

Deploy an ExtraHop sensor in AWS

Published: 2024-06-27

The following procedure guides you through the deployment process of the sensor AMI to monitor your Amazon Web Services (AWS) environment.

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 sensors.


 **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:

- An AWS account
- Access to the Amazon Machine Image (AMI) of the ExtraHop sensor
- The sensor product key
- An AWS instance type that most closely matches the virtual ExtraHop sensor size, as follows:

Sensors	Recommended Instance Type
EDA 1000v	m5.large (2 vCPU and 8 GB RAM)
Reveal(x) EDA 1100v	c5.xlarge (4 vCPU and 8 GB RAM)
EDA 2000v	c5.2xlarge (8 vCPU and 16 GB RAM)
EDA 6100v	m5.4xlarge (16 vCPU and 64 GB RAM) c5.9xlarge (36 vCPU and 72 GB RAM)
Reveal(x) EDA 8200v	c5n.9xlarge (36 vCPU and 96 GB RAM)

 **Important:** AWS enforces a session limit of 10 sessions for 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.

- (Optional) A storage disk for deployments that include precision packet capture. Refer to the AWS documentation for instructions to add a disk.
 - For the EDA 1000v, 1100v, and 2000v add a disk with up to 250 GB capacity.
 - For the EDA 6100v and 8200v, add a disk with up to 500 GB capacity.

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 **Private 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**.
7. Select a supported instance type for the sensor you are deploying.
8. Click **Next: Configure Instance Details**.
9. Click the **Network** drop-down list and select one of the VPCs for your organization.
10. From the Shutdown behavior drop-down list, select **Stop**.
11. Click the **Protect against accidental termination** checkbox.
12. Click the **IAM role** drop-down list and select an IAM role.



Note: If you are deploying a flow sensor (EFC 1291v), this should be the IAM role created in the [Deploy an ExtraHop Flow Sensor with AWS](#) guide.

13. If you launched into a VPC and want to have more than one interface, scroll down to the **Network Interfaces** section and click **Add Device** to add additional interfaces to the instance.



Note: If you have more than one interface, make sure that each interface is on a different subnet.

14. On the **Configure Instance Details** page, click **Next: Add Storage**. The recommended storage capacities are listed below.

Sensor	Storage Capacity
EDA 1000v	61 GiB
EDA 1100v	61 GiB
EDA 2000v	276 GiB
EDA 6100v	1000 GiB
EDA 8200v	2000 GiB

15. Change the **Size (GiB)** field for the root volume to the value recommended in the table above for your sensor. From the **Volume Type** drop-down list, select **General Purpose SSD (gp2)**.
16. Optional: Add a new volume for a precision packet capture disk.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-02f9654a333fc2619	61	General Purpose SSD (gp2)	183 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit)	250	General Purpose SSD (gp2)	750 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

17. Click **Next: Tag Instance**.
18. In the **Value** field, enter a name for the instance.
19. Click **Next: Configure Security Group**.
20. On the **Configure Security Group** page, follow the procedure below with the table that follows to create a new security group or add ports to an existing group. If you already have a security group with the required ports for ExtraHop, you can skip this step.
 - a) Select either **Create a new security group** or **Select an 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**.
 - b) Click the **Type** drop-down list, and select a protocol type. Type the port number in the **Port Range** field.
 - c) For each additional port needed, click the **Add Rule** button. Then click the **Type** drop-down list, select a protocol type, and type the port number in the **Port Range** field.

The following ports need to be open for the ExtraHop AWS instance:

- **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](#).
- **(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](#).
- **UDP port 53 outbound to your DNS server:** UDP port 53 must be open so the sensor can connect to the ExtraHop licensing server.

21. Click **Review and Launch**.
22. Select **Make General Purpose (SSD)...** and click **Next**.



Note: If you select **Make General Purpose (SSD)...**, then you will not see this step on subsequent instance launches.

23. Scroll down to review the AMI details, instance type, and security group information, and then click **Launch**.
24. In the pop-up window, click the first drop-down list and select **Proceed without a key pair**.
25. Click the **I acknowledge...** checkbox and then click **Launch Instance**.
26. Click **View 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.

27. [Register your ExtraHop system](#).

Next steps

- (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](#).
- Review the [Sensor and console post-deployment checklist](#).

Create a traffic mirror target

Complete these steps for each ENI you created.

1. Return to the AWS Management Console.
2. From the top menu, click **Services**.
3. In the Networking & Content Delivery section, click **VPC**.
4. In the left pane, under Traffic Mirroring, click **Mirror Targets**.
5. Click **Create traffic mirror target** and complete the following fields:

Option	Description
Name tag	(Optional) Type a descriptive name for the target.
Description	(Optional) Type a description for the target.

Option	Description
Target type	Select Network Interface .
Target	Select the ENI you previously created.

6. 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** and complete the following fields:

Option	Description
Name tag	Type a name for the filter.
Description	Type a description for the filter.
Network services	Select the amazon-dns checkbox.

3. In the Inbound rules section, click **Add rule** and then complete the following fields:

Option	Description
Number	Type a number for the rule, such as 100.
Rule action	Select reject from the drop-down list.
Protocol	Select All protocols from the drop-down list.
Source CIDR block	Type the CIDR block for the subnet.
Destination CIDR block	Type the CIDR block for the subnet.
Description	(Optional) Type a description for the rule.

4. In the Inbound rules section, click **Add rule** again and then complete the following fields:

Option	Description
Number	Type a number for the rule, such as 200.
Rule action	Select accept from the drop-down list.
Protocol	Select All protocols from the drop-down list.
Source CIDR block	Type 0 . 0 . 0 . 0 / 0.
Destination CIDR block	Type 0 . 0 . 0 . 0 / 0.
Description	(Optional) Type a description for the rule.


- In the Outbound rules section, click **Add rule** and then complete the following fields:

Option	Description
Number	Type a number for the rule, such as 100.
Rule action	Select accept from the drop-down list.
Protocol	Select All protocols from the drop-down list.
Source CIDR block:	Type 0 . 0 . 0 . 0 / 0.
Destination CIDR block:	Type 0 . 0 . 0 . 0 / 0.
Description	(Optional) Type a description for the rule.

- 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](#).

- In the AWS Management Console, in the left pane, under Traffic Mirroring, click **Mirror Session**.
- Click **Create traffic mirror session** and complete the following fields:

Option	Description
Name tag	(Optional) Type a descriptive name for the session.
Description	(Optional) Type a description for the session
Mirror source	Select the source ENI. The source ENI is typically attached to the EC2 instance that you want to monitor.
Mirror target	Select the traffic mirror target ID generated for the target ENI.
Session number	Type 1.
VNI	Leave this field empty.
Packet length	Leave this field empty.
Filter	From the drop-down menu, select the ID for the traffic mirror filter you created.

- Click **Create**.