Deploy the ExtraHop Explore Appliance in Azure

Published: 2019-02-11

In this guide, you will learn how to deploy an ExtraHop Explore virtual appliance in a Microsoft Azure environment and join multiple Explore appliances to create an Explore cluster.

System requirements

Your environment must meet the following requirements to deploy a virtual Explore appliance:

- An Explore appliance product key
- An Azure storage account
- A Linux, Mac, or Windows client with the latest version of Azure CLI installed.
- The ExtraHop Explore 5100v virtual hard disk (VHD) file, available on the ExtraHop Customer Portal
- An Azure instance size that most closely matches the Explore appliance VM size, as listed below:

vCPUs	Memory	Datastore disk	Azure Instance Size
4	8 GB RAM	150 GB to 500 GB	Standard_F4s_v2
8	16 GB RAM	150 GB to 1.2 TB	Satndard_F8s_v2
16	32 GB RAM	150 GB to 2.5 TB	Standard_F16s_v2
32	64 GB RAM	150 GB to 4.1 TB	Standard_F32s_v2

Deploy the EXA 5100v

Before you begin
The procedures below assume that you do not have the required resource group, storage account, storage container, and network security group configured. If you already have these parameters configured, you can proceed to step 5 after you log into your Azure account.

1. Open a terminal application on your client and log into to your Azure account.

```
az login
```

2. Open `https://aka.ms/devicelogin` in a web browser and enter the code to authenticate, and then return to the command-line-interface.
3. Create a resource group.

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

For example, create a new resource group in the West US region.

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

4. Create a storage account.

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

For example:

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

5. View the storage account key. The value for `key1` is required for step 6.

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

For example:

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

Output similar to the following appears:

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

6. Set default Azure storage account environment variables. You can have multiple storage accounts in your Azure subscription. To select one of them to apply to all subsequent storage commands, set these environment variables. If you do not set environment variables you will always have to specify `--account-name` and `--account-key` in the commands in the rest of this procedure.

```
export AZURE_STORAGE_ACCOUNT=<storage account name>
```

```
export AZURE_STORAGE_KEY=<key1>
```

Where *<key1>* is the storage account key value that appears in step 5.

For example:

```
export AZURE_STORAGE_ACCOUNT=exampleSA
```

```
export AZURE_STORAGE_KEY=CORuU8mTcxLxq0bbszhZ4RKTB93CqLpjZdAhCrNJugAor
AyvJjhGmBSedjYPmnzXPikSRigd5T5/YGYBoIzxNg==
```

7. Create a storage container.

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

For example:

```
az storage container create --name exampleSC
```

8. Upload the Explore appliance VHD file to the blob storage.

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

For example:

```
az storage blob upload --container-name exampleSC --type page
--name explore_appliance.vhd --file /Users/admin/Downloads/extrahop-
exa-5100v-azure-7.2.0.5000.vhd --validate-content
```

9. Retrieve the blob URI. You need the URI when you create the managed disk in the next step.

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

For example:

```
az storage blob url --container-name exampleSC --name
 explore_appliance.vhd
```

Output similar to the following appears:

```
https://exampleSA.blob.core.windows.net/exampleSC/explore_appliance.vhd
```

10. Create a managed disk, sourcing the Explore VHD file.

```
az disk create --resource-group <resource group name> --location <Azure
 region>
--name <disk name> --sku Premium_LRS --source <blob uri> --size-gb <size
 gb>
```

Where `storage SKU` specifies the type of disk and desired replication pattern. For example, `Premium_LRS`, `StandardSSD_LRS`, or `Standard_LRS`.

For example:

```
az disk create --resource-group exampleRG --location westus
--name exampleDisk --sku Standard_LRS --source https://
exampleSA.blob.core.windows.net/exampleSC/explore_appliance.vhd
--size-gb 200
```

11. Create the VM and attach the managed disk. This command creates the Explore appliance VM with a default network security group and private IP address.

```
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>
```

For example:

```
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. Log into the Azure portal, https://portal.azure.com, and configure the networking rules for the appliance. The network security group must have the following rules configured:

Table 1: Inbound Port Rules

Name	Port	Protocol
EXA	9443	TCP
HTTPS	443	TCP
SSH	22	TCP

Table 2: Outbound Port Rules

Name	Port	Protocol
EXA	9443	ANY
HTTPS	443	TCP
SSH	22	TCP

13. Repeat steps 10 - 12 to deploy additional Explore appliances to create your Explore cluster.

> **Important:** Do not create a copy of an existing ExtraHop virtual machine to deploy a new instance. Always start by creating a new managed disk from the original VHD file.

Next steps

Open a web browser and log into the Admin UI on the Explore appliance through the configured IP address. The default login name is `setup` and the password is `default`.

Complete the following procedures:

- Register your ExtraHop appliance
- Create an Explore cluster
- Connect the Discover and Command appliances to Explore appliances
- Send record data to the Explore appliance
- Review the Explore Post-deployment Checklist and configure additional Explore appliance settings.