Stellen Sie einen ExtraHop-Sensor auf Azure bereit

Veröffentlicht: 2025-03-27

Die folgenden Verfahren erklären, wie Sie einen virtuellen ExtraHop bereitstellen. Sensor in einer Microsoft Azure-Umgebung. Sie müssen Erfahrung in der Verwaltung in einer Azure-Umgebung haben.

Ein virtueller ExtraHop Sensor kann Ihnen helfen, die Leistung Ihrer Anwendungen in internen Netzwerken, im öffentlichen Internet oder einer virtuellen Desktop-Schnittstelle (VDI), einschließlich Datenbank- und Speicherebenen, zu überwachen. Das ExtraHop-System kann die Anwendungsleistung in geografisch verteilten Umgebungen wie Zweigstellen oder virtualisierten Umgebungen über den Verkehr zwischen virtuellen Rechnern überwachen.

Bevor du anfängst

- Sie müssen Erfahrung mit der Bereitstellung virtueller Maschinen in Azure innerhalb Ihrer virtuellen Netzwerkinfrastruktur haben. Um sicherzustellen, dass die Bereitstellung erfolgreich ist, stellen Sie sicher, dass Sie Zugriff auf die erforderlichen Ressourcen haben oder in der Lage sind, diese zu erstellen. Möglicherweise müssen Sie mit anderen Experten in Ihrer Organisation zusammenarbeiten, um sicherzustellen, dass die erforderlichen Ressourcen verfügbar sind.
- Sie benötigen einen Linux-, Mac- oder Windows-Client mit der neuesten Version von Azure-CLI installiert.
- Sie benötigen die ExtraHop-Datei für virtuelle Festplatten (VHD), verfügbar auf der ExtraHop Kundenportal. Extrahieren Sie die VHD-Datei aus der heruntergeladenen `.zip` Archivdatei.
- Sie benötigen einen ExtraHop-Produktschlüssel.
- Azure erstellt eine temporäre Festplatte, die auf der Seite „Festplatten“ angezeigt wird, nachdem die Hauptdatenspeicherfestplatte erstellt und das System neu gestartet wurde. Diese Diskette ist nicht für Ihren Sensor oder Packetstore vorgesehen. Sie können diese Festplatte ignorieren.

Wichtig: Um die beste Leistung bei der ersten Gerätesynchronisierung zu gewährleisten, schließen Sie alle Sensoren an die Konsole an und konfigurieren Sie dann die Weiterleitung des Netzwerkverkehrs zu den Sensoren.

Anforderungen an das System

Sie müssen die folgenden Umgebungsparameter in Azure konfigurieren, um Ihren virtuellen ExtraHop-Sensor bereitzustellen:

- Ein Azure-Konto.
- Eine Ressourcengruppe, die verwandte Ressourcen für den ExtraHop-Sensor enthält.
- Eine geografische Region, in der sich die Azure-Ressourcen zur Unterstützung Ihres virtuellen Sensor befinden.
- Ein Azure-Speicherkonto, das alle Ihre Azure Storage-Datenobjekte enthält, einschließlich Blobs und Festplatten.
- Ein Speicherbehälter, in dem das ExtraHop-Sensorbild als Blob gespeichert wird.
- Eine Standard_LRS-Speicher-SKU-Diskette oder vier StandardSSD_LRS-Speicher-SKU-Disketten zum Speichern von ExtraHop-Sensordaten.
- Eine Netzwerksicherheitsgruppe, die Sicherheitsregeln enthält, die eingehenden Netzwerkverkehr zum ExtraHop-Sensor oder ausgehenden Netzwerkverkehr vom ExtraHop-Sensor zulassen oder verweigern.
- Eine öffentliche oder private IP-Adresse, die den Zugriff auf das ExtraHop-System ermöglicht.

VM-Anforderungen

Sie müssen eine Azure-Instanzgröße bereitstellen, die die folgenden Anforderungen erfüllt.

Fühler	Instanztyp
EDA 1100 V	Standard_A4_v2 (4 vCPU und 8 GiB RAM)
EDA 6100 v	Standard_D16_V3 (16 vCPU und 64 GiB RAM)
EDA 6370v	Standard_D48s_V5 (48 vCPUs und 192 GiB RAM)

Festplattenanforderungen für die präzise PCAP

Wenn Ihre Bereitstellung eine präzise PCAP umfasst, müssen Sie konfiguriere eine Packetstore-Festplatte das erfüllt die folgenden Anforderungen.

Fühler	Festplattenspeicher-SKU	Maximale Größe
EDA 1100 V	Standard LRS	256 GiB
EDA 6100 v	Standard LRS	512 GiB
EDA 6370v	Standard LRS	512 GiB

Hinweis: Fügen Sie den EDA 6370v-Sensoren keine Precision PCAP Disk hinzu, wenn das Packet Forensics Modul aktiviert ist. Fügen Sie stattdessen eine Paketforensik-Festplatte hinzu.

Festplattenanforderungen für Packet Forensics

Wenn Ihre Bereitstellung die globale PCAP mit dem Modul Packet Forensics beinhaltet, müssen Sie Packetstore-Festplatten konfigurieren die die folgenden Anforderungen erfüllen.

Fühler	Festplattenspeicher-SKU	Festplattengröße (für jede Festplatte)	Anzahl der Festplatten
EDA 6370v	Standard-SSD_LRS	81,92 GiB	4

Hinweis: Die Sensoren EDA 1100v und EDA 6100v unterstützen das Packet Forensics Modul nicht.

Stellen Sie den Sensor bereit

Bevor Sie beginnen
Bei den folgenden Verfahren wird davon ausgegangen, dass Sie die erforderliche Ressourcengruppe, das Speicherkonto, den Speichercontainer und die Netzwerksicherheitsgruppe nicht konfiguriert haben. Wenn Sie diese Parameter bereits konfiguriert haben, können Sie mit Schritt 6 fortfahren, nachdem Sie sich bei Ihrem Azure-Konto angemeldet haben, um Azure-Umgebungsvariablen festzulegen.

1. Melden Sie sich über die Azure-CLI bei Azure an.
   Weitere Informationen finden Sie in der Microsoft-Dokumentationswebsite.
2. Erstellen Sie eine Ressourcengruppe.

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

Erstellen Sie beispielsweise eine neue Ressourcengruppe in der Region West USA.

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

3. Erstellen Sie ein Speicherkonto.

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

Zum Beispiel:

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

4. Zeigen Sie den Speicherkontoschlüssel an. Der Wert für `key1` ist erforderlich , um die standardmäßigen Umgebungsvariablen für Azure-Speicherkonten festzulegen.

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

Zum Beispiel:

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

Es wird eine Ausgabe ähnlich der folgenden angezeigt:

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

5. Legen Sie standardmäßige Umgebungsvariablen für Azure-Speicherkonten fest. Sie können mehrere Speicherkonten in Ihrem Azure-Abonnement haben. Um eine davon auszuwählen, die auf alle nachfolgenden Speicherbefehle angewendet werden soll, setzen Sie diese Umgebungsvariablen. Wenn Sie keine Umgebungsvariablen setzen, müssen Sie immer angeben `--account-name` und `--account-key` in den Befehlen im Rest dieses Verfahrens.

PowerShell

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

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

Wo *<key1>* ist der Speicherkonto-Schlüsselwert, den Sie im vorherigen Schritt angesehen haben.

Zum Beispiel:

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

```
$Env:AZURE_STORAGE_KEY=CORuU8mTcxLxq0bbszhZ4RKTB93CqLpjZdAhCrNJugAor
AyvJjhGmBSedjYPmnzXPikSRigd5T5/YGYBoIzxNg==
```

Hinweis: Legen Sie die Umgebungsvariablen im Windows-Befehlsinterpreter (Cmd.exe) mit der folgenden Syntax fest:

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

- Legen Sie Umgebungsvariablen in der Linux-Befehlszeilenschnittstelle mit der folgenden Syntax fest:

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

6. Erstellen Sie einen Speichercontainer.

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

Zum Beispiel:

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

7. Laden Sie die ExtraHop VHD-Datei in den Blob-Speicher hoch.

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

Zum Beispiel:

```
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. Sehen Sie sich den Blob-URI an. Der URI ist erforderlich, um den verwalteten Datenträger zu erstellen.

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

Zum Beispiel:

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

Es wird eine Ausgabe ähnlich der folgenden angezeigt:

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

9. Erstellen Sie eine verwaltete Festplatte und beziehen Sie die ExtraHop-VHD-Datei.

```
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>
```

Geben Sie die folgende Festplattengröße für `--size-gb` Parameter:

Fühler	Festplattengröße (GiB)
EDA 1100 V - RevealX	61
EDA 6100 v	1000
EDA 6370v	1400

Zum Beispiel:

```
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. Erstellen Sie die Netzwerkumgebung und die VM für den EDA 6100v-Sensor.

    Hinweis: Führen Sie diese Schritte nur aus, wenn Sie einen EDA 6100V-Sensor konfigurieren.

    a) Erstellen Sie ein virtuelles Netzwerk.

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

    Zum Beispiel:

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

    b) Erstellen Sie das Management-Subnetz.

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

    Zum Beispiel:

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

    c) Erstellen Sie das Überwachungs- (Ingest-) Subnetz.

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

    Zum Beispiel:

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

    d) Erstellen Sie die Verwaltungsnetzwerkschnittstelle.

    ```
    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
    ```

Zum Beispiel:

```
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) Erstellen Sie die Überwachungs- (Ingest-) Netzwerkschnittstelle

```
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
```

Zum Beispiel:

```
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) Erstellen Sie die 6100v-VM. Mit diesem Befehl wird die EDA 6100v-Sensor-VM mit den konfigurierten Netzwerkschnittstellen erstellt.

```
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 ""
```

Zum Beispiel:

```
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) Erstellen Sie die 6100v-VM. Mit diesem Befehl wird die EDA 6100v-Sensor-VM mit den konfigurierten Netzwerkschnittstellen erstellt.

```
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 ""
```

Zum Beispiel:

```
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. Erstellen Sie die Netzwerkumgebung und die VM für den EDA 6370v-Sensor.

    Wichtig: Führen Sie diese Schritte nur aus, wenn Sie einen EDA 6370v-Sensor konfigurieren.

a) Erstellen Sie ein virtuelles Netzwerk.

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

Zum Beispiel:

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

b) Erstellen Sie das Management-Subnetz.

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

Zum Beispiel:

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

c) Erstellen Sie die Verwaltungsnetzwerkschnittstelle.

```
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
```

Zum Beispiel:

```
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) Erstellen Sie die 6370v-VM. Mit diesem Befehl wird die EDA 6370v-Sensor-VM mit den konfigurierten Netzwerkschnittstellen erstellt.

```
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 ""
```

Zum Beispiel:

```
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. Erstellen Sie die EDA 1100v-VM und hängen Sie die verwaltete Festplatte an.

Wichtig: Führen Sie diesen Schritt nur aus, wenn Sie einen EDA 1100V-Sensor konfigurieren. Mit diesem Befehl wird die Sensor-VM mit einer Standard-Netzwerksicherheitsgruppe und einer privaten IP-Adresse erstellt.

```
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>
```

Zum Beispiel:

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

13. Melden Sie sich beim Azure-Portal an über https://portal.azure.com und konfigurieren Sie die Netzwerkregeln für die Appliance. Für die Netzwerksicherheitsgruppe müssen die folgenden Regeln konfiguriert sein:

Tabelle 1: Regeln für eingehende Ports

Name	Hafen	Protokoll
HTTPS	443	TCP
RPCAP	2003	TCP
RPCAP	2003-2034	UDP
SSH	22	TCP

Tabelle 2: Regeln für ausgehende Ports

Name	Hafen	Protokoll
DNS	53	UDP
HTTPS	443	TCP
RPCAP	2003	TCP
SSH	22	TCP

Fügen Sie eine Festplatte für die präzise PCAP hinzu

Wenn Ihr Sensor für die präzise PCAP lizenziert ist, müssen Sie der VM eine dedizierte Speicherfestplatte hinzufügen, um die Pakete zu speichern.

1. Führen Sie den folgenden Befehl aus, um eine neue Festplatte hinzuzufügen:

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

Zum Beispiel:

```
az vm disk attach --new --name packetcap --resource-group exampleRG --
size-gb 512 --sku Standard_LRS --vm-name exampleVM
```

Hinweis siehe Festplattenanforderungen für die präzise PCAP für Größenanforderungen.

2. PCAP konfigurieren.

Den Sensor konfigurieren

Bevor Sie beginnen
Bevor Sie den Sensor konfigurieren können, müssen Sie bereits eine Verwaltungs-IP-Adresse konfiguriert haben.

1. Zeigen Sie die ID der Sensor-VM an.

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

Zum Beispiel:

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

Notieren Sie den Wert von `vmId` Feld.

2. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

   Der Standard-Anmeldename ist `setup` und das Passwort ist der Wert von `vmId` Feld, das Sie im vorherigen Schritt aufgezeichnet haben.
3. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich dann an.
4. Folgen Sie den Anweisungen, um den Produktschlüssel einzugeben, das Standard-Setup und die Passwörter für das Shell-Benutzerkonto zu ändern, eine Verbindung zu den ExtraHop Cloud Services herzustellen und eine Verbindung zu einer ExtraHop-Konsole herzustellen.

Nächste Schritte
Nachdem das System lizenziert ist und Sie sich vergewissert haben, dass Datenverkehr erkannt wird, führen Sie die empfohlenen Verfahren in der Checkliste für Sensor und Konsole nach der Bereitstellung.

Festplatten für Packet Forensics hinzufügen

Wenn Ihre Bereitstellung die globale PCAP mit dem Modul Packet Forensics beinhaltet, müssen Sie dedizierte Speicherfestplatten auf der VM hinzufügen, um die Pakete zu speichern.

1. Führen Sie den folgenden Befehl aus, um eine neue Festplatte hinzuzufügen:

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

   Zum Beispiel:

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

   Hinweis Wiederholen Sie diesen Schritt für jede Festplatte, die Sie hinzufügen möchten. siehe Festplattenanforderungen für Packet Forensics für Größenanforderungen.
2. PCAP konfigurieren.