Deploy Reveal(x) Ultra in AWS

Published: 2024-04-02

In this guide, you will learn how to deploy the ExtraHop Reveal(x) Ultra sensor through AWS Marketplace.

After you deploy the sensor, configure AWS traffic mirroring or remote packet capture (RPCAP) to forward traffic from remote devices to the sensor.

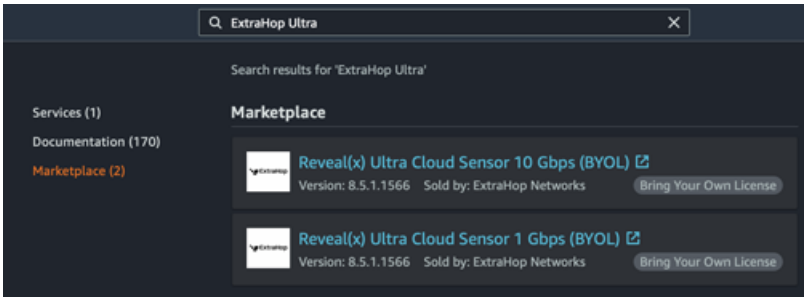
System requirements

Make sure you have everything you need to successfully deploy the sensor:

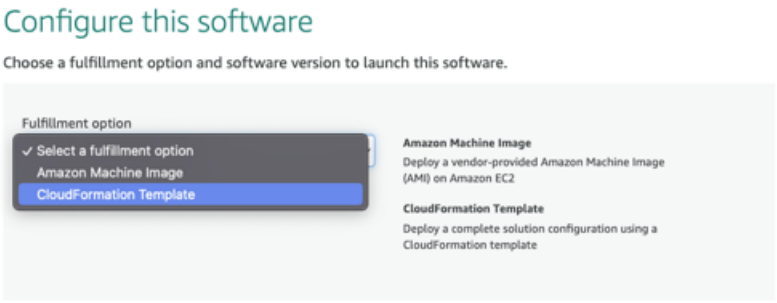
- An AWS account
- An ExtraHop Reveal(x) Ultra license or product key
- A VPC where the sensor will be deployed
- Two ENI subnets. One subnet to access the management interface of the sensor and one subnet that will forward traffic to the sensor. Both subnets must be in the same Availability Zone.

Deploy the sensor

1. Log in to your AWS Management Console.
2. In Marketplace, search for ExtraHop Ultra sensors.



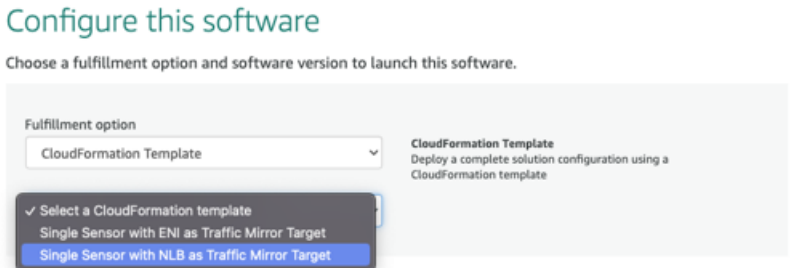
3. Click one of the following sensor names:
   - **Reveal(x) Ultra Cloud Sensor 1 Gbps (BYOL)**
   - **Reveal(x) Ultra Cloud Sensor 10 Gbps (BYOL)**
4. Click **Continue to Subscribe**.
5. Read the ExtraHop Terms and Conditions, and then click **Accept Terms**.
6. After the subscription process completes, click **Continue to Configuration**.
7. Select **CloudFormation Template** from the **Fulfillment option** drop-down list.



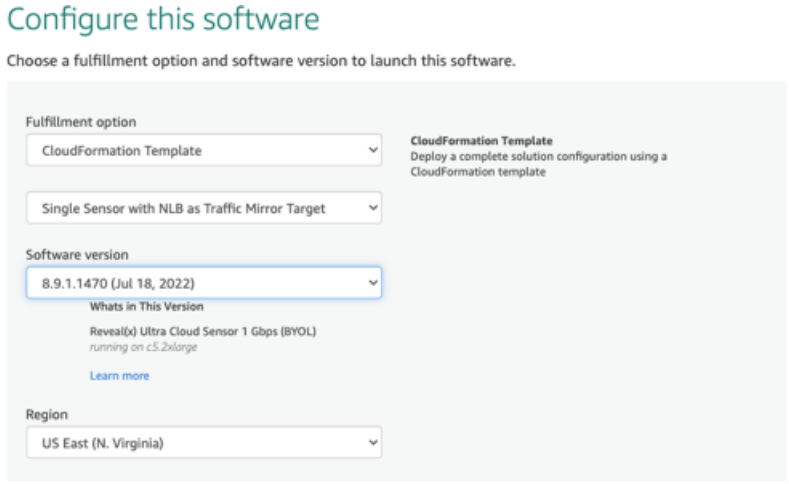
8. Select one of the following CloudFormation templates from the drop-down list:

© 2024ExtraHop Networks, Inc. All rights reserved.

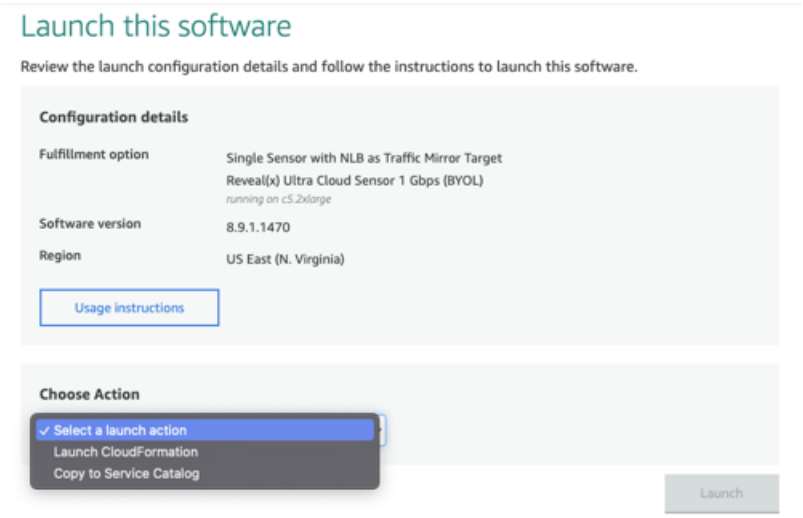
- **Single sensor with ENI as traffic mirror target**
- **Single sensor with NLB as traffic mirror target**. This option is recommended when you have more than ten traffic sources.



9. Select a firmware version from the **Software Version** drop-down list.
10. Select your AWS region from the **Region** drop-down list.



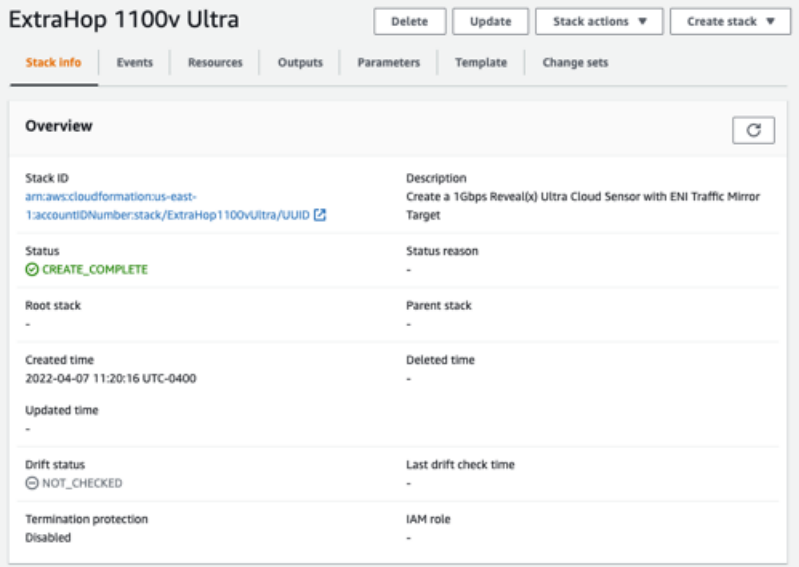
11. Click **Continue to Launch**.
12. On the Launch this software page, under Choose Action, select **Launch CloudFormation**.



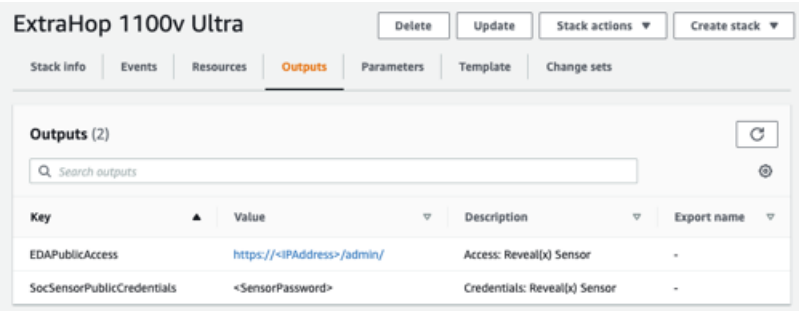
13. Click **Launch**.
14. On the Create stack page, leave the default settings unchanged and click **Next**.
15. On the Specify stack details page, type a name in the **Stack name** field to identify your instance in AWS.
16. In the Network configuration section, configure the following fields:

- **VPCID:** Select the VPC where the sensor will be deployed
- **MgmtSubnetID:** Select the subnet where the management ENI will be deployed
- **CaptureSubnetID:** Select the subnet where the data capture ENI will be deployed
- **RemoteAccessCIDR:** Type a CIDR IP range to restrict user access to the instance. We recommend that you configure a trusted IP address range.

17. In the ExtraHop configuration section, select one of the following options for the PublicIP field:
    - Select **false** if you do not want a public-facing IP address.
    - Select **true** if you want the sensor available to users through the public internet. The `MgmtSubnetID` specified in the previous step must be a public subnet.
18. Optional: In the Other parameters section, type an AMI ID for the source instance.
19. **Click Next**.
20. Add one or more tags in the Tags section and then click **Next**.
21. Review your configuration settings and then click **Create stack**.
22. Wait for the creation to complete. The `CREATE_COMPLETE` status appears on the Stack info page when the stack creation is successful.



23. Click the **Outputs** tab.



24. Copy the **SocSensorPublicCredentials** value. This is the setup user password required to log in to the ExtraHop system.
25. Click the **EDAPublicAccess** value URL to go to the sensor Administration settings page.

Next steps

- Register your ExtraHop system

- Configure the sensor network interfaces by clicking **Connectivity** in the Administration settings. Ensure that **Management** is selected on Interface 1. For Interface 2, choose one of the following options:
  - For the 1 Gbps sensor, select **Management + RPCAP/ERSPAN/VXLAN/GENEVE Target**.
  - For the 10 Gbps sensor, select **High-Performance ERSPAN/VXLAN/GENEVE Target**.

  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.
- (Recommended) configure AWS traffic mirroring or remote packet capture (RPCAP) to forward traffic from remote devices to the sensor.
- (Optional) Forward GENEVE-encapsulated traffic from an AWS Gateway Load Balancer.
- Complete the recommended procedures in the 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**.