



How-To Guide

Configure AWS CloudTrail to forward logs to Netsurion Open XDR

Publication Date:

December 08, 2023

Abstract

This guide provides instructions to configure and retrieve the Amazon Web services (AWS) events via the Amazon CloudTrail and then forward the logs to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Amazon CloudTrail and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Amazon CloudTrail logs in Netsurion Open XDR.

Table of Contents

1	Overview	4
2	Prerequisites	4
3	Integrating AWS CloudTrail with Netsurion Open XDR.....	4
3.1	Enabling the CloudTrail Logging	4
3.2	Implementing the Netsurion Open XDR Lambda Function	6
3.3	Creating Lambda Subscription Filter for CloudWatch	9

1 Overview

Amazon Web Services (AWS) is a collection of remote computing services (also called web services) that make up a cloud computing platform offered over the internet by Amazon.com.

Amazon CloudTrail is enabled on your AWS account when you create it. When an activity occurs in your AWS account, it gets recorded as a CloudTrail event. With CloudTrail, you will get the history of AWS API calls for your account, including the API calls made via the AWS Management Console, AWS SDKs, command-line tools, and higher-level AWS services (such as AWS CloudFormation). Amazon EC2 and Amazon VPC are examples of a few services integrated with CloudTrail that is, CloudTrail captures the API calls made on behalf of Amazon EC2 and Amazon VPC.

Netsurion Open XDR manages logs retrieved from CloudTrail and filters them to get the critical event types. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in AWS services.

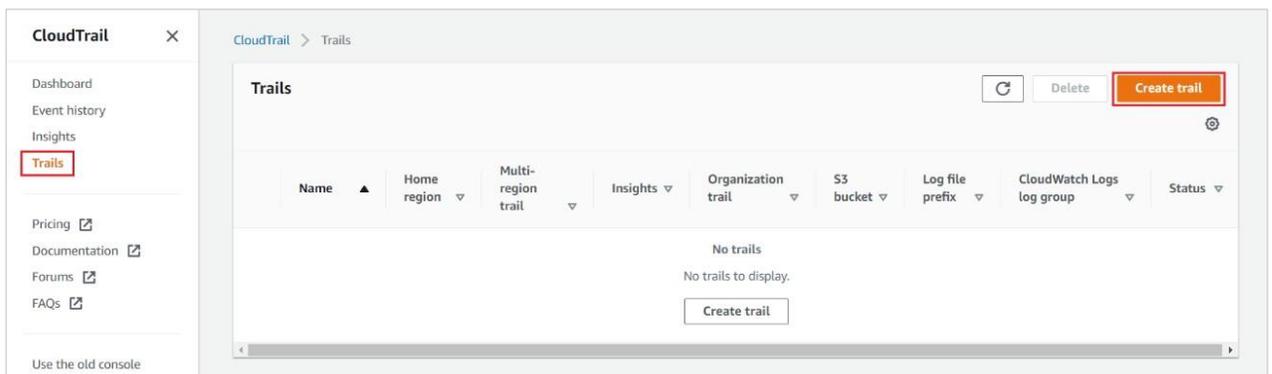
2 Prerequisites

- Root level access to the [AWS](#) console.
- The Netsurion Open XDR VCP port must be Network Address Translation (NAT) with a public IP address.

3 Integrating AWS CloudTrail with Netsurion Open XDR

3.1 Enabling the CloudTrail Logging

1. Log in to the AWS [CloudTrail](#).
2. Navigate to the **Trails** section and click the **Create trail** button.



3. In the **General details** interface, specify the following details and click **Next**.

Trail name: Provide the Trail name.

CloudWatch Logs: Select the **Enabled** check box to enable the **CloudWatch Logs** option.

Log group name: Provide the **Log group name**.

Role name: Provide the **Role name**.

General details

A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

Management_Events

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

CloudWatch Logs - optional

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#)

CloudWatch Logs [Info](#)
 Enabled

Log group [Info](#)
 New
 Existing

Log group name

aws-cloudtrail-logs-████████████████████

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

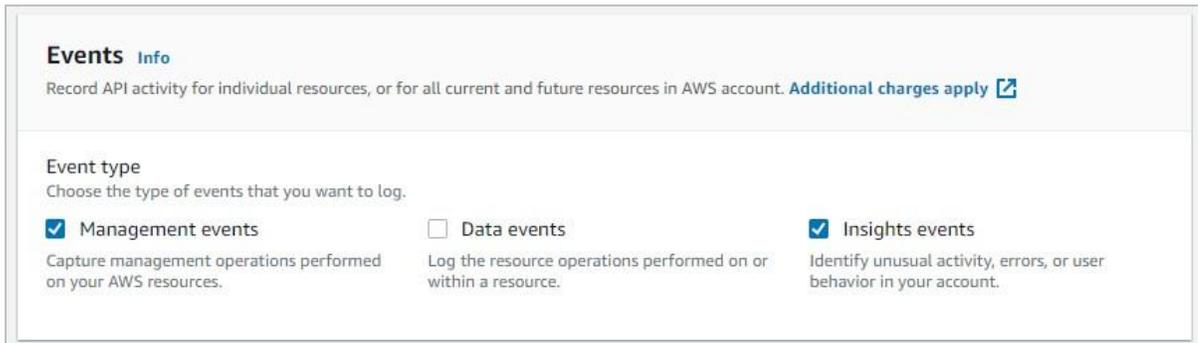
IAM Role [Info](#)
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.
 New
 Existing

Role name

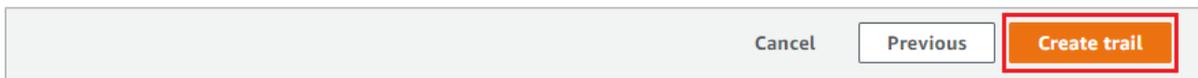
CloudTrailRoleForCloudWatchLogs_{trail-name}

[► Policy document](#)

- In the **Events > Event type**, select the **Management events** and **Insights events** checkboxes.



- Click **Next** and review the selected configurations, and then click **Create trail** to initiate sending the CloudTrail logs to CloudWatch.

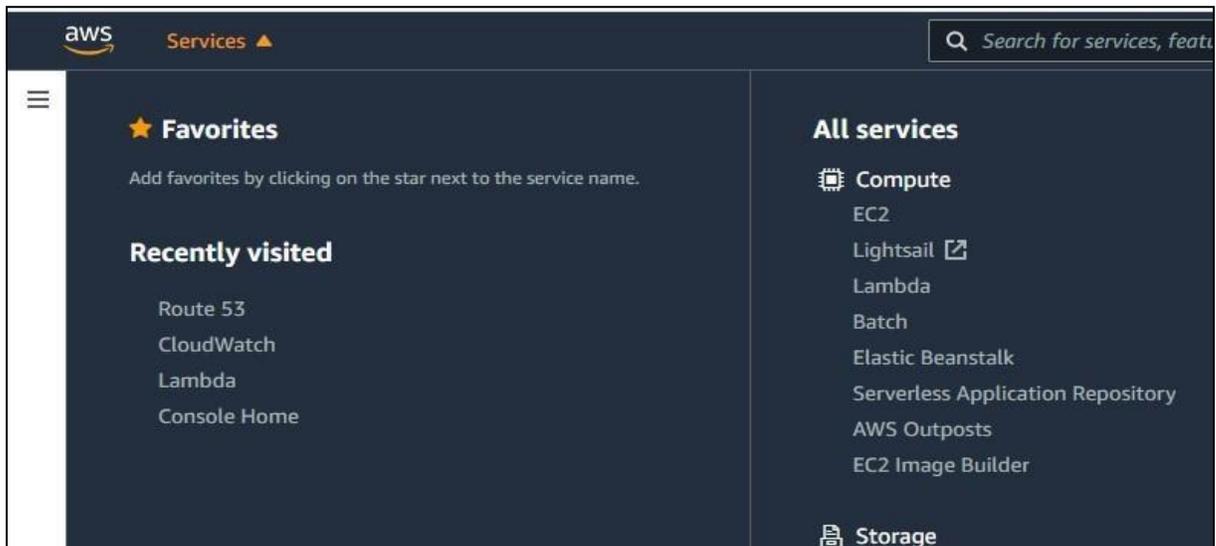


Note
 For forwarding the CloudTrail logs to open XDR you need to [create a subscription filter](#) for the log group created earlier in the step 3.

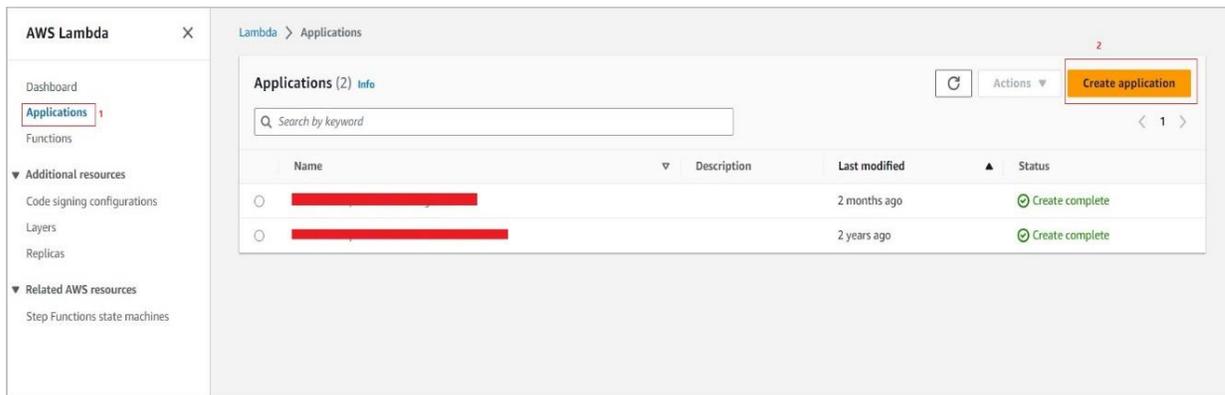
3.2 Implementing the Netsurion Open XDR Lambda Function

Perform the process to create the open XDR Lambda for integrating the **CloudWatch** with op.

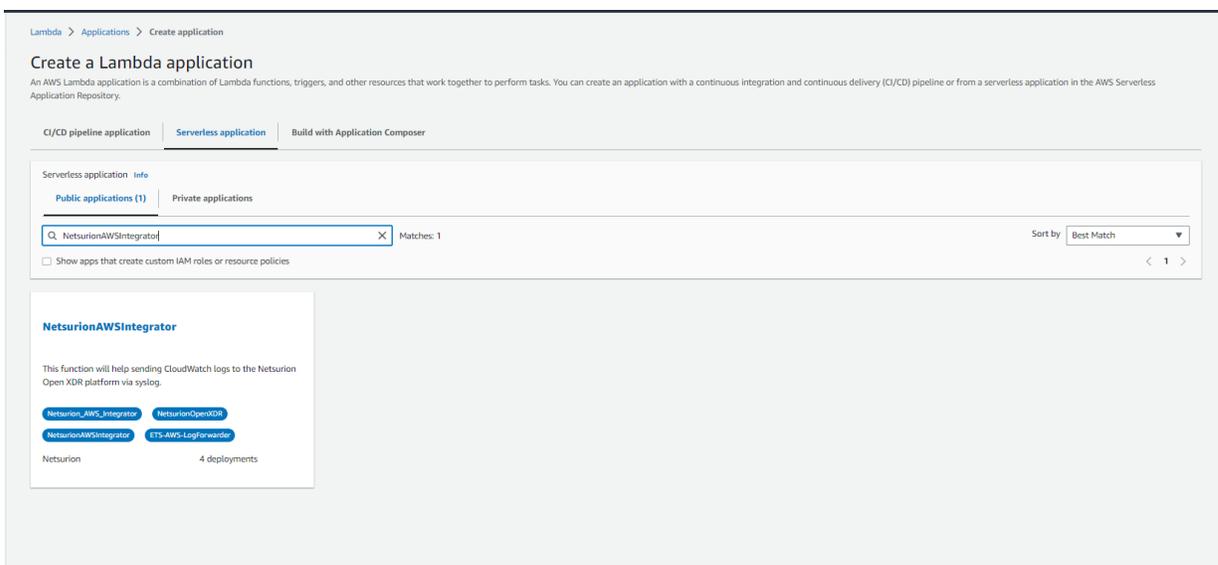
- In the **AWS** console, go to **Services > Compute > Lambda**.



- In the **AWS Lambda** interface, from the left panel, go to Applications and click **Create application**.



- In the **Create application** interface, click the **Serverless application** tab.



- In the **Public applications** tab, search and click the **NetsurionAWSIntegrator** application using the search results.

- In the **NetsurionAWSIntegrator** application settings, fill in the following details and click **Deploy** to create the function.

Application settings

Application name
The stack name of this application created via AWS CloudFormation

▼ **NetsurionAWSIntegrator**

NetsurionXDRManager
Netsurion Open XDR Manager FQDN/IP(e.g. receiver.contoso.net)

OrganizationName
Organization Name(e.g. Contoso)

SyslogOverTLS
Enable Syslog Over TLS (e.g. true or false)

SyslogPort
Netsurion Open XDR Syslog VCP Port(e.g. 4514)

EventTrackerManagerIP: Enter the Open XDR **Public Manager FQDN** or **IP address**.

OrganisationName: Enter the organization name.

SyslogOverTLS: Enter **True** to Enable syslog over TLS.

Note

Refer to [Configure Syslog Over TLS in Netsurion Open XDR](#) guide to configure syslog over TLS.

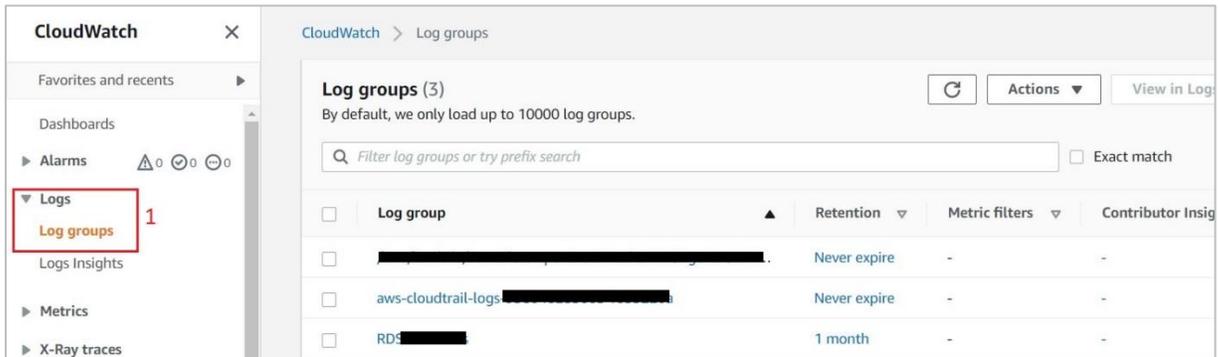
SyslogPort: Enter the syslog port details.

- After providing the details click **Deploy**, and the **Lambda function** will be created.

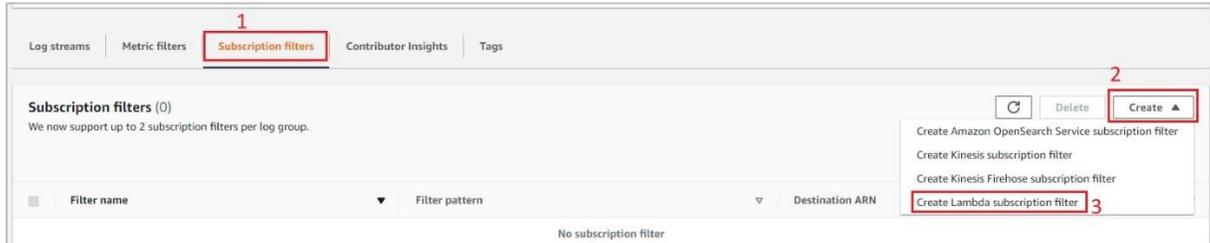
3.3 Creating Lambda Subscription Filter for CloudWatch

Perform the following steps to create a subscription filter for the log group to forward the CloudTrail logs to the Open XDR platform.

1. In the **AWS** console, go to **All Services > Management & Governance > CloudWatch**.
2. From the left of the **CloudWatch** navigation pane, go to **Logs > Log groups**.
3. In the **Log groups** section, select the **Log group name** provided while configuring [CloudTrail](#).



4. From the selected Log group name click the **Subscription filters** tab.
5. In the **Subscription filters** section, click the **Create** button and click **Create Lambda subscription filter** from the drop-down list.



6. In **Create Lambda subscription filter > Lambda function** section, click the lambda function (that was created initially) from the drop-down list.

- In the **Configure Log format and filters**, click the required **Log format** and specify the **subscription filter name**, that is, **CloudTrailTrigger**.

Create Lambda subscription filter

You are about to start streaming data from your "aws-cloudtrail-logs-956046285005-f655220a" log group to an Amazon Lambda function. Any new log data sent to this log group will be sent to the function you choose.

Choose destination

Choose the Lambda function to execute when a log event matches the filter you are going to specify. [Learn more about Lambda functions.](#)

Lambda function
Select the Lambda function you want to subscribe to the filter.

▼

1

⚠ Streaming large amounts of CloudWatch Logs data to other destinations might result in high usage charges. We recommend that you create a Budget in the Billing and Cost Management console. For more information, see: [Managing Your Costs with Budgets](#)

Configure log format and filters

Choose your log format to get a recommended filter pattern for your log data, or select "Other" to enter a custom filter pattern. An empty filter pattern matches all log events.

Log format

▼

2

Subscription filter pattern
Specify the log event structure and any filter conditions to apply on your log data as it gets streamed to the Amazon Lambda service.

Subscription filter pattern

Subscription filter name

Subscription filter name

3

- After providing all the details, scroll down the interface and click **Start streaming**.

Test pattern

Select log data to test

Custom log data ▼

Log event messages
Type log data to test with your Filter Pattern. Please use line breaks to separate log events.

```
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK: Running Start Crawl fc
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK: Classification complete
[83078518-fcc1-4d30-9573-8b9737671438] INFO: Crawler configured with Scher
[83078518-fcc1-4d30-9573-8b9737671438] INFO: Created table gluetest in datab
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK: Finished writing to Cat
```

Test pattern

Results
Please select log event messages above and click "Test pattern" to see results.

Cancel
Start streaming

4

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the [form](#) to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

<https://www.netsurion.com/support>