Deploy an ExtraHop sensor in Azure

Published: 2022-07-15

The following procedures explain how to deploy an ExtraHop Discover virtual appliance in a Microsoft Azure environment. You must have experience administering in an Azure environment to complete these procedures.

Before you begin

- You must have experience deploying virtual machines in Azure within your virtual network infrastructure. To ensure that the deployment is successful, make sure you have access to, or the ability to create the required resources. You might need to work with other experts in your organization to ensure that the necessary resources are available.
- You must have a Linux, Mac, or Windows client with the latest version of Azure CLI installed.
- You must have the ExtraHop virtual hard disk (VHD) file, available on the ExtraHop Customer Portal. Extract the VHD file from the downloaded .zip archive file.
- You must have an ExtraHop product key.

Important: If your deployment includes a console, the following workflow ensures the best performance for initial device synchronization. First, connect all sensors to the console, then configure network traffic forwarding to the sensors.

System requirements

The table below shows the environmental parameters that you need to configure, or might have already configured in your Azure environment to successfully deploy your ExtraHop virtual sensor.

Parameter	Description
Azure account	Provides access to your Azure subscriptions.
Resource Group	A container that holds related resources for the ExtraHop sensor.
Location	The geographic region where the Azure resources are located to sustain your virtual sensor.
Storage account	The Azure storage account contains all of your Azure Storage data objects, including blobs and disks.
Blob storage container	The storage container where the ExtraHop sensor image is stored as a blob.
Managed disk	The disk required for ExtraHop sensor data storage. Specify the StandardSSD_LRS storage SKU when you create the disk.
Network security group	The network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from the ExtraHop sensor.
Azure VM instance size	An Azure instance size that most closely matches the sensor VM size, as follows: • **EDA 1000v:** Standard_DS2_v2 (2 vCPU and 7 GiB RAM)

Parameter	Description
	• **Reveal(x) EDA 1100v:** Standard_A4_v2 (4 vCPU and 8 GiB RAM) • **EDA 2000v:** Standard_DS4_v2 (8 vCPU and 28 GiB RAM) • **EDA 6100v:** Standard_D16_v3 (16 vCPU and 64 GiB RAM)
Optional Packet Capture Disk	(Optional) A storage disk for deployments that include precision packet capture. Specify the Standard_LRS storage SKU when you create and add the disk. • For the EDA 1000v, 1100v, and 2000v you can add a disk with up to 250 GB capacity. • For the EDA 6100v, you can add a disk with up to 500 GB capacity.
Public or private IP address	The IP address that enables access to the ExtraHop system.

Deploy the sensor

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 6 after you log in to your Azure account to set Azure environment variables.

1. Open a terminal application on your client and log in 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.

   PowerShell

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

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

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

   For example:

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

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

   Tip:
   - Set environment variables in the Windows command interpreter (cmd.exe) with the following syntax:

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

   - Set environment variables in the Linux command-line interface with the following syntax:

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

7. Create a storage container.

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

   For example:

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

8. Upload the ExtraHop 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 extrahop.vhd --file /Users/admin/Downloads/extrahop-eda-1000v-
azure-7.4.0.5000.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 extrahop.vhd
```

Output similar to the following appears:

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

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

```
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>
```

Specify the following disk size for the `--size-gb` parameter:

Sensor	Disk Size (GiB)
EDA 1000v	61
EDA 1100v - Reveal(x)	61
EDA 2000v	276
EDA 6100v	1000

For example:

```
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
```

Important: Steps 11 through 16 are required to configure the network interfaces for the EDA 6100v. If you are deploying the EDA 1000v, EDA 1100v, or EDA 2000v, proceed to **step 17**.

11. (6100v only) Create a virtual network.

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

For example:

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

12. (6100v only) Create the management subnet.

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

For example:

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

13. (6100v only) Create the monitoring (ingest) subnet.

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

For example:

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

14. (6100v only) Create the management network interface.

```
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
```

For example:

```
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. (6100v only) Create the monitoring (ingest) network interface.

```
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
```

For example:

```
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. (6100v only) Create the 6100v VM. This command creates the EDA 6100v sensor VM with the configured network interfaces.

```
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 ""
```

For example:

```
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 ""
```

After the EDA 6100v is created, proceed to step 18.

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

```
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>
```

For example:

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

18. Log in to the Azure portal through 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
HTTPS	443	TCP
RPCAP	2003	TCP
RPCAP	2003-2034	UDP
SSH	22	TCP

Table 2: Outbound Port Rules

Name	Port	Protocol
DNS	53	UDP
HTTPS	443	TCP
RPCAP	2003	TCP
SSH	22	TCP

(Optional) Add a disk for precision packet captures

If your sensor is licensed for precision packet capture, you must add a dedicated storage disk on the virtual machine to store the packets.

1. Run the following command to add a new disk:

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

   For example:

```
az vm disk attach --new --name packetstore --resource-group exampleRG --
size-gb 40 --sku Standard_LRS --vm-name exampleVM
```

2. Configure packet capture.

Next steps

- Open a web browser and navigate to the ExtraHop system through the configured management IP address. Accept the license agreement and then log in. The default login name is `setup` and the password is `default`. Follow the prompts to enter the product key, change the default setup and shell user account passwords, connect to ExtraHop Cloud Services, and connect to a console.
- After the sensor is licensed, and you have verified that traffic is detected, complete the recommended procedures in the post-deployment checklist.