur Microsoft Azure et indique les différences entre les options d'images.

Tableau 3.1. Options d'images

Option d'image	Abonnements	Exemple de scénario	Considérations
Déployez une image Red Hat Gold.	Utilisez vos abonnements Red Hat existants.	Sélectionnez une Red Hat Gold Image sur Azure. Pour plus de détails sur les Gold Images et la manière d'y accéder sur Azure, consultez le Guide de référence de Red Hat Cloud Access.	L'abonnement inclut le coût du produit Red Hat ; vous payez Microsoft pour tous les autres coûts d'instance.

Option d'image	Abonnements	Exemple de scénario	Considérations
Déployez une image personnalisée que vous déplacez vers Azure.	Utilisez vos abonnements Red Hat existants.	Téléchargez votre image personnalisée et joignez vos abonnements.	L'abonnement inclut le coût du produit Red Hat ; vous payez Microsoft pour tous les autres coûts d'instance.
Déployer une image Azure existante qui inclut RHEL.	Les images Azure comprennent un produit Red Hat.	Choisissez une image RHEL lorsque vous créez une VM à l'aide de la console Azure, ou choisissez une VM sur Azure Marketplace.	Vous payez Microsoft à l'heure sur la base du modèle *pay-as-you-go*. Ces images sont appelées "à la demande" Azure fournit une assistance pour les images à la demande par le biais d'un accord d'assistance. Red Hat fournit des mises à jour aux images. Azure rend les mises à jour disponibles via l'infrastructure de mise à jour Red Hat (RHUI).

Ressources supplémentaires

- Utilisation de Red Hat Gold Images sur Microsoft Azure
- Place de marché Azure
- Options de facturation dans Azure Marketplace
- Red Hat Enterprise Linux Bring-Your-Own-Subscription Gold Images dans Azure
- Guide de référence de Red Hat Cloud Access

3.2. COMPRENDRE LES IMAGES DE BASE

Cette section contient des informations sur l'utilisation d'images de base préconfigurées et leurs paramètres de configuration.

3.2.1. Utilisation d'une image de base personnalisée

Pour configurer manuellement une machine virtuelle (VM), créez d'abord une image VM de base (starter). Vous pouvez ensuite modifier les paramètres de configuration et ajouter les paquets dont la VM a besoin pour fonctionner sur le nuage. Vous pouvez apporter des modifications supplémentaires à la configuration pour votre application spécifique après avoir téléchargé l'image.

Pour préparer une image cloud de RHEL, suivez les instructions des sections ci-dessous. Pour préparer une image Hyper-V de RHEL, reportez-vous à la section Préparer une machine virtuelle basée sur Red Hat à partir du Gestionnaire Hyper-V.

3.2.2. Paquets système requis

Pour créer et configurer une image de base de RHEL, les paquets suivants doivent être installés sur votre système hôte.

Tableau 3.2. Paquets de systèmes

Paquet	Référentiel	Description
libvirt	rhel-9-for-x86_64-appstream-rpms	API, démon et outil de gestion open source pour la gestion de la virtualisation des plateformes
virt-install	rhel-9-for-x86_64-appstream-rpms	Un utilitaire en ligne de commande pour construire des VM
libguestfs	rhel-9-for-x86_64-appstream-rpms	Une bibliothèque pour l'accès et la modification des systèmes de fichiers VM
guestfs-tools	rhel-9-for-x86_64-appstream-rpms	Outils d'administration du système pour les machines virtuelles ; comprend l'utilitaire **virt-customize**

3.2.3. Paramètres de configuration de la VM Azure

Les VM Azure doivent disposer des paramètres de configuration suivants. Certains de ces paramètres sont activés lors de la création initiale de la VM. D'autres paramètres sont définis lors du provisionnement de l'image de la VM pour Azure. Gardez ces paramètres à l'esprit tout au long des procédures. Reportez-vous-y si nécessaire.

Tableau 3.3. Paramètres de configuration de la VM

Paramètres	Recommandation
ssh	ssh doit être activé pour permettre l'accès à distance à vos machines virtuelles Azure.
dhcp	L'adaptateur virtuel principal doit être configuré pour dhcp (IPv4 uniquement).
Espace d'échange	Ne créez pas de fichier ou de partition d'échange dédié. Vous pouvez configurer l'espace d'échange avec l'agent Windows Azure Linux (WALinuxAgent).

Paramètres	Recommandation
NIC	Choisissez **virtio** pour la carte réseau virtuelle principale.
chiffrement	Pour les images personnalisées, utilisez Network Bound Disk Encryption (NBDE) pour un chiffrement complet du disque sur Azure.

3.2.4. Création d'une image de base à partir d'une image ISO

La procédure suivante énumère les étapes et les exigences de configuration initiale pour la création d'une image ISO personnalisée. Une fois l'image configurée, vous pouvez l'utiliser comme modèle pour créer d'autres instances de VM.

Conditions préalables

- Assurez-vous d'avoir activé la virtualisation de votre machine hôte. Voir Activation de la virtualisation dans RHEL 9 pour plus d'informations et de procédures.

Procédure

1. Téléchargez la dernière image ISO DVD de Red Hat Enterprise Linux 9 à partir du portail client de Red Hat.
2. Créez et démarrez une VM Red Hat Enterprise Linux de base. Pour obtenir des instructions, voir Création de machines virtuelles.
   a. Si vous utilisez la ligne de commande pour créer votre VM, veillez à définir la mémoire et les processeurs par défaut en fonction de la capacité souhaitée pour la VM. Définissez votre interface réseau virtuelle sur **virtio**.
   Par exemple, la commande suivante crée une VM **kvmtest** à l'aide de l'image **rhel-9.0-x86_64-kvm.qcow2**:

```
# virt-install \
    --name kvmtest --memory 2048 --vcpus 2 \
    --disk rhel-9.0-x86_64-kvm.qcow2,bus=virtio \
    --import --os-variant=rhel9.0
```

   b. Si vous utilisez la console web pour créer votre machine virtuelle, suivez la procédure décrite dans la section Création de machines virtuelles à l'aide de la console web , avec les mises en garde suivantes :
      - Ne pas vérifier **Immediately Start VM**.
      - Modifiez la taille de votre site **Memory** en fonction de vos préférences.
      - Avant de commencer l'installation, assurez-vous que vous avez changé **Model** sous **Virtual Network Interface Settings** en **virtio** et changez votre **vCPUs** en fonction des paramètres de capacité que vous souhaitez pour la VM.
3. Examinez les autres choix et modifications d'installation suivants.

- Sélectionnez **Minimal Install** avec l'option **standard RHEL**.
- Pour **Installation Destination**, sélectionnez **Custom Storage Configuration**. Utilisez les informations de configuration suivantes pour effectuer vos sélections.
  - Vérifiez qu'il y a au moins 500 Mo pour **/boot**.
  - Pour le système de fichiers, utilisez xfs, ext4 ou ext3 pour les partitions **boot** et **root**.
  - Supprimer l'espace de pagination. L'espace de pagination est configuré sur le serveur lame physique dans Azure par l'agent WALinux.
- Sur l'écran **Installation Summary**, sélectionnez **Network and Host Name**. Passez de **Ethernet** à **On**.

4. Lorsque l'installation démarre :
   - Créez un mot de passe **root**.
   - Créer un compte d'utilisateur administratif.
5. Une fois l'installation terminée, redémarrez la VM et connectez-vous au compte root.
6. Une fois que vous êtes connecté en tant que **root**, vous pouvez configurer l'image.

3.3. CONFIGURATION D'UNE IMAGE DE BASE PERSONNALISÉE POUR MICROSOFT AZURE

Pour déployer une machine virtuelle (VM) RHEL 9 avec des paramètres spécifiques dans Azure, vous pouvez créer une image de base personnalisée pour la VM. Les sections suivantes décrivent les modifications de configuration supplémentaires requises par Azure.

3.3.1. Installation des pilotes de périphériques Hyper-V

Microsoft fournit des pilotes de périphériques de réseau et de stockage dans le cadre de ses services d'intégration Linux (LIS) pour Hyper-V. Il se peut que vous deviez installer les pilotes de périphériques Hyper-V sur l'image de la VM avant de l'approvisionner en tant que machine virtuelle Azure (VM). Utilisez la commande **lsinitrd | grep hv** pour vérifier que les pilotes sont installés.

Procédure

1. Entrez la commande suivante **grep** pour déterminer si les pilotes de périphériques Hyper-V requis sont installés.

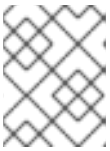
```
# lsinitrd | grep hv
```

Dans l'exemple ci-dessous, tous les pilotes nécessaires sont installés.

```
# *lsinitrd | grep hv*
drwxr-xr-x   2 root     root            0 Aug 12 14:21 usr/lib/modules/3.10.0-
932.el{ProductNumber}.x86_64/kernel/drivers/hv
-rw-r--r--   1 root     root        31272 Aug 11 08:45 usr/lib/modules/3.10.0-
932.el{ProductNumber}.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.el{ProductNumber}.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.el{ProductNumber}.x86_64/kernel/drivers/scsi/hv_storvsc.ko.xz
```

Si tous les pilotes ne sont pas installés, suivez les étapes suivantes.



NOTE

Un pilote **hv_vmbus** peut exister dans l'environnement. Même si ce pilote est présent, effectuez les étapes suivantes.

2. Créez un fichier nommé **hv.conf** dans **/etc/dracut.conf.d**.

3. Ajoutez les paramètres de pilote suivants au fichier **hv.conf**.

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

NOTE

Notez les espaces avant et après les guillemets, par exemple, **add_drivers =" hv_vmbus "**. Cela permet de s'assurer que des pilotes uniques sont chargés au cas où d'autres pilotes Hyper-V existeraient déjà dans l'environnement.

4. Régénérer l'image **initramfs**.

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

Vérification

1. Redémarrer la machine.

2. Exécutez la commande **lsinitrd | grep hv** pour vérifier que les pilotes sont installés.

3.3.2. Effectuer les changements de configuration nécessaires au déploiement de Microsoft Azure

Avant de déployer votre image de base personnalisée dans Azure, vous devez effectuer des changements de configuration supplémentaires pour vous assurer que la machine virtuelle (VM) peut fonctionner correctement dans Azure.

Procédure

1. Connectez-vous à la VM.

2. Enregistrez la VM et activez le référentiel Red Hat Enterprise Linux 9.

```
# subscription-manager register --auto-attach
Installed Product Current Status:
Product Name: Red Hat Enterprise Linux for x86_64
Status: Subscribed
```

3. Assurez-vous que les paquets **cloud-init** et **hyperv-daemons** sont installés.

```
# dnf install cloud-init hyperv-daemons -y
```

4. Créez les fichiers de configuration **cloud-init** nécessaires à l'intégration avec les services Azure :

   a. Pour activer la journalisation du service d'échange de données Hyper-V (KVP), créez le fichier de configuration **/etc/cloud/cloud.cfg.d/10-azure-kvp.cfg** et ajoutez-y les lignes suivantes.

```
reporting:
    logging:
        type: log
    telemetry:
        type: hyperv
```

   b. Pour ajouter Azure en tant que source de données, créez le fichier de configuration **/etc/cloud/cloud.cfg.d/91-azure_datasource.cfg** et ajoutez-y les lignes suivantes.

```
datasource_list: [ Azure ]
datasource:
    Azure:
        apply_network_config: False
```

5. Pour s'assurer que le chargement automatique de certains modules du noyau est bloqué, modifiez ou créez le fichier **/etc/modprobe.d/blocklist.conf** et ajoutez-y les lignes suivantes.

```
blacklist nouveau
blacklist lbm-nouveau
blacklist floppy
blacklist amdgpu
blacklist skx_edac
blacklist intel_cstate
```

6. Modifier les règles relatives aux périphériques réseau sur **udev**:

   a. Supprimez les règles suivantes relatives aux périphériques réseau persistants, si elles existent.

```
# 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
```

   b. Pour vous assurer que Accelerated Networking on Azure fonctionne comme prévu, créez une nouvelle règle de périphérique réseau **/etc/udev/rules.d/68-azure-sriov-nm-unmanaged.rules** et ajoutez-y la ligne suivante.

```
SUBSYSTEM=="net", DRIVERS=="hv_pci", ACTION=="add",
ENV{NM_UNMANAGED}="1"
```

7. Configurez le service **sshd** pour qu'il démarre automatiquement.

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

8. Modifier les paramètres de démarrage du noyau :

   a. Ouvrez le fichier **/etc/default/grub** et assurez-vous que la ligne **GRUB_TIMEOUT** contient la valeur suivante.

   ```
   GRUB_TIMEOUT=10
   ```

   b. Supprimer les options suivantes à la fin de la ligne **GRUB_CMDLINE_LINUX** si elles sont présentes.

   ```
   rhgb quiet
   ```

   c. Assurez-vous que le fichier **/etc/default/grub** contient les lignes suivantes avec toutes les options spécifiées.

   ```
   GRUB_CMDLINE_LINUX="loglevel=3 crashkernel=auto console=tty1 console=ttyS0
   earlyprintk=ttyS0 rootdelay=300"
   GRUB_TIMEOUT_STYLE=countdown
   GRUB_TERMINAL="serial console"
   GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --
   stop=1"
   ```

   d. Régénérer le fichier **grub.cfg**.
   Sur une machine basée sur le BIOS :

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

   Sur une machine basée sur l'UEFI :

   ```
   # grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
   ```

   Si votre système utilise un emplacement autre que celui par défaut pour **grub.cfg**, adaptez la commande en conséquence.

9. Configurez l'agent Windows Azure Linux (**WALinuxAgent**) :

   a. Installez et activez le paquetage **WALinuxAgent**.

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

   b. Pour s'assurer qu'une partition de swap n'est pas utilisée dans les VM provisionnées, modifiez les lignes suivantes dans le fichier **/etc/waagent.conf**.

   ```
   Provisioning.DeleteRootPassword=y
   ResourceDisk.Format=n
   ResourceDisk.EnableSwap=n
   ```

10. Préparer la VM pour le provisionnement Azure :

a. Désenregistrez la VM du Gestionnaire d'abonnements de Red Hat.

```
# subscription-manager unregister
```

b. Nettoyer les détails de l'approvisionnement existants.

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

NOTE

Cette commande génère des avertissements, ce qui est normal car Azure gère automatiquement le provisionnement des machines virtuelles.

c. Nettoyez l'historique du shell et arrêtez la VM.

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

3.4. CONVERSION DE L'IMAGE EN UN FORMAT VHD FIXE

Toutes les images Microsoft Azure VM doivent être dans un format fixe **VHD**. L'image doit être alignée sur une limite de 1 Mo avant d'être convertie en VHD. Pour convertir l'image de **qcow2** à un format fixe **VHD** et aligner l'image, voir la procédure suivante. Une fois l'image convertie, vous pouvez la télécharger vers Azure.

Procédure

1. Convertir l'image du format **qcow2** au format **raw**.

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

2. Créez un script shell en utilisant le contenu ci-dessous.

```
#!/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. Exécutez le script. Cet exemple utilise le nom **align.sh**.

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

- Si le message *"Your image is already aligned. You do not need to resize."* s'affiche, passez à l'étape suivante.

- Si une valeur s'affiche, votre image n'est pas alignée.

4. Utilisez la commande suivante pour convertir le fichier en un format fixe **VHD**.
The sample uses qemu-img version 2.12.0.

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

Une fois converti, le fichier **VHD** est prêt à être téléchargé sur Azure.

5. Si l'image **raw** n'est pas alignée, procédez comme suit pour l'aligner.

a. Redimensionnez le fichier **raw** en utilisant la valeur arrondie affichée lors de l'exécution du script de vérification.

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

b. Convertir le fichier image **raw** au format **VHD**.
The sample uses qemu-img version 2.12.0.

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

Une fois converti, le fichier **VHD** est prêt à être téléchargé sur Azure.

3.5. INSTALLATION DE L'INTERFACE DE PROGRAMMATION AZURE

Suivez les étapes suivantes pour installer l'interface de ligne de commande Azure (Azure CLI 2.1). Azure CLI 2.1 est un utilitaire basé sur Python qui permet de créer et de gérer des machines virtuelles dans Azure.

Conditions préalables

- Vous devez disposer d'un compte Microsoft Azure avant de pouvoir utiliser l'interface de programmation Azure.
- L'installation d'Azure CLI nécessite Python 3.x.

Procédure

1. Importer la clé du référentiel Microsoft.

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

2. Créez une entrée dans le référentiel local Azure CLI.

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

3. Mise à jour de l'index du paquet **dnf**.

```
$ dnf check-update
```

4. Vérifiez votre version de Python (**python --version**) et installez Python 3.x, si nécessaire.

```
$ sudo dnf install python3
```

5. Installez le CLI Azure.

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

6. Exécutez le CLI Azure.

```
$ az
```

Ressources supplémentaires

- CLI Azure
- Référence des commandes de la CLI Azure

3.6. CRÉER DES RESSOURCES DANS AZURE

Suivez la procédure suivante pour créer les ressources Azure dont vous avez besoin avant de télécharger le fichier **VHD** et de créer l'image Azure.

Procédure

1. Authentifiez votre système avec Azure et connectez-vous.

```
$ az login
```

NOTE

Si un navigateur est disponible dans votre environnement, l'interface CLI ouvre votre navigateur sur la page de connexion à Azure. Voir Sign in with Azure CLI pour plus d'informations et d'options.

2. Créer un groupe de ressources dans une région Azure.

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

Exemple :

```
[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. Créer un compte de stockage. Voir Types d'UGS pour plus d'informations sur les valeurs d'UGS valides.

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

Exemple :

```
[clouduser@localhost]$ az storage account create -l southcentralus -n azrhelclistact -g azrhelclirsgrp --sku Standard_LRS
{
  "accessTier": null,
  "creationTime": "2017-04-05T19:10:29.855470+00:00",
  "customDomain": null,
  "encryption": null,
  "id":
"/subscriptions//resourceGroups/azrhelclirsgrp/providers/Microsoft.Storage/storageAccounts/azrhelclistact",
  "kind": "StorageV2",
  "lastGeoFailoverTime": null,
  "location": "southcentralus",
  "name": "azrhelclistact",
  "primaryEndpoints": {
    "blob": "https://azrhelclistact.blob.core.windows.net/",
    "file": "https://azrhelclistact.file.core.windows.net/",
    "queue": "https://azrhelclistact.queue.core.windows.net/",
    "table": "https://azrhelclistact.table.core.windows.net/"
},
"primaryLocation": "southcentralus",
"provisioningState": "Succeeded",
"resourceGroup": "azrhelclirsgrp",
"secondaryEndpoints": null,
"secondaryLocation": null,
"sku": {
  "name": "Standard_LRS",
  "tier": "Standard"
},
"statusOfPrimary": "available",
"statusOfSecondary": null,
"tags": {},
  "type": "Microsoft.Storage/storageAccounts"
}
```

4. Obtenir la chaîne de connexion du compte de stockage.

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

Exemple :

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

5. Exportez la chaîne de connexion en la copiant et en la collant dans la commande suivante. Cette chaîne connecte votre système au compte de stockage.

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

Exemple :

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

6. Créer le conteneur de stockage.

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

Exemple :

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

7. Créer un réseau virtuel.

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

Exemple :

```
[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
  }
}
```


Ressources supplémentaires

- Vue d'ensemble des disques gérés Azure
- Types de SKU

3.7. TÉLÉCHARGEMENT ET CRÉATION D'UNE IMAGE AZURE

Effectuez les étapes suivantes pour télécharger le fichier **VHD** dans votre conteneur et créer une image personnalisée Azure.

NOTE

La chaîne de connexion de stockage exportée ne persiste pas après un redémarrage du système. Si l'une des commandes des étapes suivantes échoue, exportez à nouveau la chaîne de connexion.

Procédure

1. Téléchargez le fichier **VHD** dans le conteneur de stockage. Cela peut prendre plusieurs minutes. Pour obtenir une liste des conteneurs de stockage, entrez la commande **az storage container list**.

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

Exemple :

```
[clouduser@localhost]$ *az storage blob upload \*
*--account-name azrhelclistact --container-name azrhelclistcont \*
*--type page --file rhel-image-{ProductNumber}.vhd --name rhel-image-
{ProductNumber}.vhd*

Percent complete: %100.0
```

2. Obtenir l'URL du fichier **VHD** téléchargé pour l'utiliser dans l'étape suivante.

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

Exemple :

```
$ az storage blob url -c azrhelclistcont -n rhel-image-9.vhd
"https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-9.vhd"
```

3. Créez l'image personnalisée Azure.

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

NOTE

La génération d'hyperviseur par défaut de la VM est V1. Vous pouvez éventuellement spécifier une génération d'hyperviseur V2 en incluant l'option **--hyper-v-generation V2**. Les VM de génération 2 utilisent une architecture de démarrage basée sur l'UEFI. Voir Support for generation 2 VMs on Azure pour plus d'informations sur les VMs de génération 2.

La commande peut renvoyer l'erreur suivante : "Seuls les blobs formatés en tant que VHD peuvent être importés" Cette erreur peut signifier que l'image n'a pas été alignée à la limite de 1 Mo la plus proche avant d'être convertie en **VHD**.

Exemple :

```
$ az image create -n rhel9 -g azrhelclirsgrp2 -l southcentralus --source
https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-9.vhd --os-type linux
```

3.8. CRÉATION ET DÉMARRAGE DE LA VM DANS AZURE

Les étapes suivantes fournissent les options de commande minimales pour créer une VM Azure à disque géré à partir de l'image. Voir az vm create pour des options supplémentaires.

Procédure

1. Entrez la commande suivante pour créer la VM.

```
$ az vm create \
   -g <resource-group> -l <azure-region> -n <vm-name> \
   --vnet-name <vnet-name> --subnet <subnet-name> --size Standard_A2 \
```

```
--os-disk-name <simple-name> --admin-username <administrator-name> \
--generate-ssh-keys --image <path-to-image>
```

NOTE

L'option **--generate-ssh-keys** crée une paire de clés privée/publique. Les fichiers de clés privée et publique sont créés dans **~/.ssh** sur votre système. La clé publique est ajoutée au fichier **authorized_keys** sur la machine virtuelle pour l'utilisateur spécifié par l'option **--admin-username**. Voir Autres méthodes d'authentification pour plus d'informations.

Exemple :

```
[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 rhel9

{
  "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"
```

Notez l'adresse **publicIpAddress**. Vous avez besoin de cette adresse pour vous connecter à la VM à l'étape suivante.

2. Démarrez une session SSH et connectez-vous à la VM.

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

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

Si vous voyez une invite d'utilisateur, vous avez déployé avec succès votre VM Azure.

Vous pouvez maintenant vous rendre sur le portail Microsoft Azure et vérifier les journaux d'audit et les propriétés de vos ressources. Vous pouvez gérer vos machines virtuelles directement sur ce portail. Si vous gérez plusieurs machines virtuelles, vous devez utiliser la CLI d'Azure. Le CLI Azure fournit une interface puissante pour vos ressources dans Azure. Saisissez **az --help** dans la CLI ou consultez la référence des commandes de la CLI Azure pour en savoir plus sur les commandes que vous utilisez pour gérer vos machines virtuelles dans Microsoft Azure.

3.9. AUTRES MÉTHODES D'AUTHENTIFICATION

Bien que recommandée pour une sécurité accrue, l'utilisation de la paire de clés générée par Azure n'est pas obligatoire. Les exemples suivants présentent deux méthodes d'authentification SSH.

Example 1: Ces options de commande permettent de provisionner une nouvelle VM sans générer de fichier de clé publique. Elles permettent l'authentification SSH à l'aide d'un mot de passe.

```
$ az vm create \
   -g <resource-group> -l <azure-region> -n <vm-name> \
   --vnet-name <vnet-name> --subnet <subnet-name> --size 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: Ces options de commande permettent de provisionner une nouvelle VM Azure et d'autoriser l'authentification SSH à l'aide d'un fichier de clés publiques existant.

```
$ az vm create \
   -g <resource-group> -l <azure-region> -n <vm-name> \
   --vnet-name <vnet-name> --subnet <subnet-name> --size Standard_A2 \
   --os-disk-name <simple-name> --admin-username <administrator-name> \
   --ssh-key-value <path-to-existing-ssh-key> --image <path-to-image>
```

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

3.10. ATTACHER DES ABONNEMENTS RED HAT

Pour attacher votre abonnement Red Hat à une instance RHEL, suivez les étapes suivantes.

Conditions préalables

- Vous devez avoir activé vos abonnements.

Procédure

1. Enregistrez votre système.

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

2. Joignez vos abonnements.
   - Vous pouvez utiliser une clé d'activation pour attacher des abonnements. Pour plus d'informations, reportez-vous à la section Créer des clés d'activation pour le portail client Red Hat.
   - Vous pouvez également rattacher manuellement un abonnement à l'aide de l'ID du pool d'abonnements (Pool ID). Voir Attacher et supprimer des abonnements via la ligne de commande.

Ressources supplémentaires

- Création de clés d'activation pour le portail client de Red Hat

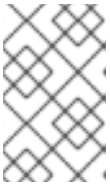
- Attacher et supprimer des abonnements via la ligne de commande
- Utilisation et configuration du Gestionnaire d'abonnements Red Hat

3.11. CONFIGURATION DE L'ENREGISTREMENT AUTOMATIQUE SUR LES IMAGES AZURE GOLD

Pour rendre le déploiement des machines virtuelles RHEL 9 sur Micorsoft Azure plus rapide et plus confortable, vous pouvez configurer les images Gold de RHEL 9 pour qu'elles soient automatiquement enregistrées dans le gestionnaire d'abonnement Red Hat (RHSM).

Conditions préalables

- Les images d'or RHEL 9 sont disponibles dans Microsoft Azure. Pour obtenir des instructions, voir Utilisation d'images Gold sur Azure .



NOTE

Un compte Microsoft Azure ne peut être rattaché qu'à un seul compte Red Hat à la fois. Par conséquent, assurez-vous qu'aucun autre utilisateur n'a besoin d'accéder au compte Azure avant de l'attacher à votre compte Red Hat.

Procédure

1. Utilisez l'image Gold pour créer une VM RHEL 9 dans votre instance Azure. Pour obtenir des instructions, voir Création et démarrage de la VM dans Azure .
2. Démarrer la VM créée.
3. Dans la VM RHEL 9, activez l'enregistrement automatique.

```
# subscription-manager config --rhsmcertd.auto_registration=1
```

4. Activer le service **rhsmcertd**.

```
# systemctl enable rhsmcertd.service
```

5. Désactiver le dépôt **redhat.repo**.

```
# subscription-manager config --rhsm.manage_repos=0
```

6. Mettez la machine virtuelle hors tension et enregistrez-la en tant qu'image gérée sur Azure. Pour plus d'informations, voir Comment créer une image gérée d'une machine virtuelle ou d'un VHD.
7. Créez des machines virtuelles à l'aide de l'image gérée. Elles seront automatiquement abonnées à RHSM.

Vérification

- Dans une VM RHEL 9 créée à l'aide des instructions ci-dessus, vérifiez que le système est enregistré dans le RHSM en exécutant la commande **subscription-manager identity**. Sur un système enregistré avec succès, cette commande affiche l'UUID du système. Par exemple :

```
# subscription-manager identity
system identity: fdc46662-c536-43fb-a18a-bbcb283102b7
name: 192.168.122.222
org name: 6340056
org ID: 6340056
```

Ressources supplémentaires

- Red Hat Gold Images dans Azure
- Aperçu des images RHEL dans Azure
- Configuration des sources cloud pour les services Red Hat

3.12. RESSOURCES SUPPLÉMENTAIRES

- Red Hat dans le nuage public
- Guide de référence de Red Hat Cloud Access
- Foire aux questions et pratiques recommandées pour Microsoft Azure

CHAPITRE 4. CONFIGURER UN CLUSTER RED HAT HIGH AVAILABILITY SUR MICROSOFT AZURE

Pour configurer un cluster Red Hat High Availability (HA) sur Azure en utilisant des instances de machines virtuelles (VM) Azure comme nœuds de cluster, consultez les sections suivantes. Les procédures de ces sections supposent que vous créez une image personnalisée pour Azure. Vous disposez d'un certain nombre d'options pour obtenir les images RHEL 9 que vous utilisez pour votre cluster. Voir Options d'image Red Hat Enterprise Linux sur Azure pour obtenir des informations sur les options d'image pour Azure.

Les sections suivantes fournissent des informations :

- Procédures préalables à la configuration de votre environnement pour Azure. Après avoir configuré votre environnement, vous pouvez créer et configurer des instances de VM Azure.
- Procédures spécifiques à la création de clusters HA, qui transforment des nœuds individuels en un cluster de nœuds HA sur Azure. Il s'agit notamment des procédures d'installation des packages et des agents de haute disponibilité sur chaque nœud de cluster, de la configuration de la clôture et de l'installation des agents de ressources réseau Azure.

Conditions préalables

- Créez un compte sur le portail client de Red Hat .
- Ouvrez un compte Microsoft Azure avec des privilèges d'administrateur.
- Vous devez installer l'interface de ligne de commande Azure (CLI). Pour plus d'informations, voir Installation de l'interface de ligne de commande Az ure.

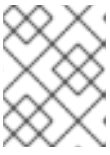
4.1. CRÉER DES RESSOURCES DANS AZURE

Suivez la procédure suivante pour créer une région, un groupe de ressources, un compte de stockage, un réseau virtuel et un ensemble de disponibilité. Vous avez besoin de ces ressources pour configurer un cluster sur Microsoft Azure.

Procédure

1. Authentifiez votre système avec Azure et connectez-vous.

```
$ az login
```



NOTE

Si un navigateur est disponible dans votre environnement, l'interface de programmation ouvre votre navigateur sur la page de connexion Azure.

Exemple :

```
[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. Créer un groupe de ressources dans une région Azure.

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

Exemple :

```
[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. Créer un compte de stockage.

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

Exemple :

```
[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. Obtenir la chaîne de connexion du compte de stockage.

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

Exemple :

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

5. Exportez la chaîne de connexion en la copiant et en la collant dans la commande suivante. Cette chaîne connecte votre système au compte de stockage.

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

Exemple :

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

6. Créer le conteneur de stockage.

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

Exemple :

```
[clouduser@localhost]$ az storage container create -n azrhelclistcont
```

```
{
  "created": true
}
```

7. Créez un réseau virtuel. Tous les nœuds du cluster doivent se trouver dans le même réseau virtuel.

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

Exemple :

```
[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. Créez un ensemble de disponibilité. Tous les nœuds du cluster doivent se trouver dans le même ensemble de disponibilité.

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

Exemple :

```
[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]
```

Ressources supplémentaires

- Se connecter avec Azure CLI
- Types de SKU
- Vue d'ensemble des disques gérés Azure

4.2. PAQUETS SYSTÈME REQUIS POUR LA HAUTE DISPONIBILITÉ

La procédure suppose que vous créez une image VM pour Azure HA à l'aide de Red Hat Enterprise Linux. Pour mener à bien la procédure, les paquets suivants doivent être installés.

Tableau 4.1. Paquets de systèmes

Paquet	Référentiel	Description
libvirt	rhel-9-for-x86_64-appstream-rpms	API, démon et outil de gestion open source pour la gestion de la virtualisation des plateformes
virt-install	rhel-9-for-x86_64-appstream-rpms	Un utilitaire en ligne de commande pour construire des VM
libguestfs	rhel-9-for-x86_64-appstream-rpms	Une bibliothèque pour l'accès et la modification des systèmes de fichiers VM

Paquet	Référentiel	Description
guestfs-tools	rhel-9-for-x86_64-appstream-rpms	Outils d'administration du système pour les machines virtuelles ; comprend l'utilitaire **virt-customize**

4.3. PARAMÈTRES DE CONFIGURATION DE LA VM AZURE

Les VM Azure doivent disposer des paramètres de configuration suivants. Certains de ces paramètres sont activés lors de la création initiale de la VM. D'autres paramètres sont définis lors du provisionnement de l'image de la VM pour Azure. Gardez ces paramètres à l'esprit tout au long des procédures. Reportez-vous-y si nécessaire.

Tableau 4.2. Paramètres de configuration de la VM

Paramètres	Recommandation
ssh	ssh doit être activé pour permettre l'accès à distance à vos machines virtuelles Azure.
dhcp	L'adaptateur virtuel principal doit être configuré pour dhcp (IPv4 uniquement).
Espace d'échange	Ne créez pas de fichier ou de partition d'échange dédié. Vous pouvez configurer l'espace d'échange avec l'agent Windows Azure Linux (WALinuxAgent).
NIC	Choisissez **virtio** pour la carte réseau virtuelle principale.
chiffrement	Pour les images personnalisées, utilisez Network Bound Disk Encryption (NBDE) pour un chiffrement complet du disque sur Azure.

4.4. INSTALLATION DES PILOTES DE PÉRIPHÉRIQUES HYPER-V

Microsoft fournit des pilotes de périphériques de réseau et de stockage dans le cadre de ses services d'intégration Linux (LIS) pour Hyper-V. Il se peut que vous deviez installer les pilotes de périphériques Hyper-V sur l'image de la VM avant de l'approvisionner en tant que machine virtuelle Azure (VM). Utilisez la commande **lsinitrd | grep hv** pour vérifier que les pilotes sont installés.

Procédure

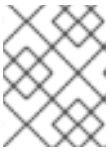
1. Entrez la commande suivante **grep** pour déterminer si les pilotes de périphériques Hyper-V requis sont installés.

```
# lsinitrd | grep hv
```

Dans l'exemple ci-dessous, tous les pilotes nécessaires sont installés.

```
# *lsinitrd | grep hv*
drwxr-xr-x   2 root     root            0 Aug 12 14:21 usr/lib/modules/3.10.0-
932.el{ProductNumber}.x86_64/kernel/drivers/hv
-rw-r--r--   1 root     root        31272 Aug 11 08:45 usr/lib/modules/3.10.0-
932.el{ProductNumber}.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.el{ProductNumber}.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.el{ProductNumber}.x86_64/kernel/drivers/scsi/hv_storvsc.ko.xz
```

Si tous les pilotes ne sont pas installés, suivez les étapes suivantes.



NOTE

Un pilote **hv_vmbus** peut exister dans l'environnement. Même si ce pilote est présent, effectuez les étapes suivantes.

2. Créez un fichier nommé **hv.conf** dans **/etc/dracut.conf.d**.

3. Ajoutez les paramètres de pilote suivants au fichier **hv.conf**.

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

NOTE

Notez les espaces avant et après les guillemets, par exemple, **add_drivers =" hv_vmbus "**. Cela permet de s'assurer que des pilotes uniques sont chargés au cas où d'autres pilotes Hyper-V existeraient déjà dans l'environnement.

4. Régénérer l'image **initramfs**.

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

Vérification

1. Redémarrer la machine.

2. Exécutez la commande **lsinitrd | grep hv** pour vérifier que les pilotes sont installés.

4.5. EFFECTUER LES CHANGEMENTS DE CONFIGURATION NÉCESSAIRES AU DÉPLOIEMENT DE MICROSOFT AZURE

Avant de déployer votre image de base personnalisée dans Azure, vous devez effectuer des changements de configuration supplémentaires pour vous assurer que la machine virtuelle (VM) peut fonctionner correctement dans Azure.

Procédure

1. Connectez-vous à la VM.
2. Enregistrez la VM et activez le référentiel Red Hat Enterprise Linux 9.

```
# subscription-manager register --auto-attach
Installed Product Current Status:
Product Name: Red Hat Enterprise Linux for x86_64
Status: Subscribed
```

3. Assurez-vous que les paquets **cloud-init** et **hyperv-daemons** sont installés.

```
# dnf install cloud-init hyperv-daemons -y
```

4. Créez les fichiers de configuration **cloud-init** nécessaires à l'intégration avec les services Azure :
   a. Pour activer la journalisation du service d'échange de données Hyper-V (KVP), créez le fichier de configuration **/etc/cloud/cloud.cfg.d/10-azure-kvp.cfg** et ajoutez-y les lignes suivantes.

```
reporting:
    logging:
        type: log
    telemetry:
        type: hyperv
```

   b. Pour ajouter Azure en tant que source de données, créez le fichier de configuration **/etc/cloud/cloud.cfg.d/91-azure_datasource.cfg** et ajoutez-y les lignes suivantes.

```
datasource_list: [ Azure ]
datasource:
    Azure:
        apply_network_config: False
```

5. Pour s'assurer que le chargement automatique de certains modules du noyau est bloqué, modifiez ou créez le fichier **/etc/modprobe.d/blocklist.conf** et ajoutez-y les lignes suivantes.

```
blacklist nouveau
blacklist lbm-nouveau
blacklist floppy
blacklist amdgpu
blacklist skx_edac
blacklist intel_cstate
```

6. Modifier les règles relatives aux périphériques réseau sur **udev**:
   a. Supprimez les règles suivantes relatives aux périphériques réseau persistants, si elles existent.

```
# 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
```

   b. Pour vous assurer que Accelerated Networking on Azure fonctionne comme prévu, créez

b. Pour vous assurer que Accelerated Networking on Azure fonctionne comme prévu, créez une nouvelle règle de périphérique réseau **/etc/udev/rules.d/68-azure-sriov-nm-unmanaged.rules** et ajoutez-y la ligne suivante.

```
SUBSYSTEM=="net", DRIVERS=="hv_pci", ACTION=="add",
ENV{NM_UNMANAGED}="1"
```

7. Configurez le service **sshd** pour qu'il démarre automatiquement.

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

8. Modifier les paramètres de démarrage du noyau :

a. Ouvrez le fichier **/etc/default/grub** et assurez-vous que la ligne **GRUB_TIMEOUT** contient la valeur suivante.

```
GRUB_TIMEOUT=10
```

b. Supprimer les options suivantes à la fin de la ligne **GRUB_CMDLINE_LINUX** si elles sont présentes.

```
rhgb quiet
```

c. Assurez-vous que le fichier **/etc/default/grub** contient les lignes suivantes avec toutes les options spécifiées.

```
GRUB_CMDLINE_LINUX="loglevel=3 crashkernel=auto console=tty1 console=ttyS0
earlyprintk=ttyS0 rootdelay=300"
GRUB_TIMEOUT_STYLE=countdown
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --
stop=1"
```

d. Régénérer le fichier **grub.cfg**.
Sur une machine basée sur le BIOS :

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

Sur une machine basée sur l'UEFI :

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

Si votre système utilise un emplacement autre que celui par défaut pour **grub.cfg**, adaptez la commande en conséquence.

9. Configurez l'agent Windows Azure Linux (**WALinuxAgent**) :

a. Installez et activez le paquetage **WALinuxAgent**.

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

b. Pour s'assurer qu'une partition de swap n'est pas utilisée dans les VM provisionnées, modifiez les lignes suivantes dans le fichier **/etc/waagent.conf**.

```
Provisioning.DeleteRootPassword=y
ResourceDisk.Format=n
ResourceDisk.EnableSwap=n
```

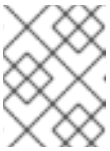
10. Préparer la VM pour le provisionnement Azure :

a. Désenregistrez la VM du Gestionnaire d'abonnements de Red Hat.

```
# subscription-manager unregister
```

b. Nettoyer les détails de l'approvisionnement existants.

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



NOTE

Cette commande génère des avertissements, ce qui est normal car Azure gère automatiquement le provisionnement des machines virtuelles.

c. Nettoyez l'historique du shell et arrêtez la VM.

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

4.6. CRÉATION D'UNE APPLICATION AZURE ACTIVE DIRECTORY

Suivez la procédure suivante pour créer une application AD Azure Active Directory. L'application Azure AD autorise et automatise l'accès aux opérations HA pour tous les nœuds du cluster.

Conditions préalables

Installez l'interface de ligne de commande Azure (CLI) .

Procédure

1. Assurez-vous que vous êtes administrateur ou propriétaire de l'abonnement Microsoft Azure. Vous avez besoin de cette autorisation pour créer une application Azure AD.

2. Connectez-vous à votre compte Azure.

```
$ az login
```

3. Entrez la commande suivante pour créer l'application Azure AD. Pour utiliser votre propre mot de passe, ajoutez l'option **--password** à la commande. Veillez à créer un mot de passe fort.

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

Exemple :

```
[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. Enregistrez les informations suivantes avant de continuer. Vous avez besoin de ces informations pour configurer l'agent de clôture.
   - ID de l'application Azure AD
   - Mot de passe de l'application Azure AD
   - ID du locataire
   - ID d'abonnement à Microsoft Azure

Ressources supplémentaires

- Afficher l'accès d'un utilisateur aux ressources Azure

4.7. CONVERSION DE L'IMAGE EN UN FORMAT VHD FIXE

Toutes les images Microsoft Azure VM doivent être dans un format fixe **VHD**. L'image doit être alignée sur une limite de 1 Mo avant d'être convertie en VHD. Pour convertir l'image de **qcow2** à un format fixe **VHD** et aligner l'image, voir la procédure suivante. Une fois l'image convertie, vous pouvez la télécharger vers Azure.

Procédure

1. Convertir l'image du format **qcow2** au format **raw**.

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

2. Créez un script shell en utilisant le contenu ci-dessous.

```
#!/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. Exécutez le script. Cet exemple utilise le nom **align.sh**.

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

   - Si le message *"Your image is already aligned. You do not need to resize."* s'affiche, passez à l'étape suivante.
   - Si une valeur s'affiche, votre image n'est pas alignée.

4. Utilisez la commande suivante pour convertir le fichier en un format fixe **VHD**.
   The sample uses qemu-img version 2.12.0.

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

   Une fois converti, le fichier **VHD** est prêt à être téléchargé sur Azure.

5. Si l'image **raw** n'est pas alignée, procédez comme suit pour l'aligner.

   a. Redimensionnez le fichier **raw** en utilisant la valeur arrondie affichée lors de l'exécution du script de vérification.

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

   b. Convertir le fichier image **raw** au format **VHD**.
   The sample uses qemu-img version 2.12.0.

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

   Une fois converti, le fichier **VHD** est prêt à être téléchargé sur Azure.

4.8. TÉLÉCHARGEMENT ET CRÉATION D'UNE IMAGE AZURE

Effectuez les étapes suivantes pour télécharger le fichier **VHD** dans votre conteneur et créer une image personnalisée Azure.

NOTE

La chaîne de connexion de stockage exportée ne persiste pas après un redémarrage du système. Si l'une des commandes des étapes suivantes échoue, exportez à nouveau la chaîne de connexion.

Procédure

1. Téléchargez le fichier **VHD** dans le conteneur de stockage. Cela peut prendre plusieurs minutes. Pour obtenir une liste des conteneurs de stockage, entrez la commande **az storage container list**.

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

Exemple :

```
[clouduser@localhost]$ *az storage blob upload \*
*--account-name azrhelclistact --container-name azrhelclistcont \*
*--type page --file rhel-image-{ProductNumber}.vhd --name rhel-image-
{ProductNumber}.vhd*

Percent complete: %100.0
```

2. Obtenir l'URL du fichier **VHD** téléchargé pour l'utiliser dans l'étape suivante.

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

Exemple :

```
$ az storage blob url -c azrhelclistcont -n rhel-image-9.vhd
"https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-9.vhd"
```

3. Créez l'image personnalisée Azure.

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

NOTE

La génération d'hyperviseur par défaut de la VM est V1. Vous pouvez éventuellement spécifier une génération d'hyperviseur V2 en incluant l'option **--hyper-v-generation V2**. Les VM de génération 2 utilisent une architecture de démarrage basée sur l'UEFI. Voir Support for generation 2 VMs on Azure pour plus d'informations sur les VMs de génération 2.

La commande peut renvoyer l'erreur suivante : "Seuls les blobs formatés en tant que VHD peuvent être importés" Cette erreur peut signifier que l'image n'a pas été alignée à la limite de 1 Mo la plus proche avant d'être convertie en **VHD**.

Exemple :

```
$ az image create -n rhel9 -g azrhelclirsgrp2 -l southcentralus --source
https://azrhelclistact.blob.core.windows.net/azrhelclistcont/rhel-image-9.vhd --os-type linux
```

4.9. INSTALLATION DES PAQUETS ET DES AGENTS RED HAT HA

Effectuez les étapes suivantes sur tous les nœuds.

Procédure

1. Lancez une session SSH et connectez-vous à la VM en utilisant le nom de l'administrateur et l'adresse IP publique.

```
$ ssh administrator@PublicIP
```

Pour obtenir l'adresse IP publique d'une VM Azure, ouvrez les propriétés de la VM dans le portail Azure ou entrez la commande CLI Azure suivante.

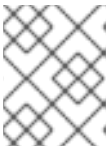
```
$ az vm list -g <resource-group> -d --output table
```

Exemple :

```
[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. Enregistrez la VM auprès de Red Hat.

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



NOTE

Si la commande **--auto-attach** échoue, enregistrez manuellement la VM dans votre abonnement.

3. Désactiver tous les dépôts.

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

4. Activer les référentiels RHEL 9 Server HA.

```
# subscription-manager repos --enable=rhel-9-for-x86_64-highavailability-rpms
```

5. Mettre à jour tous les paquets.

```
# dnf update -y
```

6. Installez les paquets logiciels Red Hat High Availability Add-On, ainsi que tous les agents de clôture disponibles dans le canal High Availability.

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

7. L'utilisateur **hacluster** a été créé lors de l'installation de pcs et pacemaker à l'étape précédente. Créez un mot de passe pour **hacluster** sur tous les nœuds du cluster. Utilisez le même mot de passe pour tous les nœuds.

```
# passwd hacluster
```

8. Ajouter le service **high availability** au pare-feu RHEL si **firewalld.service** est installé.

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

9. Démarrer le service **pcs** et l'autoriser à démarrer au démarrage.

```
# 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.
```

Vérification

- Assurez-vous que le service **pcs** est en cours d'exécution.

```
# 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 &
```

4.10. CRÉATION D'UN CLUSTER

Effectuez les étapes suivantes pour créer la grappe de nœuds.

Procédure

1. Sur l'un des nœuds, entrez la commande suivante pour authentifier l'utilisateur pcs **hacluster**. Dans la commande, indiquez le nom de chaque nœud de la grappe.

```
# pcs host auth <hostname1> <hostname2> <hostname3>
```

Exemple :

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

2. Create the cluster.

```
# pcs cluster setup <cluster_name> <hostname1> <hostname2> <hostname3>
```

Exemple :

```
[root@node01 clouduser]# pcs cluster setup new_cluster node01 node02 node03

[...]

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
```

Vérification

1. Activer le cluster.

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

2. Démarrer le cluster.

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

4.11. APERÇU DES CLÔTURES

Si la communication avec un seul nœud de la grappe échoue, les autres nœuds de la grappe doivent être en mesure de restreindre ou de libérer l'accès aux ressources auxquelles le nœud défaillant peut avoir accès. Il n'est pas possible de le faire en contactant le nœud de la grappe lui-même, car il risque de ne pas être réactif. Au lieu de cela, vous devez fournir une méthode externe, appelée clôture avec un agent de clôture.

Un nœud qui ne répond pas peut encore accéder à des données. La seule façon d'être certain que vos données sont en sécurité est de clôturer le nœud à l'aide de STONITH. STONITH est l'acronyme de " Shoot The Other Node In The Head " (Tirez sur l'autre nœud dans la tête) et protège vos données contre la corruption par des nœuds malveillants ou des accès simultanés. Grâce à STONITH, vous pouvez vous assurer qu'un nœud est réellement hors ligne avant d'autoriser l'accès aux données à partir d'un autre nœud.

Ressources supplémentaires

- Clôture dans Red Hat High Availability Cluster

4.12. CRÉATION D'UN DISPOSITIF DE CLÔTURE

Effectuez les étapes suivantes pour configurer la clôture. Exécutez ces commandes à partir de n'importe quel nœud du cluster

Conditions préalables

Vous devez définir la propriété du cluster **stonith-enabled** sur **true**.

Procédure

1. Identifiez le nom du nœud Azure pour chaque VM RHEL. Vous utilisez les noms de nœuds Azure pour configurer le dispositif de clôture.

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

Exemple :

```
[root@node01 clouduser]# fence_azure_arm \
-l e04a6a49-9f00-xxxx-xxxx-a8bdda4af447 -p
z/a05AwCN0IzAjVwXXXXXXXEWIoeVp0xg7QT//JE=
--resourceGroup azrhelclirsgrp --tenantId 77ecefb6-cff0-XXXX-XXXX-757XXXX9485
--subscriptionId XXXXXXXX-38b4-4527-XXXX-012d49dfc02c -o list

node01,
node02,
node03,
```

2. Voir les options de l'agent Azure ARM STONITH.

```
# pcs stonith describe fence_azure_arm
```

Exemple :

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

AVERTISSEMENT

Pour les agents de clôture qui fournissent une option de méthode, ne spécifiez pas une valeur de cycle car elle n'est pas prise en charge et peut entraîner une corruption des données.

Certains dispositifs de clôture ne peuvent clôturer qu'un seul nœud, tandis que d'autres peuvent clôturer plusieurs nœuds. Les paramètres que vous spécifiez lorsque vous créez un dispositif de clôture dépendent de ce que votre dispositif de clôture prend en charge et exige.

Vous pouvez utiliser le paramètre **pcmk_host_list** lors de la création d'un dispositif de clôture pour spécifier toutes les machines qui sont contrôlées par ce dispositif de clôture.

Vous pouvez utiliser le paramètre **pcmk_host_map** lors de la création d'un dispositif de clôture pour faire correspondre les noms d'hôtes aux spécifications qui comprennent le dispositif de clôture.

3. Créer un dispositif de clôture.

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

Vérification

1. Testez l'agent de clôture pour l'un des autres nœuds.

```
# pcs stonith fence azurenodename
```

Exemple :

```
[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
```

2. Démarrez le nœud qui a été clôturé à l'étape précédente.

```
# pcs cluster start <hostname>
```

3. Vérifier l'état pour s'assurer que le nœud a démarré.

```
# pcs status
```

Exemple :

```
[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
```

Ressources supplémentaires

- Clôture dans un cluster Red Hat High Availability
- Propriétés générales des dispositifs de clôture

4.13. CRÉATION D'UN ÉQUILIBREUR DE CHARGE INTERNE AZURE

L'équilibreur de charge interne Azure supprime les nœuds de cluster qui ne répondent pas aux demandes d'analyse de l'état de santé.

Suivez la procédure suivante pour créer un équilibreur de charge interne Azure. Chaque étape fait référence à une procédure Microsoft spécifique et inclut les paramètres de personnalisation de l'équilibreur de charge pour HA.

Conditions préalables

Panneau de contrôle Azure

Procédure

1. Créez un équilibreur de charge de base . Sélectionnez **Internal load balancer**, **Basic SKU** et **Dynamic** pour le type d'attribution d'adresse IP.
2. Créer un pool d'adresses back-end . Associez le pool d'adresses dorsal à l'ensemble de disponibilité créé lors de la création des ressources Azure en HA. Ne définissez aucune configuration IP du réseau cible.
3. Créez une sonde de santé . Pour la sonde de santé, sélectionnez **TCP** et entrez le port **61000**. Vous pouvez utiliser un numéro de port TCP qui n'interfère pas avec un autre service. Pour certaines applications de produits HA (par exemple, SAP HANA et SQL Server), vous devrez peut-être travailler avec Microsoft pour identifier le port correct à utiliser.
4. Créez une règle d'équilibrage de charge . Pour créer la règle d'équilibrage de charge, les valeurs par défaut sont pré-remplies. Veillez à ce que **Floating IP (direct server return)** soit remplacé par **Enabled**.

4.14. CONFIGURATION DE L'AGENT DE RESSOURCES DE L'ÉQUILIBREUR DE CHARGE

Après avoir créé la sonde de santé, vous devez configurer l'agent de ressources **load balancer**. Cet agent de ressource exécute un service qui répond aux demandes de sonde de santé de l'équilibreur de charge Azure et supprime les nœuds de cluster qui ne répondent pas aux demandes.

Procédure

1. Installez les agents de ressources **nmap-ncat** sur tous les nœuds.

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

Effectuez les étapes suivantes sur un seul nœud.

1. Créez les ressources et le groupe **pcs**. Utilisez l'adresse FrontendIP de votre équilibreur de charge pour l'adresse IPaddr2.

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

2. Configurer l'agent de ressources **load balancer**.

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

Vérification

- Lancez **pcs status** pour voir les résultats.

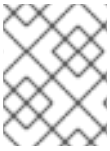
```
[root@node01 clouduser]# pcs status
```

Exemple de sortie :

```
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
```

4.15. CONFIGURATION DU STOCKAGE EN BLOC PARTAGÉ

Pour configurer le stockage en bloc partagé pour un cluster Red Hat High Availability avec Microsoft Azure Shared Disks, utilisez la procédure suivante. Notez que cette procédure est facultative et que les étapes ci-dessous supposent trois VM Azure (un cluster à trois nœuds) avec un disque partagé de 1 To.



NOTE

Il s'agit d'un exemple de procédure autonome pour la configuration du stockage par blocs. Elle suppose que vous n'avez pas encore créé votre cluster.

Conditions préalables

- Vous devez avoir installé Azure CLI sur votre système hôte et créé vos clés SSH.
- Vous devez avoir créé votre environnement de cluster dans Azure, ce qui inclut la création des ressources suivantes. Les liens renvoient à la documentation de Microsoft Azure.
  - Groupe de ressources
  - Réseau virtuel
  - Groupe(s) de sécurité du réseau
  - Règles du groupe de sécurité du réseau
  - Sous-réseau(x)
  - Équilibreur de charge (facultatif)
  - Compte de stockage
  - Groupe de placement de proximité
  - Disponibilité

Procédure

1. Créer un volume de blocs partagé à l'aide de la commande 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>
```

Par exemple, la commande suivante crée un volume de blocs partagés nommé **shared-block-volume.vhd** dans le groupe de ressources **sharedblock** au sein de la zone de disponibilité 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. Vérifiez que vous avez créé le volume de blocs partagés à l'aide de la commande Azure **az disk show**.

```
$ az disk show -g <resource_group> -n <shared_block_volume_name>
```

Par exemple, la commande suivante affiche les détails du volume de blocs partagés **shared-block-volume.vhd** dans le groupe de ressources **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. Créer trois interfaces réseau à l'aide de la commande Azure **az network nic create**. Exécutez la commande suivante trois fois en utilisant une adresse **<nic_name>** différente pour chacune d'entre elles.

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

Par exemple, la commande suivante crée une interface réseau portant le nom **shareblock-nodea-vm-nic-protected**.

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

4. Créez trois machines virtuelles et attachez le volume de blocs partagé à l'aide de la commande Azure **az vm create**. Les valeurs des options sont les mêmes pour chaque VM, sauf que chaque VM a ses propres **<vm_name>**, **<new_vm_disk_name>**, et **<nic_name>**.

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

Par exemple, la commande suivante crée une VM nommée **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-9.3.0-20200713.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": ""
}
```

Vérification

1. Pour chaque VM de votre cluster, vérifiez que le périphérique de bloc est disponible en utilisant la commande **ssh** avec l'adresse IP de votre VM.

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

Par exemple, la commande suivante répertorie les détails, y compris le nom d'hôte et le périphérique de bloc pour la VM IP **198.51.100.3**.

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

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

2. Utilisez la commande **ssh** pour vérifier que chaque VM de votre cluster utilise le même disque partagé.

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

Par exemple, la commande suivante répertorie les détails, y compris le nom d'hôte et l'ID du volume de disque partagé pour l'adresse IP de l'instance **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
```

Après avoir vérifié que le disque partagé est attaché à chaque VM, vous pouvez configurer le stockage résilient pour le cluster.

Ressources supplémentaires

- Configuration d'un système de fichiers GFS2 dans un cluster
- Configuration des systèmes de fichiers GFS2

4.16. RESSOURCES SUPPLÉMENTAIRES

- Politiques de support pour les grappes de haute disponibilité RHEL - Machines virtuelles Microsoft Azure en tant que membres de la grappe
- Configuration et gestion des clusters de haute disponibilité