Stellen Sie die ExtraHop ECA VM-Konsole in Azure bereit

Veröffentlicht: 2023-10-24

In den folgenden Verfahren wird erklärt, wie Sie eine virtuelle ExtraHop-Konsole in einer Microsoft Azure-Umgebung bereitstellen. Sie müssen über Erfahrung in der Verwaltung in einer Azure-Umgebung verfügen, um diese Verfahren durchführen zu können.

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 diese erstellen können. 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-Befehlszeilenschnittstelle installiert.
- Sie benötigen die virtuelle ExtraHop-Festplattendatei (VHD), verfügbar auf ExtraHop Kundenportal. Extrahieren Sie die VHD-Datei aus der heruntergeladenen ZIP-Archivdatei.
- Sie benötigen einen ExtraHop-Produktschlüssel.

Anforderungen an das System

Die folgende Tabelle zeigt die Umgebungsparameter, die Sie konfigurieren müssen oder die Sie möglicherweise bereits in Ihrer Azure-Umgebung konfiguriert haben, um Ihre virtuelle ExtraHop-Konsole erfolgreich bereitzustellen.

Parameter	Beschreibung
Azure-Konto	Bietet Zugriff auf Ihre Azure-Abonnements.
Ressourcengruppe	Ein Container, der verwandte Ressourcen für das ExtraHop-System enthält.
Standort	Die geografische Region, in der sich die Azure-Ressourcen für den Betrieb Ihres ExtraHop-Systems befinden.
Speicherkonto	Das Azure-Speicherkonto enthält alle Ihre Azure Storage-Datenobjekte, einschließlich Blobs und Festplatten.
Blob Aufbewahrungsbehälter	Der Speichercontainer, in dem das virtuelle ExtraHop-Konsolen-Image als Blob gespeichert wird.
Verwaltete Festplatte	Die Festplatte, die für den ExtraHop-Systemdatenspeicher erforderlich ist.
Netzwerksicherheitsgruppe	Die Netzwerksicherheitsgruppe enthält Sicherheitsregeln, die eingehenden Netzwerkverkehr zum ExtraHop-System oder ausgehenden Netzwerkverkehr vom ExtraHop-System zulassen oder verweigern.

Parameter	Beschreibung
Größe der Azure-VM-Instanz	Eine Azure-Instanzgröße, die für die Anzahl der verbundenen ExtraHop optimiert ist Sensoren, Plattenläden und Paketläden. Die Leistung der ECA VM Konsole hängt von der Anzahl der Sensoren ab, die Sie einsetzen, in Kombination mit der Anzahl der Geräte, die das System voraussichtlich in Ihrer Umgebung entdecken wird. Informationen zur Bestimmung der geeigneten Größe finden Sie in der ECA VM Console Performance Guidelines. • **Kleine Bereitstellungen:** Standard_D4_v3 (4 vCPU und 16 GiB RAM) • **Mittlere Bereitstellungen:** Standard_D8_v3 (8 vCPU und 32 GiB RAM) • **Große Bereitstellungen:** Standard_D16_v3 (16 vCPU und 64 GiB RAM) • **Extra große Bereitstellungen :** Standard_D32_v3 (32 vCPU und 128 GiB RAM)
Öffentliche oder private IP-Adresse	Die IP-Adresse, die den Zugriff auf das ExtraHop-System ermöglicht.

Stellen Sie die Konsole 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.

1. Öffnen Sie eine Terminalanwendung auf Ihrem Client und melden Sie sich bei Ihrem Azure-Konto an.

   ```
   az login
   ```

2. Öffnen Sie https://aka.ms/devicelogin in einem Webbrowser, 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 ein Konto auszuwählen, das 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-eca-
azure-7.2.0.5000.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 dem folgenden Beispiel 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 <Azure sku> --source <blob uri> --size-gb <size
 gb>
```

Wo `sku` gibt den Festplattentyp und das gewünschte Replikationsmuster an. Verwaltete Festplatten unterstützen nur Standard_LRS und Premium_LRS. Premium_LRS hat eine maximale Festplattengröße von 1 TB und Standard_LRS hat eine maximale Festplattengröße von 4 TB.

Beziehen Sie sich auf die ECA VM Console Performance Guidelines die Festplattengröße für die empfohlene `--size-gb` Parameter.

Zum Beispiel:

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

```
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>
```

Zum Beispiel:

```
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. 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
SSH	22	TCP

Tabelle 2: Regeln für ausgehende Ports

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

Nächste Schritte
Öffnen Sie einen Webbrowser und melden Sie sich über die konfigurierte private IP-Adresse beim ExtraHop-System an. Der Standard-Anmeldename ist `setup` und das Passwort ist `default`.

Führen Sie die folgenden empfohlenen Verfahren durch:

- Registrieren Sie Ihr ExtraHop-System
- Systemzeit konfigurieren
- E-Mail-Einstellungen für Benachrichtigungen konfigurieren
- Verbinde die Konsole und die Sensoren mit ExtraHop Recordstores
- Sensoren und Konsole mit dem Packetstore verbinden