


Deploy an ExtraHop sensor on AWS


Published: 2024-04-19

The following procedures explain how to deploy a virtual ExtraHop sensor in an Amazon Web Services (AWS) environment. You must have experience deploying virtual machines in AWS 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.

 **Important:** 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](#).

After you deploy the sensor in AWS, configure [AWS traffic mirroring](#) or [remote packet capture](#) (RPCAP) to forward traffic from remote devices to your sensor. AWS traffic mirroring is configurable for all instance sizes and is the preferred method of sending AWS traffic to the EDA 6100v and 8200v sensor.

 **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.

System requirements

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

- You must have an AWS account.
- You must have access to the Amazon Machine Image (AMI) of the ExtraHop sensor.
- You must have an ExtraHop sensor product key.
- You can optionally configure a storage disk for deployments that include precision packet capture. Refer to the AWS documentation for instructions to add a disk.
 - For the EDA 1100v add a disk with up to 250 GB capacity.
 - For the EDA 6100v and 8200v, add a disk with up to 500 GB capacity.

Virtual machine requirements

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

Sensor	Modules	Recommended Instance Type	Disk Size
EDA 1100v	EDA	c5.xlarge (4 vCPUs and 8 GB RAM)	61 GB
EDA 6320v	EDA + IDS	m5.8xlarge (32 vCPUs, 128 GB RAM)	1400 GB

Sensor	Modules	Recommended Instance Type	Disk Size
EDA 6100v	EDA	m5.4xlarge (16 vCPUs and 64 GB RAM) c5.9xlarge (36 vCPUs and 72 GB RAM) *	1000 GB
EDA 8200v	EDA	c5n.9xlarge (36 vCPUs and 96 GB RAM)	2000 GB

* Recommended when the EDA 6100v cannot be deployed in the same cluster placement group as the monitored traffic. The c5.9xlarge instance has a higher cost, but is more resilient in environments where data feed fidelity is critical.



Note: Whenever possible, locate the sensor within the same cluster placement group as the devices that are forwarding traffic. This best practice optimizes the quality of feed that the sensor receives.



Important: AWS enforces a limit of 10 sessions for Virtual Private Cloud (VPC) traffic mirroring; however, the session limit can be increased for sensors running on a c5 dedicated host. We recommend the c5 dedicated host for EDA 8200v and EDA 6100v instances that require a larger session limit. Contact AWS support to request the session limit increase.

Port requirements

The following ports must be open for ExtraHop AWS instances.


Port	Description
TCP ports 22, 80, and 443 inbound to the ExtraHop system	These ports are required to administer the ExtraHop system.
TCP port 443 outbound to ExtraHop Cloud Services	Add the current ExtraHop Cloud Services IP address. For more information, see Configure your firewall rules .
UDP port 53 outbound to your DNS server	UDP port 53 must be open so the sensor can connect to the ExtraHop licensing server.
(Optional) TCP/UDP ports 2003-2034 inbound to the ExtraHop system from the AWS VPC	If you are not configuring AWS traffic mirroring , you must open a port (or a range of ports) for the packet forwarder to forward RPCAP traffic from your AWS VPC resources. For more information, see Packet Forwarding with RPCAP .


Create the ExtraHop instance in AWS

The Amazon Machine Images (AMIs) for ExtraHop sensors are available in the [AWS Marketplace](#). You can create an ExtraHop instance in AWS from one of these AMIs.

1. Sign in to AWS with your username and password.
2. Click **EC2**.
3. In the left navigation panel, under Images, click **AMIs**.
4. Above the table of AMIs, change the Filter from **Owned by Me** to **Public Images**.
5. In the filter box, type `ExtraHop` and then press ENTER.

6. Select the checkbox next to the appropriate ExtraHop sensor AMI and click **Launch instance from AMI**.
For more information on selecting a virtual sensor, see [Virtual machine requirements](#).
7. In the Name field, type a name to identify the ExtraHop sensor.
8. In the Application and OS Images (Amazon Machine Image) section, verify the selected AMI.
9. In the Instance Type section, verify the selected instance type.
10. In the Key pair (login) section, select an existing key pair or create a new key pair.
11. In the Network settings section, click **Edit**.
12. From the VPC drop-down list, select a VPC.
13. From the Subnet drop-down list, select a subnet.
14. Optional: If you plan to add additional network interfaces, from the Auto-assign public IP drop-down list, select Disable.
15. Click **Create security group** or **Select existing security group**.
If you choose to edit an existing group, select the group you want to edit. If you choose to create a new group, enter a Security group name and Description.
16. In the Inbound Security Group Rules section, configure any necessary rules.
For more information on which port requirements for ExtraHop systems, see [Port requirements](#).
 - a) From the Type drop-down list, select a protocol type.
 - b) In the Port range field, type the port number.
 - c) For each additional port needed, click **Add security group rule**, and then configure the Type and Port range, as needed.
17. Optional: To add additional network interfaces into an instance in a Virtual Private Cloud (VPC), click **Advanced network configuration**.
 - a) Click **Add network interface**.
 - b) From the Network interface drop-down list, select the network interface that you want to attach to the instance.
 - c) From the Subnet drop-down list, select a subnet.

 **Note:** If you have more than one interface, make sure that each interface is on a different subnet.
18. In the Configure storage section, change the GiB field for the root volume and select **General Purpose SSD (gp3)**.
For more information on selecting a disk size for storage capacity, see [Virtual machine requirements](#).
19. Optional: Click **Add new volume** to create a volume for a precision packet capture disk.
20. Click **Advanced details** to expand additional settings.
21. Optional: Click the IAM role drop-down list and select an IAM role.

 **Note:** If you are deploying an ExtraHop flow sensor, this should be the IAM role created in the [Deploy an ExtraHop Flow Sensor with AWS](#) guide.
22. From the Shutdown behavior drop-down list, select **Stop**.
23. From the Termination protection drop-down list, select **Enable**.
24. Review the AMI details, instance type, and security group information, and then click **Launch Instance**.
25. Click **View all instances** to return to the AWS Management Console.
From the AWS Management Console, you can view your instance on the Initializing screen. Under the table, on the Description tab, you can find the IP address or hostname for the ExtraHop system that is accessible from your environment.

Next steps

- [Register your ExtraHop system](#)

- (Recommended) Configure [AWS traffic mirroring](#) to copy network traffic from your EC2 instances to a high-performance ERSPAN/VXLAN/GENEVE interface on your sensor.



Tip: If your deployment requires more than 15 Gbps of throughput, divide your traffic mirroring sources across two high-performance ERSPAN/VXLAN/GENEVE interfaces on the EDA 8200v.

- (Optional) [Forward GENEVE-encapsulated traffic from an AWS Gateway Load Balancer](#).
- [Configure the sensor.](#)
- Review the [Sensor and console post-deployment checklist](#).

Create a traffic mirror target

Complete these steps for each Elastic network interface (ENI) you created.

1. In the AWS Management Console, in the top menu, click **Services**.
2. Click **Networking & Content Delivery > VPC**.
3. In the left pane, under Traffic Mirroring, click **Mirror Targets**.
4. Click **Create traffic mirror target**.
5. Optional: In the Name tag field, type a descriptive name for the target.
6. Optional: In the Description field, type a description for the target.
7. From the Target type drop-down list, select Network Interface.
8. From the Target drop-down list, select the ENI you previously created.
9. Click **Create**.

Note the Target ID for each ENI. You will need the ID when you create a traffic mirror session.

Create a traffic mirror filter

You must create a filter to allow or restrict traffic from your ENI traffic mirror sources to your ExtraHop system.

We recommend the following filtering rules to help avoid mirroring duplicate frames from peer EC2 instances that are in a single VPC to the sensor.

- All outbound traffic is mirrored to the sensor, whether the traffic is sent from one peer device to another on the subnet or if the traffic is sent to a device outside of the subnet.
- Inbound traffic is only mirrored to the sensor when the traffic is from an external device. For example, this rule ensures that an app server request is not mirrored twice: once from the sending app server and once from the database that received the request.
- Rule numbers determine the order in which the filters are applied. Rules with lower numbers, such as 100, are applied first.




Important: These filters should only be applied when mirroring all of the instances in a CIDR block.

1. In the AWS Management Console, in the left pane under Traffic Mirroring, click **Mirror Filters**.
2. Click **Create traffic mirror filter**.
3. In the Name tag field, type a name for the filter.
4. In the Description field, type a description for the filter.
5. Under Network services, select the **amazon-dns** checkbox.
6. In the Inbound rules section, click **Add rule**.
7. Configure an inbound rule:
 - a) In the Number field, type a number for the rule, such as 100.
 - b) From the Rule action drop-down list, select **reject**.

- c) From the Protocol drop-down list, select **All protocols**.
 - d) In the Source CIDR block field, type the CIDR block for the subnet.
 - e) In the Destination CIDR block field, type the CIDR block for the subnet.
 - f) In the Description field, type a description for the rule.
8. In the Inbound rules sections, click **Add rule**.
9. Configure an additional inbound rule:
 - a) In the Number field, type a number for the rule, such as 200.
 - b) From the Rule action drop-down list, select **accept**.
 - c) From the Protocol drop-down list, select **All protocols**.
 - d) In the Source CIDR block field, type 0 . 0 . 0 . 0 / 0.
 - e) In the Destination CIDR block field, type 0 . 0 . 0 . 0 / 0.
 - f) In the Description field, type a description for the rule.
10. In the Outbound rules section, click **Add rule**.
11. Configure an outbound rule:
 - a) In the Number field, type a number for the rule, such as 100.
 - b) From the Rule action drop-down list, select **accept**.
 - c) From the Protocol drop-down list, select **All protocols**.
 - d) In the Source CIDR block field, type 0 . 0 . 0 . 0 / 0.
 - e) In the Destination CIDR block field, type 0 . 0 . 0 . 0 / 0.
 - f) In the Description field, type a description for the rule.
12. Click **Create**.

Create a traffic mirror session

You must create a session for each AWS resource that you want to monitor. You can create a maximum of 500 traffic mirror sessions per sensor.

 **Important:** To prevent mirror packets from being truncated, set the traffic mirror source interface MTU value to 54 bytes less than the traffic mirror target MTU value for IPv4 and 74 bytes less than the traffic mirror target MTU value for IPv6. For more information about configuring the network MTU value, see the following AWS documentation: [Network Maximum Transmission Unit \(MTU\) for Your EC2 Instance](#).

1. In the AWS Management Console, in the left pane, under Traffic Mirroring, click **Mirror Sessions**.
2. Click **Create traffic mirror session**.
3. In the Name tag field, type a descriptive name for the session.
4. In the Description field, type a description for the session.
5. From the Mirror source drop-down list, select the source ENI.
The source ENI is typically attached to the EC2 instance that you want to monitor.
6. From the Mirror target drop-down list, select the traffic mirror target ID generated for the target ENI.
7. In the Session number field, type 1.
8. For the VNI field, leave this field empty.
The system assigns a random unique VNI.
9. For the Packet length field, leave this field empty.
This mirrors the entire packet.
10. From the Filter drop-down list, select the ID for the traffic mirror filter you created.
11. Click **Create**.

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](#).