Stellen Sie einen ExtraHop-Sensor auf Azure bereit

Veröffentlicht: 2024-06-03

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 dem heruntergeladenen `.zip` Archivdatei.
- Sie benötigen einen ExtraHop-Produktschlüssel.

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

Die folgende Tabelle zeigt die Umgebungsparameter, die Sie in Ihrer Azure-Umgebung konfigurieren müssen oder die Sie möglicherweise bereits in Ihrer Azure-Umgebung konfiguriert haben, um Ihr virtuelles ExtraHop-Objekt erfolgreich bereitzustellen Sensor.

Parameter	Beschreibung
Azure-Konto	Ermöglicht den Zugriff auf Ihre Azure-Abonnements.
Ressourcengruppe	Ein Container, der verwandte Ressourcen für den ExtraHop enthält Sensor.
Standort	Die geografische Region, in der sich die Azure-Ressourcen befinden, um Ihre virtuelle Umgebung aufrechtzuerhalten Sensor.
Speicherkonto	Das Azure-Speicherkonto enthält alle Ihre Azure Storage-Datenobjekte, einschließlich Blobs und Festplatten.
Blob-Speicherbehälter	Der Aufbewahrungsbehälter, in dem sich der ExtraHop befand Sensor Bild wird als Blob gespeichert.

© 2024ExtraHop Networks, Inc. Alle Rechte vorbehalten.

Parameter	Beschreibung
Verwaltete Festplatte	Die für ExtraHop benötigte Festplatte Sensor Datenspeicherung. Geben Sie die StandardSSD_LRS Speicher-SKU an, wenn Sie die Festplatte erstellen.
Netzwerksicherheitsgruppe	Die Netzwerksicherheitsgruppe enthält Sicherheitsregeln, die eingehenden Netzwerkverkehr zum ExtraHop oder ausgehenden Netzwerkverkehr vom ExtraHop zulassen oder verweigern Sensor.
Größe der Azure-VM-Instanz	Eine Azure-Instanzgröße, die der am ehesten entspricht Sensor VM-Größe wie folgt: • **EDA 1100 V:** Standard_A4_v2 (4 vCPU und 8 GiB RAM) • **EDA 6100 v:** Standard_D16_V3 (16 vCPU und 64 GiB RAM)
Optionale Paketerfassungsdiskette	(Optional) Eine Speicherfestplatte für Bereitstellungen, die eine präzise Paketerfassung beinhalten. Geben Sie die Standard_LRS-Speicher-SKU an, wenn Sie das Laufwerk erstellen und hinzufügen. • Für den EDA 1100v können Sie eine Festplatte mit einer Kapazität von bis zu 250 GB hinzufügen. • Für den EDA 6100v können Sie eine Festplatte mit einer Kapazität von bis zu 500 GB hinzufügen.
Öffentliche oder private IP-Adresse	Die IP-Adresse, die den Zugriff auf das ExtraHop-System ermöglicht.

Setzen Sie den Sensor ein

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. Öffnen Sie den Windows-Befehlsinterpreter Cmd.exe und melden Sie sich bei Ihrem Azure-Konto an.

   ```
   az login
   ```

2. Offen `https://aka.ms/devicelogin` in einem Webbrowser und geben Sie den Code zur Authentifizierung ein und kehren Sie dann zur Befehlszeilenschnittstelle zurück.
3. Erstellen Sie eine Ressourcengruppe.

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

   Erstellen Sie beispielsweise eine neue Ressourcengruppe in der Region USA, Westen.

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

4. 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
```

5. Sehen Sie sich den Speicherkontoschlüssel an. Der Wert für `key1` ist für Schritt 6 erforderlich.

```
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 erscheint eine Ausgabe, die der folgenden ähnelt:

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

6. Legen Sie die Standard-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, legen Sie diese Umgebungsvariablen fest. 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 Schlüsselwert des Speicherkontos, der in Schritt 5 angezeigt wird.

Zum Beispiel:

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

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

Hinweis:
- Legen Sie 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>
```

7. Erstellen Sie einen Lagercontainer.

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

Zum Beispiel:

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

8. 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
```

9. Ruft den Blob-URI ab. Sie benötigen den URI, wenn Sie die verwaltete Festplatte im nächsten Schritt 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 erscheint eine Ausgabe, die der folgenden ähnelt:

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

10. Erstellen Sie eine verwaltete Festplatte und beziehen Sie dabei 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 - Enthüllen (x)	61
EDA 6100 v	1000

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
```

Wichtig: Die Schritte 11 bis 16 sind erforderlich, um die Netzwerkschnittstellen für den EDA 6100v zu konfigurieren. Wenn Sie den EDA 1100v einsetzen, fahren Sie fort mit **Schritt 17**.

11. (nur 6100v) 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
```

12. (nur 6100v) 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
```

13. (nur 6100v) 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
```

14. (nur 6100v) 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
```

15. (nur 6100V) Erstellen Sie die Überwachungsnetzwerkschnittstelle (Ingest).

```
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
```

16. (nur 6100v) Erstellen Sie die 6100v-VM. Dieser Befehl erstellt die EDA 6100v-Sensor-VM mit den konfigurierten Netzwerkschnittstellen.

```
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 ""
```

Nachdem der EDA 6100v erstellt wurde, fahren Sie mit Schritt 18 fort.

17. Erstellen Sie die VM und hängen Sie die verwaltete Festplatte an. Dieser Befehl erstellt die Sensor-VM mit einer standardmäßigen Netzwerksicherheitsgruppe und einer privaten IP-Adresse.

```
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
```

18. 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

(Optional) Fügen Sie eine Festplatte für präzise Paketerfassungen hinzu

Wenn Ihr Sensor für die präzise Paketerfassung lizenziert ist, müssen Sie der virtuellen Maschine 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 packetstore --resource-group exampleRG --
size-gb 40 --sku Standard_LRS --vm-name exampleVM
```

2. PCAP konfigurieren.

Nächste Schritte

- Öffnen Sie einen Webbrowser und navigieren Sie über die konfigurierte Management-IP-Adresse zum ExtraHop-System. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich an. Der Standard-Anmeldename ist `setup` und das Passwort ist `default`. Folgen Sie den Anweisungen, um den Produktschlüssel einzugeben, das Standard-Setup und die Passwörter für das Shell-Benutzerkonto zu ändern, eine Verbindung zu ExtraHop Cloud Services herzustellen und eine Verbindung zu einer Konsole herzustellen.
- Nachdem der Sensor lizenziert wurde und Sie sich vergewissert haben, dass Datenverkehr erkannt wurde, führen Sie die empfohlenen Verfahren in der Checkliste nach der Bereitstellung.