

Déployer un espace de stockage des enregistrements ExtraHop dans Azure

Publié: 2023-10-24

Les procédures suivantes expliquent comment déployer un espace de stockage des enregistrements dans un environnement Microsoft Azure et comment joindre plusieurs magasins d'enregistrements pour créer un cluster. Vous devez avoir de l'expérience en administration dans un environnement Azure pour effectuer ces procédures.

Avant de commencer

- Vous devez avoir de l'expérience dans le déploiement de machines virtuelles dans Azure au sein de votre infrastructure de réseau virtuel. Pour garantir le succès du déploiement, assurez-vous que vous avez accès aux ressources requises ou que vous êtes en mesure de les créer. Vous devrez peut-être travailler avec d'autres experts de votre organisation pour vous assurer que les ressources nécessaires sont disponibles.
- Vous devez disposer d'un client Linux, Mac ou Windows doté de la dernière version de [Azure CLI](#) installé.
- Vous devez disposer du fichier du disque dur virtuel (VHD) ExtraHop, disponible sur [Portail client ExtraHop](#). Extrayez le fichier VHD du fichier d'archive .zip téléchargé.
- Vous devez disposer d'une clé de produit ExtraHop.

Exigences du système

Le tableau ci-dessous indique les paramètres environnementaux que vous devez configurer ou que vous avez peut-être déjà configurés dans votre environnement Azure pour déployer avec succès votre espace de stockage des enregistrements virtuel ExtraHop.

Paramètre	Descriptif
compte Azure	Permet d'accéder à vos abonnements Azure.
Groupe de ressources	Un conteneur qui contient les ressources associées pour l'espace de stockage des enregistrements ExtraHop.
Emplacement	La région géographique dans laquelle se trouvent les ressources Azure nécessaires à la gestion de vos magasins de disques virtuels.
Compte de stockage	Le compte de stockage Azure contient tous vos objets de données Azure Storage, y compris les blobs et les disques.
Conteneur de stockage Blob	Le conteneur de stockage dans lequel l'image de l'espace de stockage des enregistrements ExtraHop est stockée sous forme de blob.
Disque géré	Le disque requis pour le stockage des données de l'espace de stockage des enregistrements ExtraHop.
Groupe de sécurité réseau	Le groupe de sécurité réseau contient des règles de sécurité qui autorisent ou interdisent le trafic réseau entrant ou sortant depuis l'espace de stockage des enregistrements ExtraHop.

Paramètre	Descriptif
Taille de l'instance de machine virtuelle Azure	Une taille d'instance Azure qui correspond le mieux à la taille de la machine virtuelle de l'espace de stockage des enregistrements Explore. Consultez le tableau ci-dessous.
adresse IP publique ou privée	L'adresse IP qui permet d'accéder au système ExtraHop.

Tableau 1: Tailles des banques de données et des instances Azure

processeurs virtuels	Mémoire	Disque de banque de données	Taille de l'instance Azure
4	8 GO DE RAM	150 Go à 250 Go	Standard_F4S_V2
8	16 GO DE RAM	150 Go à 500 Go	Standard_F8S_V2
16	32 GO DE RAM	150 Go à 1 To	Standard_F16S_V2
32	64 GO DE RAM	150 Go à 2 To	Standard_F32S_V2

Déployez l'EXA 5100v

Avant de commencer

Les procédures ci-dessous supposent que le groupe de ressources, le compte de stockage, le conteneur de stockage et le groupe de sécurité réseau requis ne sont pas configurés. Si ces paramètres sont déjà configurés, vous pouvez passer à l'étape 5 après vous être connecté à votre compte Azure.

1. Ouvrez une application de terminal sur votre client et connectez-vous à votre compte Azure.

```
az login
```

2. Ouvrez <https://aka.ms/devicelogin> dans un navigateur Web et entrez le code d'authentification, puis revenez à l'interface de ligne de commande.
3. Créez un groupe de ressources.

```
az group create --name <name> --location <location>
```

Par exemple, créez un nouveau groupe de ressources dans la région de l'ouest des États-Unis.

```
az group create --name exampleRG --location westus
```

4. Créez un compte de stockage.

```
az storage account create --resource-group <resource group name> --name <storage account name>
```

Par exemple :

```
az storage account create --resource-group exampleRG --name examplesa
```

5. Affichez la clé du compte de stockage. La valeur de `key1` est obligatoire pour l'étape 6.

```
az storage account keys list --resource-group <resource group name> --account-name <storage account name>
```

Par exemple :

```
az storage account keys list --resource-group exampleRG --account-name
examplesa
```

Un résultat similaire à ce qui suit s'affiche :

```
[
  {
    "keyName": "key1",
    "permissions": "Full",
    "value":
      "CORuU8mTcxLxq0bbszhZ4RKTb93CqLpjZdAhCrNJugAorAyvJjhGmBSedjYPmnzXPikSRigd
      5T5/YGYBoIzxNg=="
  },
  {
    "keyName": "key2",
    "permissions": "Full",
    "value": "D0lda4+6U3Cf5TUAng8/GKotfX1HHJuc3yljAlU+aktRAF4/
      KwVQUuAUhndrw2yg5Pba5FpZn6oZYvROncnT8Q=="
  }
]
```

- Définissez les variables d'environnement du compte de stockage Azure par défaut. Vous pouvez avoir plusieurs comptes de stockage dans votre abonnement Azure. Pour sélectionner l'une d'entre elles à appliquer à toutes les commandes de stockage suivantes, définissez ces variables d'environnement. Si vous ne définissez pas de variables d'environnement, vous devrez toujours spécifier `--account-name` et `--account-key` dans les commandes du reste de cette procédure.

PowerShell

```
$Env:AZURE_STORAGE_ACCOUNT = <storage account name>
```

```
$Env:AZURE_STORAGE_KEY = <key1>
```

Où `<key1>` est la valeur de clé du compte de stockage qui apparaît à l'étape 5.

Par exemple :

```
$Env:AZURE_STORAGE_ACCOUNT=examplesa
```

```
$Env:AZURE_STORAGE_KEY=CORuU8mTcxLxq0bbszhZ4RKTb93CqLpjZdAhCrNJugAor
AyvJjhGmBSedjYPmnzXPikSRigd5T5/YGYBoIzxNg==
```



Conseil: Définissez les variables d'environnement dans l'interpréteur de commandes Windows (cmd.exe) avec la syntaxe suivante :

```
set <variable name>=<string>
```

- Définissez les variables d'environnement dans l'interface de ligne de commande Linux avec la syntaxe suivante :

```
export <variable name>=<string>
```

- Créez un conteneur de stockage.

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

Par exemple :

```
az storage container create --name examplesc
```

8. Téléchargez le fichier VHD ExtraHop sur le stockage blob.

```
az storage blob upload --container-name <container> --type page --name
<blob name> --file <path/to/file> --validate-content
```

Par exemple :

```
az storage blob upload --container-name examplesc --type page
--name extrahop.vhd --file /Users/admin/Downloads/extrahop-exa-5100v-
azure-7.2.0.5000.vhd --validate-content
```

9. Récupérez l'URI du blob. Vous aurez besoin de l'URI lorsque vous créerez le disque géré à l'étape suivante.

```
az storage blob url --container-name <storage container name> --name
<blob name>
```

Par exemple :

```
az storage blob url --container-name examplesc --name extrahop.vhd
```

Un résultat similaire à ce qui suit s'affiche :

```
https://examplesa.blob.core.windows.net/examplesc/extrahop.vhd
```

10. Créez un disque géré, en vous procurant le fichier VHD ExtraHop.

```
az disk create --resource-group <resource group name> --location <Azure
region>
--name <disk name> --sku <storage SKU> --source <blob uri> --size-gb
<size gb>
```

Où `storage SKU` indique le type de disque et le modèle de réplication souhaité. Par exemple, `Premium_LRS`, `StandardSSD_LRS`, ou `Standard_LRS`.

Par exemple :

```
az disk create --resource-group exampleRG --location westus
--name exampleDisk --sku Premium_LRS --source https://
examplesa.blob.core.windows.net/examplesc/extrahop.vhd
--size-gb 200
```

11. Créez la machine virtuelle et connectez le disque géré. Cette commande crée l'espace de stockage des enregistrements avec un groupe de sécurité réseau par défaut et une adresse IP privée.

```
az vm create --resource-group <resource group name> --public-ip-address
" "
--location <Azure region> --name <vm name> --os-type linux --attach-os-
disk <disk name>
--size <azure machine size>
```

Par exemple :

```
az vm create --resource-group exampleRG --public-ip-address " " --location
westus --name exampleVM --os-type linux
--attach-os-disk exampleDisk --size Standard_F4s_v2
```

12. Connectez-vous au portail Azure via <https://portal.azure.com> et configurez les règles de mise en réseau de l'appliance. Les règles suivantes doivent être configurées pour le groupe de sécurité réseau :

Tableau 2: Règles relatives aux ports entrants

Nom	Port	Protocole
EXA	9443	TCP
HTTPS	443	TCP
SSH	22	TCP

Tableau 3: Règles relatives aux ports sortants

Nom	Port	Protocole
DNS	53	UDP
EXA	9443	N'IMPORTE LEQUEL
HTTPS	443	TCP
SSH	22	TCP

13. Répétez les étapes 10 à 12 pour déployer des magasins de disques supplémentaires afin de créer votre cluster.

 **Important:** Ne créez pas de copie d'une machine virtuelle ExtraHop existante pour déployer une nouvelle instance. Commencez toujours par créer un nouveau disque géré à partir du fichier VHD d'origine.

Prochaines étapes

Ouvrez un navigateur Web et connectez-vous aux paramètres d'administration du système ExtraHop via <https://<extrahop-hostname-or-IP-address>/admin>. Le nom de connexion par défaut est `setup` et le mot de passe est `default`.

Effectuez les procédures suivantes :

- [Enregistrez votre système ExtraHop](#)
- [Création d'un cluster d'espace de stockage des enregistrements](#)
- [Connectez la console et les capteurs aux magasins de disques ExtraHop](#)
- [Envoyer les données d'enregistrement à l'appliance Explore](#)
- Passez en revue le [Découvrir la liste de contrôle après le déploiement](#) et configurez des paramètres d'espace de stockage des enregistrements supplémentaires.