Deploy an ExtraHop Flow Sensor with AWS

Published: 2022-06-07

This guide explains how to deploy the ExtraHop flow sensor virtual appliance (EFC 1291v) on the Amazon Web Services (AWS) platform.

The EFC 1291v is designed to connect to Reveal(x) 360 and collect flow-based traffic from your network. Packet analysis is not available.

Your environment must meet the following requirements to deploy an EFC 1291v appliance in AWS:

- An AWS account
- Access to the Amazon Machine Image (AMI) of the ExtraHop 1100v appliance
- An EFC 1291v appliance product key
- An AWS instance type that most closely matches the EFC appliance VM size, as follows:

Appliance	Supported Instance Type
Reveal(x) EFC 1291v	c5.xlarge (4 vCPU and 8 GB RAM)

Deployment overview

Collecting flow logs requires the following configuration setup.

1. Configure an IAM policy and IAM role.
2. Deploy the ExtraHop flow sensor instance in AWS.
3. Download and configure an ExtraHop-supplied Lambda function. The Lambda function runs whenever new flow logs become available and then relays any new events to your sensor. See the following AWS documentation for more information: Using Lambda with CloudWatch Logs.
4. Enable VPC Flow Logs publishing for a set of VPCs in your environment.
5. Add a Lambda trigger.
6. Configure Route 53.

Configure an IAM permission policy and IAM role

1. Create an IAM policy through the JSON tab with the following parameters:

```
{
    "Statement": [
        {
            "Action": [
                "ec2:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

2. Create an IAM role and attach the permission policy.

   The ExtraHop system requires an instance IAM role to correlate IP addresses from flow logs to instances, gateways, and Lambdas.

Deploy the sensor AMI

1. Deploy a Reveal(x) EDA 1100V by following the Deploy an ExtraHop sensor in AWS guide.

   The EDA 1100V is a packet sensor that becomes a flow logs sensor when the license is entered. The sensor will no longer process packets.

   Tip: You can subscribe to the Reveal(x) 1100v (BYOL) software through the AWS Marketplace.
2. After the instance is created and running, attach the IAM role you created above.
3. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`. The username is setup and the password is the string of numbers after the i- in the instance ID.
4. Follow the prompts to accept the license agreement, enter the product key, change the default setup and shell user account passwords, connect to ExtraHop Cloud Services, and connect to Reveal(x) 360.
5. Click the System Settings icon, and then click **All Administration**.
6. In the Access Settings section, click **API Access**.
7. In the Generate an API Key section, type a description for the new key and then click **Generate**.
8. Generate the Flow Log secret from the REST API Explorer.
   a) Click **Open ExtraHop API Explorer**.
   b) Click **Enter API Key** and then paste or type your API key into the API Key field.
   c) Click **Authorize** and then click **Close**.
   d) Click **ExtraHop** and then click **POST /extrahop/flowlogs/secret**.
   e) Click **Try it out** and then click **Send Request**.
   f) In the Response Body section, view and record the `secret` value. You will need the secret for the EXTRAHOP_SECRET_KEY environment variable in the next procedure.

Configure the Lambda function

An ExtraHop-supplied lambda function routes new flow log events to the ExtraHop flow sensor whenever called by a CloudWatch lambda trigger.

For more information about creating Lambda functions, see the AWS documentation.

Important: The Lambda function must be on the same VPC and subnet as the flow log sensor. The function must also be part of a security group that allows outbound TCP 443 traffic to the management interface of the collector.

1. Download the `exflowlogs-lambda.zip` file from the ExtraHop downloads page.
2. In AWS, create a Lambda function.
   - The function must have the Go1.x runtime.
   - The function must have an execution role with the following permissions:
     - **CloudWatch Logs:**
       - CreateLogGroup
       - CreateLogStream
       - PutLogEvents
     - **EC2:**
       - CreateNetworkInterface
       - DeleteNetworkInterface
       - DescribeNetworkInterfaces

- You must enable connectivity between your Lambda function and the VPC and subnet that your collector is on. The function must also be part of a security group that allows traffic between the function and collector.
- Upload the `exflowlogs-lambda.zip` file.
- Under General configuration settings, set the Memory field to `128 MB`.
- Under General configuration settings, set the Timeout field to `10 seconds`.
- Under Code, Runtime settings, set the handler value to `exflowlogs-lambda`.
- In the Environment variables settings, set the following environment variables:

  • **EDA_HOST:** The IP address or hostname of the VPC flow logs sensor.

  • **EXTRAHOP_SECRET_KEY:** The secret you generated through the ExtraHop REST API in the previous procedure.

  • **VERIFY_EDA_HOST_CERT:** If the sensor has the default self-signed certificate, specify `0` to disable certificate verification in the Lambda HTTP client. Otherwise, specify `1`.

  Note: It can take up to 10 minutes before devices are discovered and metrics are published from flow logs.

Publish flow logs to CloudWatch

For more information about publishing flow logs, see the following AWS documentation: Publish flow logs to CloudWatch Logs.

1. Identify the VPCs that you want to monitor with the flow sensor.
   - If your ExtraHop AWS deployment includes packet sensors, you should avoid monitoring a particular VPC with both a packet sensor and a flow logs sensor.
   - While it is possible to send logs for smaller units like individual subnets or interfaces, sending the entire VPC yields the best discovery of devices.
2. Create a CloudWatch log group to receive the flow logs.
3. Create an IAM policy through the JSON tab with the following statement:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

4. Identify an existing IAM role or create a new IAM role with a custom trust policy that allows Amazon EC2 to publish flow logs to a CloudWatch log group. The custom trust policy must have the following statement:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. Add the permission policy you created in step 3 to the role.
6. Configure how VPC flow logs are sent to the CloudWatch group. The ExtraHop system requires the following configuration:
   - **Filter:** Accept
   - **Maximum aggregation interval:** 1 Minute
   - **Custom log format:** You must select the attributes in the following order:
     - **start**
     - **end**
     - **log-status**
     - **action**
     - **vpc-id**
     - **subnet-id**
     - **interface-id**
     - **instance-id**
     - **srcaddr**
     - **dstaddr**
     - **srcport**
     - **dstport**
     - **protocol**
     - **tcp-flags**
     - **packets**
     - **bytes**
     - **pkt-srcaddr**
     - **pkt-dstaddr**

   The format preview should appear similar to the following figure.

Add a Lambda trigger

Add a CloudWatch Logs trigger to the Lambda function you created in the Publish flow logs to CloudWatchsection. Create the trigger with the following properties:

- **Type:** CloudWatch Logs
- **Log group:** The log group you created in the Publish flow logs to CloudWatch section.
- **Filter name:** Type a name for the trigger.
- **Filter pattern:** Leave this field blank.

Configure Route 53 logs (optional)

Amazon Route 53 provides DNS query logging, which is not required for the flow log configuration but is strongly recommended when the Amazon DNS server is configured.

To configure Route 53 to log DNS queries that originate in your VPCs, see the following AWS documentation: Managing Resolver query logging configurations.

1. Go to the Route 53 service.
2. In the Resolver section, click **Query logging**.
3. Click **Configure query logging**.
    a. Type a query logging configuration name.
    b. Select **CloudWatch Logs log group** as the query logs destination.
    c. From the CloudWatch Logs log groups drop-down list, select the log group you created in the Publish flow logs to CloudWatch section.
    d. In the VPCs to log queries for section, click **Add VPC**.
    e. Select the VPCs that you want to log queries for and then click **Add**.
    f. Click **Configure query logging**.