Deploy an ExtraHop sensor on Google Cloud Platform

Published: 2023-05-16

The following procedures explain how to deploy a virtual ExtraHop sensor in a Google Cloud environment. You must have experience deploying virtual machines in Google Cloud within your virtual network infrastructure.

To ensure that the deployment is successful, make sure you have access and 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.

System requirements

Your environment must meet the following requirements to deploy a virtual ExtraHop sensor in GCP:

- You must have a Google Cloud Platform (GCP) account
- You must have the ExtraHop deployment file, which is available on the ExtraHop Customer Portal.
- You must have an ExtraHop product key.
- You must have packet mirroring enabled in GCP to forward network traffic to the ExtraHop system. Packet mirroring must be configured to send traffic to nic1 (not nic0) of the ExtraHop instance. See https://cloud.google.com/vpc/docs/using-packet-mirroring.

  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.
- You must have firewall rules configured to allow DNS, HTTP, HTTPS, and SSH traffic for ExtraHop administration. See https://cloud.google.com/vpc/docs/using-firewalls.
- You must provision a GCP instance type that most closely matches the virtual sensor size, as follows:

Sensor	Recommended Instance Type
Reveal(x) EDA 1100v	n1-standard-4 (4 vCPU, 15 GB memory)

Upload the ExtraHop deployment file

1. Sign in to your Google Cloud Platform account.
2. From the navigation menu, click **Cloud Storage** > **Browser**.
3. Click the name of the storage bucket where you want to upload the ExtraHop deployment file. If you do not have a preconfigured storage bucket, create one now.
4. Click **Upload files**.
5. Browse to the `extrahop-eda-gcp-<version>.tar.gz` file you previously downloaded and click **Open**. Wait for the file to upload, and then continue to the next procedure.

Create the image

1. From the navigation menu, click **Compute Engine** > **Images**.
2. Click **Create Image** and complete the following steps:
   a) In the Name field, type a name to identify the ExtraHop sensor.
   b) From the Source drop-down list, select **Cloud Storage file**.

c) In the Cloud Storage file section, click **Browse**, locate the `extrahop-eda-gcp-<version>.tar.gz` file in your storage bucket and then click **Select**.
d) Configure any additional fields that are required for your environment.

3. Click **Create**.

Create the datastore disk

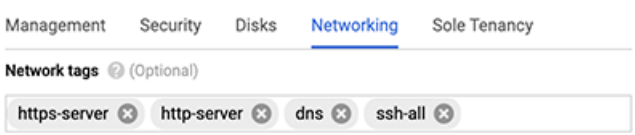
1. From the navigation menu, click **Compute Engine** > **Disks**.
2. Click **Create Disk** and complete the following steps:
   a) In the Name field, type a name to identify the ExtraHop disk.
   b) From the Type drop-down menu, select **Standard persistent disk**.
   c) In the Source type section, click **Image**.
   d) From the Source image drop-down list, select the image you created in the previous procedure.
   e) In the Size field, type `61`.
   f) Configure any additional fields that are required for your environment.
3. Click **Create**.

Create the VM instance

1. From the navigation menu, click **Compute Engine** > **VM instances**.
2. Click **Create Instance** and complete the following steps:
   a) In the Name field, type a name to identify the ExtraHop instance.
   b) From the Region drop-down list, select your geographic region.
   c) From the Zone drop-down list, select a location within your geographic zone.
   d) In the Machine configuration section, select **General Purpose** for the machine family, **N1** for the series, and **n1-standard-4 (4 vCPU, 15 GB memory)** for the machine type.
   e) In the Boot disk section, click **Change**.
   f) Click **Existing disks**.
   g) From the Disk drop-down list, select the disk you created in the previous procedure.
   h) Click **Select**.
3. Click **Advanced options**.
4. Click **Networking**.
5. In the Network tags field, type the following tag names:

   Important: Network tags are required to apply firewall rules to the ExtraHop instance. If you do not have existing firewall rules that allow this traffic, you must create the rules. See https://cloud.google.com/vpc/docs/using-firewalls.

   - `https-server`
   - `http-server`
   - `dns`
   - `ssh-all`



6. In the Network interfaces section, click the edit icon to edit the management interface.
   a) From the **Network** drop-down list, select your management network.
   b) From the **Subnetwork** drop-down list, select your management network subnet.

c) Configure any additional fields that are required for your environment.
d) Click **Done**.

7. Click **Add network interface** to configure the data capture interface.

   Important: The management interface and data capture interface must be in different Virtual Private Cloud (VPC) networks.

   a) From the **Network** drop-down list, select your network that will mirror traffic to the ExtraHop system.
   b) From the **Subnetwork** drop-down list, select your network subnet.
   c) From the **External IP** drop-down list, select **None**.
   d) Configure any additional fields that are required for your environment.
   e) Click **Done**.
8. Click **Create**.

Create an instance group

1. In the left pane on the Compute Engine page, click **Instance groups**.
2. Click **Create Instance Group**.
3. Click **New unmanaged instance group**.
4. Enter an instance group name in the **Name** field.
5. In the Network and instances section, select the network that the instance can access from the **Network** drop-down list.
6. Select the subnet from the **Subnet** drop-down list.
7. Select the sensor from the **Select VM** drop-down list.
8. Click **Create**.

Create a load balancer

1. On the Network services page, click **Load balancing**.
2. Click **Create Load Balancer**.
3. In the UDP Load Balancing section, click **Start Configuration**.
4. Select **Only between my VMs**.
5. Click **Continue**.
6. Enter a load balancer name.
7. Select your region from the **Region** drop-down list.
8. Select your network from the **Network** drop-down list.
9. In the New Backend section, select your instance group from the drop-down list.
10. Click **Health check** and then click **Create a Health Check**.
11. Enter a health check name.
12. Select **TCP** from the Protocol drop-down list.
13. Type 443 in the Port field.
14. Click **Save**.

Create a traffic mirroring policy

1. On the VPC Network page, click **Packet mirroring**.
2. Click **Create Policy**.

3. In the Define policy overview section, enter a new policy name.
4. Select your region from the **Region** drop-down list.
5. Click **Continue**.
6. Select **Mirrored source and collector destination are in the same VPC network**.
7. Select the VPC network from the **Network** drop-down list.
8. Click **Continue**.
9. Select the **Select one or more subnetworks** checkbox.
10. From the **Select subnet** drop-down list, select the checkbox next to your subnet.
11. Select the **Select individual instances** checkbox.
12. Click **Select**.
13. Select the checkbox next to the VM instance.
14. Click **Continue**.
15. Select the load balancer you created previously from the **Collector destination** drop-down list.
16. Click **Continue**.
17. Select **Mirror all traffic (default)**.
18. Click **Submit**.

Configure the sensor

After you configure an IP address for the sensor, open a web browser and navigate to the ExtraHop system through the configured IP address. Accept the license agreement and then log in. The default login name is `setup` and the password is `default`. 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.

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

Configure L3 device discovery

You must configure the ExtraHop system to discover and track local and remote devices by their IP address (L3 Discovery). To learn how device discovery works in the ExtraHop system, see Device discovery.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Device Discovery**.
4. In the Local Device Discovery section, select the **Enable local device discovery** checkbox to enable L3 Discovery.
5. In the Remote Device Discovery section, type the IP address in the IP address ranges field. You can specify one IP address or a CIDR notation, such as `192.168.0.0/24` for an IPv4 network or `2001:db8::/32` for an IPv6 network.
6. Click **Save**.