Stellen Sie einen ExtraHop-Recordstore in Azure bereit

Veröffentlicht: 2024-04-09

In den folgenden Verfahren wird erklärt, wie Sie einen Recordstore in einer Microsoft Azure-Umgebung bereitstellen und mehrere Datensatzspeicher verbinden, um einen Cluster zu erstellen. 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 Ihren virtuellen ExtraHop-Recordstore erfolgreich bereitzustellen.

Parameter	Beschreibung
Azure-Konto	Bietet Zugriff auf Ihre Azure-Abonnements.
Ressourcengruppe	Ein Container, der verwandte Ressourcen für den ExtraHop-Recordstore enthält.
Standort	Die geografische Region, in der sich die Azure-Ressourcen befinden, um Ihre virtuellen Datenspeicher zu verwalten.
Speicherkonto	Das Azure-Speicherkonto enthält alle Ihre Azure Storage-Datenobjekte, einschließlich Blobs und Festplatten.
Blob Aufbewahrungsbehälter	Der Speichercontainer, in dem das ExtraHop-Recordstore-Bild als Blob gespeichert wird.
Verwaltete Festplatte	Die Festplatte, die für die Datenspeicherung im ExtraHop Recordstore erforderlich ist.
Netzwerksicherheitsgruppe	Die Netzwerksicherheitsgruppe enthält Sicherheitsregeln, die eingehenden Netzwerkverkehr zum ExtraHop-Recordstore oder ausgehenden Netzwerkverkehr vom ExtraHop-Recordstore zulassen oder verweigern.

Parameter	Beschreibung
Größe der Azure-VM-Instanz	Eine Azure-Instanzgröße, die der Größe der Explore Recordstore-VM am ehesten entspricht. Sehen Sie sich die Tabelle unten an.
Öffentliche oder private IP-Adresse	Die IP-Adresse, die den Zugriff auf das ExtraHop-System ermöglicht.

Tabelle 1: Azure-Datenspeicher- und Instanzgrößen

vCPUs	Speicher	Datenspeicher-Festplatte	Größe der Azure-Instanz
4	8 GB RAM	150 GB bis 250 GB	Standard F4S V2
8	16 GB RAM	150 GB bis 500 GB	Standard F8S V2
16	32 GB RAM	150 GB bis 1 TB	Standard F16S V2
32	64 GB RAM	150 GB bis 2 TB	Standard F32S V2

Stellen Sie den EXA 5100v 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 5 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. 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-exa-5100v-
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 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 <storage SKU> --source <blob uri> --size-gb
 <size gb>
```

Wo `storage SKU` gibt den Festplattentyp und das gewünschte Replikationsmuster an. Zum Beispiel `Premium_LRS`, `StandardSSD_LRS`, oder `Standard_LRS`.

Zum Beispiel:

```
az disk create --resource-group exampleRG --location westus
--name exampleDisk --sku Premium_LRS --source https://
examplesa.blob.core.windows.net/examplesc/extrahop.vhd
--size-gb 200
```

11. Erstellen Sie die VM und hängen Sie die verwaltete Festplatte an. Dieser Befehl erstellt die Recordstore-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_F4s_v2
```

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 2: Regeln für eingehende Ports

Name	Hafen	Protokoll
EXA	9443	TCP
HTTPS	443	TCP
SSH	22	TCP

Tabelle 3: Regeln für ausgehende Ports

Name	Hafen	Protokoll
DNS	53	UDP
EXA	9443	IRGENDEIN
HTTPS	443	TCP
SSH	22	TCP

13. Wiederholen Sie die Schritte 10 bis 12, um zusätzliche Datensatzspeicher für die Erstellung Ihres Cluster bereitzustellen.

> **Wichtig:** Erstellen Sie keine Kopie einer vorhandenen virtuellen ExtraHop-Maschine, um eine neue Instanz bereitzustellen. Beginnen Sie immer damit, eine neue verwaltete Festplatte aus der ursprünglichen VHD-Datei zu erstellen.

Nächste Schritte
Öffnen Sie einen Webbrowser und melden Sie sich in den Administrationseinstellungen des ExtraHop-Systems an über `https://<extrahop-hostname-or-IP-address>/admin`. Der Standard-Anmeldename ist `setup` und das Passwort ist `default`.

Führen Sie die folgenden Verfahren durch:

- Registrieren Sie Ihr ExtraHop-System
- Einen Recordstore-Cluster erstellen
- Verbinde die Konsole und die Sensoren mit ExtraHop Recordstores
- Senden Sie Datensatzdaten an die Explore-Appliance
- Überprüfen Sie die ExtraHop Recordstore Checkliste nach der Bereitstellung und konfigurieren Sie zusätzliche Recordstore-Einstellungen.