Automate AWS Traffic Mirroring with CloudFormation

Published: 2024-05-21

You can automate traffic mirroring for ExtraHop sensors in AWS with a CloudFormation template that is publically available on the ExtraHop code-examples GitHub repo. The CloudFormation template creates an EventBridge rule and Lambda function that work together to automatically mirror traffic. Here is how the system works:

The EventBridge rule runs when one of the following CloudTrail events occurs:

- CreateTags
- DeleteTags
- RunInstances
- DeleteTrafficMirrorSession

The EventBridge rule then starts the Lambda function. The Lambda function creates or deletes a traffic mirror session that mirrors traffic from an EC2 instance to a traffic mirror target that is associated with an ExtraHop sensor. The Lambda function determines how to create the mirror session based on AWS tags applied to EC2 instances, traffic mirror filters, and traffic mirror targets.

If the event is CreateTags, and a specific tag was added to an EC2 instance, the Lambda function creates a traffic mirror session for the EC2 instance. If the event is RunInstances, and the EC2 instance has a specific tag, the Lambda function creates a traffic mirror session for the EC2 instance. If the event is DeleteTrafficMirrorSession, and an associated EC2 instance has a specific tag, the Lambda function recreates the session to prevent traffic mirror sessions from being deleted accidentally or maliciously.

If the event is DeleteTags, and a specific tag was removed from an EC2 instance, the Lambda function deletes a traffic mirror session.

Before you begin

- Create traffic mirror targets for each of your ExtraHop sensors.

  The traffic mirror targets must be associated with one of the following AWS resources:

  - EC2 instance
  - Network Load Balancers
  - Gateway Load Balancer Endpoint
- Create traffic mirror filters that determine what traffic will be mirrored to your sensors.

Deploy the CloudFormation template

1. Go to the ExtraHop code-examples GitHub repository and download the `cloudformation_traffic_mirror/cloudformation_traffic_mirror.yml` file to your local machine.
2. Navigate to the CloudFormation page in AWS.
3. Create a CloudFormation stack from the CloudFormation template file you downloaded.

   Configure the following variable:

   TagMirror

   This name identifies the specific tag that you will add to mirrors and filters to coordinate traffic mirroring. Record the value of this variable.

   For more information about configuring a CloudFormation stack, see the AWS documentation.

Tag AWS Resources

The Lambda function creates traffic mirror sessions between an EC2 instance and a traffic mirror target. To facilitate this step, you must add the same tag to each instance, target, and traffic mirror filter.

For example, the following table demonstrates an environment where the name of the TagMirror variable is `EH-Mirror`. EC2 instances `ec2-A` and `ec2-B` are monitored by the sensor associated with `traffic-mirror-target-1`. Data from `ec2-A` and `ec2-B` is filtered by `traffic-mirror-filter-1`. Similarly, EC2 instances `ec2-C` and `ec2-D` are monitored by the sensor associated with `traffic-mirror-target-2`. Finally, data from `ec2-C` and `ec2-D` is filtered by `traffic-mirror-filter-2`.

Tag Key:Value (Applied to each AWS resource in row)	EC2 Instance Name	Traffic Mirror Target Name	T
`EH-Mirror:sensor-1`	`ec2-A`	`traffic-mirror-target-1`	t
`EH-Mirror:sensor-1`	`ec2-B`	`traffic-mirror-target-1`	t
`EH-Mirror:sensor-2`	`ec2-C`	`traffic-mirror-target-2`	t
`EH-Mirror:sensor-2`	`ec2-D`	`traffic-mirror-target-2`	t

1. Tag each traffic mirror target.
2. Tag each traffic mirror filter.
3. Tag each EC2 instance.

Note: The EC2 instance must support traffic mirroring. For more information, see the AWS documentation about supported instance types.

Tip: You can tag multiple EC2 instances at once with the AWS Tag Editor.