

Deploy an ExtraHop recordstore in Azure

Published: 2024-07-22

The following procedures explain how to deploy a recordstore in a Microsoft Azure environment and join multiple recordstores to create a cluster. 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.

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 recordstore.

Parameter	Description
Azure account	Provides access to your Azure subscriptions.
Resource Group	A container that holds related resources for the ExtraHop recordstore.
Location	The geographic region where the Azure resources are located to sustain your virtual recordstores.
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 recordstore image is stored as a blob.
Managed disk	The disk required for ExtraHop recordstore 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 recordstore.
Azure VM instance size	An Azure instance size that most closely matches the Explore recordstore VM size. See the table below.
Public or private IP address	The IP address that enables access to the ExtraHop system.

Table 1: Azure datastore and instance sizes

vCPUs	Memory	Datastore disk	Azure Instance Size
4	8 GB RAM	150 GB to 250 GB	Standard_F4s_v2
8	16 GB RAM	150 GB to 500 GB	Standard_F8s_v2
16	32 GB RAM	150 GB to 1 TB	Standard_F16s_v2
32	64 GB RAM	150 GB to 2 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 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": "D0lda4+6U3Cf5TUAng8/GKotfX1HHJuc3yljAlU+aktRAf4/
      KwVQUuAUUnhdrw2yg5Pba5FpZn6oZYvR0ncnT8Q=="
    }
  ]

```

- 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>
```

- Create a storage container.

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

For example:

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

- 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-exa-5100v-
azure-7.2.0.5000.vhd --validate-content
```

- 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
```

- 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`.

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 200
```

- Create the VM and attach the managed disk. This command creates the recordstore 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
```

- 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 2: Inbound Port Rules

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

Table 3: Outbound Port Rules

Name	Port	Protocol
DNS	53	UDP
EXA	9443	ANY
HTTPS	443	TCP
SSH	22	TCP

13. Repeat steps 10 - 12 to deploy additional recordstores to create your 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 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 `default`.

Complete the following procedures:

- [Register your ExtraHop system](#) 
- [Create a recordstore cluster](#) 
- [Connect the console and sensors to ExtraHop recordstores](#) 
- [Send record data to the Explore appliance](#) 
- Review the [Recordstore Post-deployment Checklist](#)  and configure additional recordstore settings.