Déploiement d'une sonde ExtraHop sur Azure

Publié: 2025-03-28

Les procédures suivantes expliquent comment déployer un ExtraHop virtuel sonde dans un environnement Microsoft Azure. Vous devez avoir de l'expérience en matière d' administration dans un environnement Azure.

Un ExtraHop virtuel sonde peut vous aider à surveiller les performances de vos applications sur les réseaux internes, l'Internet public ou une interface de bureau virtuel (VDI), y compris la base de données et les niveaux de stockage. Le système ExtraHop peut surveiller les performances des applications dans des environnements géographiquement distribués, tels que des succursales ou des environnements virtualisés via le trafic inter-machines virtuelles.

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 la réussite du déploiement, assurez-vous d'avoir accès aux ressources requises ou de pouvoir 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 CLI Azure installé.
- Vous devez disposer du fichier du disque dur virtuel (VHD) ExtraHop, disponible sur Portail client ExtraHop. Extrayez le fichier VHD du fichier téléchargé `.zip` fichier d'archive.
- Vous devez disposer d'une clé de produit ExtraHop.
- Azure crée un disque temporaire qui apparaît sur la page Disques après la création du disque principal de la banque de données et le redémarrage du système. Ce disque n'est pas destiné à votre sonde ou à votre stockage des paquets. Vous pouvez ignorer ce disque.

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

Vous devez configurer les paramètres environnementaux suivants dans Azure pour déployer votre sonde virtuelle ExtraHop :

- Un compte Azure.
- Un groupe de ressources qui contient les ressources associées à la sonde ExtraHop.
- Une région géographique où se trouvent les ressources Azure nécessaires à la maintenance de votre sonde virtuelle.
- Un compte de stockage Azure qui contient tous vos objets de données Azure Storage, y compris les blobs et les disques.
- Conteneur de stockage dans lequel l'image de la sonde ExtraHop est stockée sous forme de blob.
- Un disque SKU de stockage Standard_LRS ou quatre disques SKU de stockage Standard_SSD_LRS pour stocker les données de la sonde ExtraHop.
- Groupe de sécurité réseau contenant des règles de sécurité qui autorisent ou interdisent le trafic réseau entrant ou sortant depuis la sonde ExtraHop.
- Une adresse IP publique ou privée qui permet d'accéder au système ExtraHop.

Exigences relatives aux machines virtuelles

Vous devez provisionner une taille d'instance Azure répondant aux exigences suivantes.

Sonde	Type d'instance
EDA 1 100 V	Standard_A4_v2 (4 processeurs virtuels et 8 Go de RAM)
EDA 6100v	Standard_D16_v3 (16 processeurs virtuels et 64 Go de RAM)
EDA 6370v	Standard_D48S_v5 (48 processeurs virtuels et 192 Go de RAM)

Exigences relatives aux disques de capture de paquets Precision

Si votre déploiement inclut la capture de paquets de précision, vous devez configurer un disque de stockage des paquets qui répond aux exigences suivantes.

Sonde	SKU de stockage sur disque	Taille maximale
EDA 1 100 V	Norme_LRS	256 Gio
EDA 6100v	Norme_LRS	512 Gio
EDA 6370v	Norme_LRS	512 Gio

Note: N'ajoutez pas de disque de capture de paquets de précision aux capteurs EDA 6370v si le module Packet Forensics est activé ; ajoutez plutôt un disque de criminalistique de paquets.

Configuration requise pour les disques Packet Forensics

Si votre déploiement inclut la capture globale de paquets avec le module Packet Forensics, vous devez configurer les disques de stockage des paquets qui répondent aux exigences suivantes.

Sonde	SKU de stockage sur disque	Taille du disque (pour chaque disque)	Nombre de disques
EDA 6370v	SSD_LRS standard	8192 Gio	4

Note: Les capteurs EDA 1100v et EDA 6100v ne prennent pas en charge le module Packet Forensics.

Déploiement de la sonde

Avant de commencer
Les procédures ci-dessous partent du principe 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. Connectez-vous à Azure via l'interface de ligne de commande Azure.
   Pour plus d'informations, consultez le Site Web de documentation Microsoft.
2. 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
```

3. 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
```

4. Consultez la clé du compte de stockage. La valeur de `key1` est nécessaire pour définir les variables d'environnement du compte de stockage Azure par défaut.

```
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
```

Une sortie similaire à la suivante apparaît :

```
[
 {
   "keyName": "key1",
   "permissions": "Full",
   "value":
 "CORuU8mTcxLxq0bbszhZ4RKTB93CqLpjZdAhCrNJugAorAyvJjhGmBSedjYPmnzXPikSRigd
5T5/YGYBoIzxNg=="
 },
 { "keyName": "key2",
   "permissions": "Full",
   "value": "DOlda4+6U3Cf5TUAng8/GKotfX1HHJuc3yljAlU+aktRAf4/
KwVQUuAUnhdrw2yg5Pba5FpZn6oZYvROncnT8Q=="
 }
]
```

5. 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 de la suite 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 que vous avez consultée à l'étape précédente.

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>
```

6. Créez un conteneur de stockage.

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

Par exemple :

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

7. 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
```

8. Afficher l'URI du blob. L'URI est obligatoire pour créer le disque géré.

```
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 la suivante apparaît :

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

9. 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 :

Sonde	Taille du disque (GiB)
EDA 1100v - RevealX	61
EDA 6100v	1000
EDA 6370v	1400

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
```

10. Créez l'environnement réseau et la machine virtuelle pour la sonde EDA 6100v.

    Note: Effectuez ces étapes uniquement si vous configurez une sonde EDA 6100v .

    a) 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
    ```

    b) 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
    ```

    c) 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
    ```

    d) Créez l'interface 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
```

e) Création de 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
```

f) 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 ""
```

g) 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 ""
```

11. Créez l'environnement réseau et la machine virtuelle pour la sonde EDA 6370v.

Important: Effectuez ces étapes uniquement si vous configurez une sonde EDA 6370v.

a) 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
```

b) 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
```

c) Créez l'interface 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 6370-mgmt-
nic --vnet-name example-vnet --subnet example-mgmt-subnet --location
 westus --accelerated-networking true
```

d) Créez la machine virtuelle 6370v. Cette commande crée la machine virtuelle de la sonde EDA 6370v 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>
 --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 6370-mgmt-nic --size
 Standard_D48s_v5 --public-ip-address ""
```

12. Créez la machine virtuelle EDA 1100v et connectez le disque géré.

Important: Effectuez cette étape uniquement si vous configurez une sonde EDA 1100v. 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
```

13. 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

Nom	Port	Protocole
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

Ajoutez un disque pour une capture de paquets précise

Si votre sonde est autorisée pour la capture de paquets de précision, 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 packetcap --resource-group exampleRG --
size-gb 512 --sku Standard_LRS --vm-name exampleVM
```

Note: Voir Exigences relatives aux disques de capture de paquets Precision pour les exigences de dimensionnement.

2. Configurer la capture de paquets.

Configuration de la sonde

Avant de commencer
Avant de pouvoir configurer la sonde, vous devez avoir déjà configuré une adresse IP de gestion.

1. Afficher l'ID de la machine virtuelle de la sonde.

```
az vm show --resource-group <resource group name> --name <vm name>
```

Par exemple :

```
az vm show --resource-group exampleRG --name exampleVM
```

Enregistrez la valeur de `vmId` champ.

2. 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 la valeur de `vmId` champ que vous avez enregistré à l'étape précédente.

3. Acceptez le contrat de licence, puis connectez-vous.

4. 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 aux services cloud ExtraHop et vous connecter à une console ExtraHop.

Prochaines étapes
Une fois que le système a obtenu une licence et que vous avez vérifié que le trafic est détecté, suivez les procédures recommandées dans Liste de contrôle après le déploiement des capteurs et des consoles.

Ajouter des disques pour Packet Forensics

Si votre déploiement inclut la capture globale de paquets avec le module Packet Forensics , vous devez ajouter des disques de stockage dédiés 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 StandardSSD_LRS --vm-
name <vm_name>
```

Par exemple :

```
az vm disk attach --new --name packetstore1 --resource-group exampleRG --
size-gb 8192 --sku StandardSSD_LRS --vm-name exampleVM
```

Note: Répétez cette étape pour chaque disque que vous souhaitez ajouter. Voir Configuration requise pour les disques Packet Forensics pour les exigences de dimensionnement.

2. Configurer la capture de paquets.