Deploy the ExtraHop Trace Appliance in Azure

Published: 2018-11-07

The following procedures explain how to deploy an ExtraHop Trace virtual appliance in a Microsoft Azure environment.

System requirements

Your environment must meet the following requirements to deploy a virtual Trace Appliance in Azure:

- An Azure storage account
- A Linux, Mac, or Windows client with the latest version of Azure CLI installed
- The ExtraHop Trace 1150v virtual hard disk (VHD) file, available on the ExtraHop Customer Portal
- A Trace appliance product key
- An Azure instance size that most closely matches the Trace appliance VM size, as listed below:

Appliance	Azure Instance Size
ETA 1150v	Standard_D2s_v4

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 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 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.

```
export AZURE_STORAGE_ACCOUNT=<storage account_name>
```

```
export AZURE_STORAGE_ACCESS_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_ACCESS_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 Trace 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 trace_appliance.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 trace_appliance.vhd
```

Output similar to the following example appears:

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

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

```
az disk create --resource-group <resource group name> --location <Azure
 region>
--name <disk name> --sku Premium_LRS --source <blob uri> --size-gb <size
 gb>
```

Where `sku` specifies the type of disk and desired replication pattern. Managed disks support only Standard_LRS and Premium_LRS. Premium_LRS has a maximum disk size of 1 TB and Standard_LRS has a maximum disk size of 4TB.

You can configure the disk size (`--size-gb`) between 50 GB and 4 TB

For example:

```
az disk create --resource-group exampleRG --location westus
--name exampleDisk --sku Standard_LRS --source https://
exampleSA.blob.core.windows.net/exampleSC/trace_appliance.vhd
--size-gb 60
```

11. Create the VM and attach the managed disk. This command creates the Trace appliance VM with a default network security group and dynamic public IP address.

```
az vm create --resource-group <resource group name> --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 --location westus --name
 exampleVM --os-type linux
--attach-os-disk exampleDisk --size Standard_D2s_v4
```

12. 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
SSH	22	TCP

Next steps

Open a web browser and log into the Admin UI on the Trace appliance through the configured public IP address. The default login name is `setup` and the password is `default`.

Complete the following recommended procedures:

- Register your ExtraHop appliance
- Configure the system time
- Configure email settings for notifications
- Connect the Discover and Command appliances to the Trace appliance