Deploy the ExtraHop Discover Appliance in AWS

Published: 2022-04-21

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

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

Important: If your deployment includes a Command appliance or Reveal(x) 360, the following workflow ensures the best performance for initial device synchronization. First, connect all sensors to the Command appliance or Reveal(x) 360, then configure network traffic forwarding to the sensors.

System requirements

Your environment must meet the following requirements to deploy a virtual Discover appliance in AWS:

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

Appliance	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)

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

*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.

Important: AWS enforces a session limit of 10 sessions for VPC traffic mirroring; however, the session limit can be increased for Discover appliances 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 your vendor documentation 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

Before you begin
The Amazon Machine Images (AMIs) of ExtraHop appliances are not publicly shared. Before you can start the deployment procedure, you must send your AWS account ID to support@extrahop.com. Your account ID will be linked to the ExtraHop AMIs.

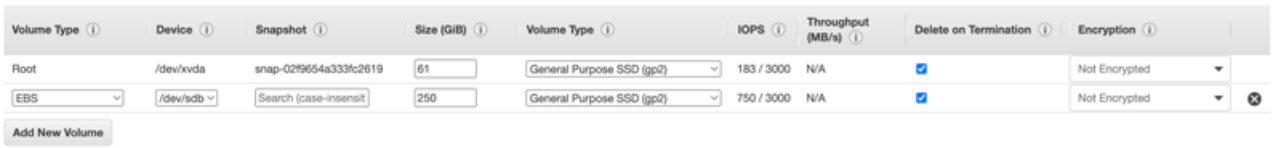
1. Sign in to AWS with your username and password.
2. Click **EC2**.
3. In the left navigation panel, under **Images**, click **AMIs**.
4. Above the table of AMIs, change the **Filter** from **Owned by Me** to **Private Images**.
5. In the filter box, type `ExtraHop` and then press ENTER.
6. Select the checkbox next to the appropriate ExtraHop Discover appliance AMI and click **Launch**.
7. Select a supported instance type for the appliance 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.
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.

Product	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.



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 Discover appliance 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 interface on your Discover appliance.

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