Deploy the ExtraHop Discover Appliance in Azure

Published: 2018-11-09

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.

System requirements

Your environment must meet the following requirements to deploy a virtual Discover appliance in Azure:

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

Appliance	Azure Instance Size
EDA 1000v	Basic_A3 or Standard_DS2
EDA 1100v - Reveal(x)	Standard_A4_v2
EDA 2000v	Basic_A4 or Standard_DS4
EDA 6100v	Standard_D16_v3

Important: If you want to deploy more than one ExtraHop virtual appliance, create the new instance with the original deployment package or clone an existing instance that has never been started.

Deploy the Discover appliance

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 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 5.

```
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 Discover 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 discover_appliance.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
 discover_appliance.vhd
```

Output similar to the following appears:

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

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

```
az disk create --resource-group <resource group name> --location <Azure
 region>
--name <disk name> --sku <storage SKU> --source <blob uri> --size-gb
 <size in GB>
```

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

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

Appliance	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 Standard_LRS --source https://
exampleSA.blob.core.windows.net/exampleSC/discover_appliance.vhd
--size-gb 61
```

Note: 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. 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. 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. 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. Create the management network interface.

```
az network nic create --resource-group <resource group name> --name
 <network interface name>
        --public-ip-address <Name or ID of existing public IP address> --
vnet-name <virtual network
        name> --subnet <management subnet name> --accelerated-networking
 true
```

For example:

```
az network nic create --resource-group exampleRG --name 6100-mgmt-nic --
public-ip-address
        '' --vnet-name example-vnet --subnet example-mgmt-subnet --
accelerated-networking true
```

15. Create the monitoring (ingest) network interface.

```
az network nic create --resource-group <resource group name> --name
 <ingest network interface
        name> --public-ip-address <Name or ID of existing public IP
 address> --vnet-name <virtual
        network name> --subnet <ingest subnet name> --private-ip-address
 <static private IP address>
```

```
        --accelerated-networking true
```

For example:

```
az network nic create --resource-group exampleRG --name 6100-ingest1-nic
        --public-ip-address '' --vnet-name green-vnet --subnet example-
ingest1-subnet
        --private-ip-address 10.0.2.100 --accelerated-networking true
```

16. Create the 6100v VM. This command creates the Discover 6100v appliance 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 Discover appliance VM with a default network security group and dynamic public IP address.

```
az vm create --resource-group <resource group name>
--name <vm name> --os-type linux --attach-os-disk <disk name> --size
 <azure machine size>
```

For example:

```
az vm create --resource-group exampleRG --name exampleVM --os-type linux
--attach-os-disk exampleDisk --size Standard_D16_v3
```

18. 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
HTTPS	443	TCP
RPCAP	2003	TCP
RPCAP	2003-2034	UDP
SSH	22	TCP

Table 2: Outbound Port Rules

Name	Port	Protocol
HTTPS	443	TCP
RPCAP	2003	TCP

Name	Port	Protocol
SSH	22	TCP

Next steps

- Open a web browser and navigate to the ExtraHop Web UI through the configured IP address. Accept the license agreement and then log in. The default login name is `setup` and the password is `default`. Enter the product key to license the appliance.
- Configure an Azure virtual network TAP for the EDA 6100v.
- After the appliance is licensed, and you have verified that traffic is detected, complete the recommended procedures in the post-deployment checklist.

Configure an Azure virtual network TAP for the EDA 6100v

To optimize performance, we recommend that you forward your virtual machine traffic through an Azure virtual network TAP (vTAP). Connect the vTAP to the virtual machines that you want to monitor and then forward that traffic through the vTAP to your EDA 6100v.

For more information about configuring an Azure virtual network TAP, see the following Microsoft resource.

Configure your EDA 6100v with the following network settings.

1. Log into the Admin UI on your Discover appliance.
2. In the Network Settings section, click **Connectivity**.
3. Click **Interface 1**.
4. From the Interface Mode drop-down, select **Management Port**.
5. Click **Save**.
6. Click **Interface 2**.
7. From the Interface Mode drop-down, select **Management Port + RPCAP/ERSPAN/VXLAN Target**.
8. In the IPv4 Address field, specify the static IP address that matches the IP address of the Azure virtual tap.
9. Configure any other settings that are required for your network, and then click **Save**.