# Déployez la console de machine virtuelle ExtraHop ECA dans Azure

Publié: 2023-10-24

Les procédures suivantes expliquent comment déployer une console virtuelle ExtraHop dans un environnement Microsoft Azure. 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 console virtuelle ExtraHop.

| Paramètre | Descriptif |
|---|---|
| compte Azure | Permet d'accéder à vos abonnements Azure. |
| Groupe de ressources | Conteneur contenant les ressources associées au système ExtraHop. |
| Emplacement | La région géographique dans laquelle se trouvent les ressources Azure nécessaires à la maintenance de votre système ExtraHop. |
| 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 la console virtuelle ExtraHop est stockée sous forme de blob. |
| Disque géré | Le disque requis pour le stockage des données du système 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 du système ExtraHop. |
| Taille de l'instance de machine virtuelle Azure | Une taille d'instance Azure optimisée pour le nombre d'ExtraHop connectés capteurs, des disquaires et des magasins de paquets. |

| Paramètre | Descriptif |
| --- | --- |
| | Les performances de la machine virtuelle ECA console dépend du nombre de capteurs que vous déployez en combinaison avec le nombre d'appareils que vous vous attendez à ce que le système découvre dans votre environnement. Pour déterminer la taille appropriée, consultez le ECA VM Console Performance Guidelines.<br>• **Petits déploiements:** Standard_D4_v3 (4 vCPU et 16 Go de RAM)<br>• **Déploiements de taille moyenne:** Standard_D8_v3 (8 vCPU et 32 Go de RAM)<br>• **Déploiements de grande envergure:** Standard_D16_v3 (16 vCPU et 64 Go de RAM)<br>• **Déploiements de très grande envergure :** Standard_D32_v3 (32 vCPU et 128 Go de RAM) |
| adresse IP publique ou privée | L'adresse IP qui permet d'accéder au système ExtraHop. |

## Déployer la console

**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 6 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": "DOlda4+6U3Cf5TUAng8/GKotfX1HHJuc3yljAlU+aktRAf4/
KwVQUuAUnhdrw2yg5Pba5FpZn6oZYvROncnT8Q=="
 }
]
```

6. 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 un compte 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>
     ```

7. 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-eca-
azure-7.2.0.5000.vhd --validate-content
```

9. Récupérez l'URI du blob. Vous aurez besoin de l'URI lors de la création du 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
```

Une sortie similaire à l'exemple suivant 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 <Azure sku> --source <blob uri> --size-gb <size
 gb>
```

Où `sku` indique le type de disque et le modèle de réplication souhaité. Les disques gérés ne prennent en charge que Standard_LRS et Premium_LRS. Premium_LRS a une taille de disque maximale de 1 To et Standard_LRS a une taille de disque maximale de 4 To.

Reportez-vous au ECA VM Console Performance Guidelines la taille de disque recommandée `--size-gb` paramètre.

Par exemple :

```
az disk create --resource-group exampleRG --location westus
--name exampleDisk --sku Standard_LRS --source https://
examplesa.blob.core.windows.net/examplesc/extrahop.vhd
--size-gb 52
```

11. Créez la machine virtuelle et connectez le disque géré. Cette commande crée la machine virtuelle ECA 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_D2_v3
```

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 1: Règles relatives aux ports entrants**

| Nom | Port | Protocole |
|---|---|---|
| HTTPS | 443 | TCP |
| SSH | 22 | TCP |

**Tableau 2: Règles relatives aux ports sortants**

| Nom | Port | Protocole |
|---|---|---|
| DNS | 53 | UDP |
| HTTPS | 443 | TCP |
| SSH | 22 | TCP |

**Prochaines étapes**
Ouvrez un navigateur Web et connectez-vous au système ExtraHop via l' adresse IP privée configurée. Le nom de connexion par défaut est `setup` et le mot de passe est `default`.

Effectuez les procédures recommandées suivantes :

- Enregistrez votre système ExtraHop
- Configurer l'heure du système
- Configuration des paramètres d'e-mail pour les notifications
- Connectez la console et les capteurs aux magasins de disques ExtraHop
- Connectez les capteurs et la console au stockage des paquets