Deploy an ExtraHop sensor on Google Cloud Platform

Published: 2024-09-03

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.

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.

This installation enables you to run network performance monitoring, network detection and response, and intrusion detection on a single sensor. By adding the IDS module, you can also upload and view IDS detections.

Important: The IDS module requires the NDR module. Before you can enable the IDS module on this sensor, you must upgrade the sensor firmware to version 9.6 or later. When the upgrade completes, you can apply the new license to the sensor.

Note: If you have enabled the IDS module on this sensor, and your ExtraHop system does not have direct access to the Internet and access to ExtraHop Cloud Services, you will need to upload IDS rules manually. For more information, see Upload IDS rules to the ExtraHop system through the REST API.

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 sensor 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.

Virtual machine requirements

You must provision a GCP instance type that most closely matches your ExtraHop virtual sensor size and that meets the following module requirements.

Sensor	Modules	Recommended Instance Type	Datastore Disk Size
EDA 1100v	NDR, NPM	n1-standard-4 (4 vCPUs and 15 GB memory)	61 GB
EDA 6320v	NDR, NPM, IDS	n2-standard-32 (32 vCPUs and 128 GB memory)	1400 GB

Note: Throughput might be affected when more than one module is enabled on the sensor.

Upload the ExtraHop deployment file

1. Sign in to your Google Cloud Platform account.
2. From the navigation menu, click **Cloud Storage** > **Buckets**.
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-<module>-gcp-<version>.tar.gz` file you previously downloaded and click **Open**.

Next steps
When the file upload completes, you can create the image.

Create the image

1. From the navigation menu, click **Compute Engine** > **Images**.
2. Click **Create Image**.
3. In the Name field, type a name to identify the ExtraHop sensor.
4. From the Source drop-down list, select **Cloud Storage file**.
5. 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**.
6. Configure any additional fields that are required for your environment.
7. Click **Equivalent Code**.
   A panel opens on the right.
8. In the Equivalent code panel, click **Copy**.
9. Click **Run in Cloud Shell**.
   The copied text displays at the prompt.
10. Add this option to the end of the command sequence:
    `--guest-os-features=GVNIC`
11. Press ENTER.

Next steps
After the command runs, close Cloud Shell, and then click **Cancel**. Clicking **Cancel** does not cancel the creation of the image through Cloud Shell.

Create the datastore disk

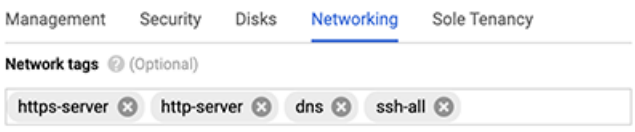
1. In the left pane on the Compute Engine page, click **Disks**.
2. Click **Create Disk**.
3. In the Name field, type a name to identify the ExtraHop datastore disk.
4. From the **Disk source type** drop-down list, select **Image**.
5. From the Disk type drop-down list, select **Standard persistent disk**.
6. From the Source image drop-down list, select the image that you previously created.
7. In the Size field, type a value, in GB, for the disk size.

   For more information on selecting a disk size, see Virtual machine requirements.
8. Configure any additional fields that are required for your environment.
9. Click **Create**.

Create the VM instance

1. In the left pane on the Compute Engine page, **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.

      For more information on selecting a machine type, see Virtual machine requirements.
   e) In the Boot disk section, click **Change**.
   f) Click **Existing disks**.
   g) From the Disk drop-down list, select the disk that you previously created.
   h) Click **Select**.
3. Click **Advanced options**.
4. Click **Networking**.
5. In the Network tags field, type the following tag names, separating each name with a space:
   - `https-server`
   - `http-server`
   - `dns`
   - `ssh-all`



> **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. For more information, see https://cloud.google.com/vpc/docs/using-firewalls.

6. In the Network interfaces section, click 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 a 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 IPv4 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. In the Name field, type an instance group name.
5. From the Network drop-down list, select the network that the instance can access.
6. From the Subnet drop-down list, select your network subnet.
7. From the Select VM drop-down list, select your sensor.
8. Click **Create**.

Create a load balancer

1. From the navigation menu, click **Network services** > **Load balancing**.

   Note: If the Network services menu is not in your navigation menu, click **More Products**.

2. Click **Create Load Balancer**.
3. In the Network Load Balancer (UDP/Multiple protocols) section, click **Start Configuration**.
4. Under Select a Load balancer type, click **UDP load balancer**.
5. Under Internet facing or internal only, select **Only between my VMs**.
6. Under Backend type, keep the default value (Backend Service).
7. Click **Continue**.
8. In the Load Balancer name field, type a load balancer name.
9. From the Region drop-down list, select your geographic region.
10. From the Network drop-down list, select your network.
11. In the Backends section, from the Instance group drop-down list, select your instance group.
12. Click **Health check** and then click **Create a Health Check**.
13. In the Name field, type a health check name.
14. From the Protocol drop-down list, select **TCP**.
15. In the Port field, type 443.
16. Click **Save**.

Create a traffic mirroring policy

1. From the navigation menu, click **VPC Network** > **Packet mirroring**.
2. Click **Create Policy**.
3. In the Policy name field, type a new policy name.
4. From the Region drop-down list, select your geographic region.
5. Click **Continue**.
6. Select **Mirrored source and collector destination are in the same VPC network**.
7. From the Network drop-down list, select the VPC network.
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. Click **Continue**.
12. Select the checkbox next to the VM instance.
13. Click **Continue**.
14. From the **Collector destination** drop-down list. select the load balancer that you previously created.
15. Click **Continue**.
16. Select **Mirror all traffic (default)**.
17. Click **Submit**.

Configure the sensor

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

1. 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 VM instance ID.
2. Accept the license agreement and then log in.
3. 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 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**.