Déployer une sonde ExtraHop dans Azure

Publié: 2024-02-16

Les procédures suivantes expliquent comment déployer une appliance virtuelle ExtraHop Discover 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.

Important: Pour garantir les meilleures performances lors de la synchronisation initiale de l'équipement, connectez tous les capteurs à la console, puis configurez le transfert du trafic réseau vers les capteurs.

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 environnement virtuel ExtraHop. sonde.

Paramètre	Description
compte Azure	Permet d'accéder à vos abonnements Azure.
Groupe de ressources	Un conteneur contenant les ressources associées à l'ExtraHop sonde.
Emplacement	La région géographique dans laquelle se trouvent les ressources Azure nécessaires à la maintenance de votre environnement virtuel sonde.
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 où se trouve l'ExtraHop sonde l'image est stockée sous forme de blob.
Disque géré	Le disque requis pour ExtraHop sonde stockage de données. Spécifiez le SKU de stockage StandardSSD_LRS lorsque vous créez le disque.
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'ExtraHop. sonde.
Taille de l'instance de machine virtuelle Azure	Une taille d'instance Azure qui correspond le mieux à sonde Taille de la machine virtuelle, comme suit :

Paramètre	Description
	• **Reveal (x) EDA 1100 v:** Standard_A4_v2 (4 vCPU et 8 Go de RAM) • **EDA 6100 V:** Standard_D16_v3 (16 vCPU et 64 Go de RAM)
Disque de capture de paquets en option	(Facultatif) Un disque de stockage pour les déploiements qui incluent la capture précise de paquets. Spécifiez le SKU de stockage Standard_LRS lorsque vous créez et ajoutez le disque. • Pour l'EDA 1100v, vous pouvez ajouter un disque d'une capacité maximale de 250 Go. • Pour l'EDA 6100v, vous pouvez ajouter un disque d'une capacité maximale de 500 Go.
adresse IP publique ou privée	L'adresse IP qui permet d'accéder au système ExtraHop.

Déployez la sonde

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 pour définir les variables d'environnement Azure.

1. Ouvrez l'interpréteur de commandes Windows, Cmd.exe, et connectez-vous à votre compte Azure.

   ```
   az login
   ```

2. Ouvert `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 au suivant apparaît :

```
[
 {
   "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 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>
     ```

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-eda-1100v-
azure-7.4.0.5000.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 au suivant apparaît :

```
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 StandardSSD_LRS --source <blob uri> --size-gb
 <size in GB>
```

Spécifiez la taille de disque suivante pour `--size-gb` paramètre :

capteur	Taille du disque (GiB)
EDA 1100v - Reveal (x)	61
EDA 6100 V	1000

Par exemple :

```
az disk create --resource-group exampleRG --location westus
--name exampleDisk --sku StandardSSD_LRS --source https://
examplesa.blob.core.windows.net/examplesc/extrahop.vhd
--size-gb 61
```

Important: Les étapes 11 à 16 sont nécessaires pour configurer les interfaces réseau de l'EDA 6100v. Si vous déployez l'EDA 1100v, passez à **étape 17**.

11. (6100 V uniquement) Créez un réseau virtuel.

```
az network vnet create --resource-group <resource group name> --name
 <virtual network name>
       --address-prefixes <IP addresses for the virtual network>
```

Par exemple :

```
az network vnet create --resource-group exampleRG --name example-vnet --
address-prefixes 10.0.0.0/16
```

12. (6100v uniquement) Créez le sous-réseau de gestion.

```
az network vnet subnet create --resource-group <resource group name> --
vnet-name <virtual
        network name> --name <subnet name> --address-prefix <CIDR address
 prefix>
```

Par exemple :

```
az network vnet subnet create --resource-group exampleRG --vnet-name
 example-vnet
--name example-mgmt-subnet --address-prefix 10.0.1.0/24
```

13. (6100 v uniquement) Créez le sous-réseau de surveillance (ingestion).

```
az network vnet subnet create --resource-group <resource group name> --
vnet-name <virtual
        network name> --name <subnet name> --address-prefix <CIDR address
 prefix>
```

Par exemple :

```
az network vnet subnet create --resource-group exampleRG --vnet-name
 example-vnet
--name example-ingest1-subnet --address-prefix 10.0.2.0/24
```

14. (6100 V uniquement) Créez l'interface du réseau de gestion.

```
az network nic create --resource-group <resource group name> --name
 <network interface name>
--vnet-name <virtual network name> --subnet <management subnet name> --
location <location> --accelerated-networking true
```

Par exemple :

```
az network nic create --resource-group exampleRG --name 6100-mgmt-nic
--vnet-name example-vnet --subnet example-mgmt-subnet --location westus
 --accelerated-networking true
```

15. (6100 V uniquement) Créez l'interface réseau de surveillance (ingestion).

```
az network nic create --resource-group <resource group name> --name
 <ingest network interface name>
 --vnet-name <virtual network name> --subnet <ingest subnet name> --
location <location> --private-ip-address
<static private IP address> --accelerated-networking true
```

Par exemple :

```
az network nic create --resource-group exampleRG --name 6100-ingest1-nic
--vnet-name green-vnet --subnet example-ingest1-subnet
--location westus --private-ip-address 10.0.2.100 --accelerated-
networking true
```

16. (6100v uniquement) Créez la machine virtuelle 6100v. Cette commande crée la machine virtuelle de la sonde EDA 6100v avec les interfaces réseau configurées.

```
az vm create --resource-group <resource group name> --name <vm name>
--os-type linux --attach-os-disk <disk name> --nics <management NIC
 ingest NIC>
--size <Azure machine size> --public-ip-address ""
```

Par exemple :

```
az vm create --resource-group exampleRG --name exampleVM --os-type linux
--attach-os-disk exampleDisk --nics 6100-mgmt-nic 6100-ingest1-nic
--size Standard_D16_v3 --public-ip-address ""
```

Une fois l'EDA 6100v créé, passez à l'étape 18.

17. Créez la machine virtuelle et connectez le disque géré. Cette commande crée la machine virtuelle de la sonde avec un groupe de sécurité réseau par défaut et une adresse IP privée.

```
az vm create --resource-group <resource group name> --public-ip-address
 ""
--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 "" --name
 exampleVM --os-type linux
--attach-os-disk exampleDisk --size Standard_A4_v2
```

18. 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
RPCAP	2003	TCP
RPCAP	2003-2034	UDP
SSH	22	TCP

Tableau 2: Règles relatives aux ports sortants

Nom	Port	Protocole
DNS	53	UDP
HTTPS	443	TCP
RPCAP	2003	TCP
SSH	22	TCP

(Facultatif) Ajoutez un disque pour des captures de paquets précises

Si votre sonde possède une licence pour la capture précise des paquets, vous devez ajouter un disque de stockage dédié sur la machine virtuelle pour stocker les paquets.

1. Exécutez la commande suivante pour ajouter un nouveau disque :

```
az vm disk attach --new --name <disk_name>  --resource-group
 <resource_group_name> --size-gb <disk_size> --sku Standard_LRS --vm-name
 <vm_name>
```

   Par exemple :

```
az vm disk attach --new --name packetstore --resource-group exampleRG --
size-gb 40 --sku Standard_LRS --vm-name exampleVM
```

2. Configurer la capture de paquets.

Prochaines étapes

- Ouvrez un navigateur Web et accédez au système ExtraHop via l'adresse IP de gestion configurée. Acceptez le contrat de licence, puis connectez-vous. Le nom de connexion par défaut est `setup` et le mot de passe est `default`. Suivez les instructions pour saisir la clé de produit, modifier la configuration par défaut et les mots de passe du compte utilisateur shell, vous connecter à ExtraHop Cloud Services et vous connecter à une console.
- Une fois que la sonde a obtenu une licence et que vous avez vérifié que le trafic est détecté, suivez les procédures recommandées dans le liste de contrôle après le déploiement.