Deploy an ExtraHop packetstore in Azure

Published: 2025-01-29

The following procedures explain how to deploy an ExtraHop virtual packetstore 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.
- Azure creates a temporary disk that appears on the Disks page after the main datastore disk is created and the system is rebooted. This disk is not intended for your sensor or packetstore. You can ignore this disk.

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 packetstore.

Parameter	Description
Azure account	Provides access to your Azure subscriptions.
Resource Group	A container that holds related resources for the ExtraHop packetstore.
Location	The geographic region where the Azure resources are located to sustain your virtual packetstore.
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 packetstore image is stored as a blob.
Managed disk	The disk required for ExtraHop packetstore data storage.
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 packetstore.
Azure VM instance size	An Azure instance size that most closely matches the sensor VM size, as follows: • **ETA 1150v:** Standard_D4S_v3 **Note:** For Azure deployments, some instances running older NICs might not support High-

Parameter	Description
	Performance ERSPAN/VXLAN/GENEVE Target mode.
Public or private IP address	The IP address that enables access to the ExtraHop system.

Deploy the ETA 1150v

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.

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 account 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-eta-
   azure-7.2.0.5000.vhd --validate-content
   ```

9. Retrieve the blob URI. You will 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 example 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 <storage SKU> --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`.

You can configure the disk size (`--size-gb`) between 50 GB and 2 TB

For example:

```
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 60
```

11. Create the VM and attach the managed disk. This command creates the packetstore 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_D4S_v3
```

12. Log in to the Azure portal through https://portal.azure.com and configure the networking rules for the packetstore. 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

Next steps

Open a web browser and 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 for the VM. You can find the `vmID` by locating the VM on https://resources.azure.com/.

Register your ExtraHop system and complete the recommended procedures in the post-deployment checklist.