Deploy an ExtraHop sensor on Azure

Published: 2025-01-16

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

An ExtraHop virtual sensor can help you to monitor the performance of your applications across internal networks, the public internet, or a virtual desktop interface (VDI), including database and storage tiers. The ExtraHop system can monitor application performance across geographically distributed environments, such as branch offices or virtualized environments through inter-VM traffic.

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: To ensure the best performance for initial device synchronization, connect all sensors to the console and then configure network traffic forwarding to the sensors.

System requirements

You must configure the following environmental parameters in Azure to deploy your ExtraHop virtual sensor:

- An Azure account.
- A Resource Group that holds related resources for the ExtraHop sensor.
- A geographic region where the Azure resources are located to sustain your virtual sensor.
- An Azure storage account that contains all of your Azure Storage data objects, including blobs and disks.
- A storage container where the ExtraHop sensor image is stored as a blob.
- A Standard_LRS storage SKU disk or four StandardSSD_LRS storage SKU disks to store ExtraHop sensor data.
- A network security group that contains security rules that allow or deny inbound network traffic to, or outbound network traffic from the ExtraHop sensor.
- A public or private IP address that enables access to the ExtraHop system.

VM requirements

You must provision an Azure instance size that meets the following requirements.

Sensor	Instance Type
EDA 1100v	Standard_A4_v2 (4 vCPU and 8 GiB RAM)
EDA 6100v	Standard_D16_v3 (16 vCPU and 64 GiB RAM)
EDA 6370v	Standard_D48s_v5 (48 vCPUs and 192 GiB RAM)

Precision packet capture disk requirements

If your deployment includes precision packet capture, you must configure a packetstore disk that meets the following requirements.

Sensor	Disk storage SKU	Maximum size
EDA 1100v	Standard_LRS	256 GiB
EDA 6100v	Standard_LRS	512 GiB
EDA 6370v	Standard_LRS	512 GiB

Note: Do not add a precision packet capture disk to EDA 6370v sensors if the Packet Forensics module is enabled; instead, add a packet forensics disk.

Packet Forensics disk requirements

If your deployment includes global packet capture with the Packet Forensics module, you must configure packetstore disks that meet the following requirements.

Sensor	Disk storage SKU	Disk size (for each disk)	Number of disks
EDA 6370v	StandardSSD_LRS	8192 GiB	4

Note: EDA 1100v and EDA 6100v sensors do not support the Packet Forensics module.

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. Sign into Azure through the Azure CLI.

   For information, see the Microsoft documentation website.
2. 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
   ```
3. 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
   ```

4. View the storage account key. The value for `key1` is required to set the default Azure storage account environment variables.

```
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=="
 }
]
```

5. 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 you viewed in the previous step.

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>
```

6. Create a storage container.

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

For example:

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

7. 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-1100v-
azure-7.4.0.5000.vhd --validate-content
```

8. View the blob URI. The URI is required to create the managed disk.

```
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
```

9. 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 1100v - RevealX	61
EDA 6100v	1000
EDA 6370v	1400

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
```

10. Create the network environment and VM for the EDA 6100v sensor.

Note: Complete these steps only if you are configuring an EDA 6100v sensor.

a) 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
```

b) 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
```

c) 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
```

d) 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
```

e) 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
```

f) 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 ""
```

g) 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 ""
```

11. Create the network environment and VM for the EDA 6370v sensor.

Important: Complete these steps only if you are configuring an EDA 6370v sensor.

a) 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
```

b) 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
```

c) 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 6370-mgmt-
nic --vnet-name example-vnet --subnet example-mgmt-subnet --location
 westus --accelerated-networking true
```

d) Create the 6370v VM. This command creates the EDA 6370v 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>
 --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 6370-mgmt-nic --size
 Standard_D48s_v5 --public-ip-address ""
```

12. Create the EDA 1100v VM and attach the managed disk.

Important: Complete this step only if you are configuring an EDA 1100v sensor. 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
```

13. 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

Add a disk for precision packet capture

If your sensor is licensed for precision packet capture, you must add a dedicated storage disk on the VM 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 packetcap --resource-group exampleRG --
size-gb 512 --sku Standard_LRS --vm-name exampleVM
```

Note: See Precision packet capture disk requirements for sizing requirements.

2. Configure packet capture.

Configure the sensor

Before you begin

Before you can configure the sensor, you must have already configured a management IP address.

1. View the ID of the sensor VM.

```
az vm show --resource-group <resource group name> --name <vm name>
```

For example:

```
az vm show --resource-group exampleRG --name exampleVM
```

Record the value of the `vmId` field.

2. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

   The default login name is `setup` and the password is the value of the `vmId` field you recorded in the previous step.

3. Accept the license agreement and then log in.
4. 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 an ExtraHop console.

Next steps

After the system is licensed, and you have verified that traffic is detected, complete the recommended procedures in the Sensor and console post-deployment checklist.

Add disks for Packet Forensics

If your deployment includes global packet capture with the Packet Forensics module, you must add dedicated storage disks on the VM 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 StandardSSD_LRS --vm-
name <vm_name>
```

For example:

```
az vm disk attach --new --name packetstore1 --resource-group exampleRG --
size-gb 8192 --sku StandardSSD_LRS --vm-name exampleVM
```

Note: Repeat this step for each disk you want to add. See Packet Forensics disk requirements for sizing requirements.

2. Configure packet capture.