Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring AWS CloudTrail to Forward Logs to EventTracker

Publication Date:

November 11, 2021

Abstract

This guide provides instructions to configure/ retrieve the Amazon Web services (AWS) events using Amazon CloudTrail. This will include services like Amazon Kinesis, Amazon DynamoDB, Amazon EKS, AWS ELB (Elastic Load Balancer), and Amazon ECR. Once EventTracker is configured to collect and parse these logs, dashboard, and reports can be configured to monitor the Amazon CloudTrail logs.

Audience

Administrators who are assigned the task to monitor the Amazon CloudTrail logs using EventTracker.

Table of Contents

1. Overview

Amazon Web Services (AWS) is a collection of remote computing services (also called web services) that together 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, that activity is recorded in a CloudTrail event. With CloudTrail, you can get the history of the 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 the e.g., of few services which are integrated with CloudTrail, i.e., CloudTrail captures the API calls made on behalf of Amazon EC2 and Amazon VPC.

EventTracker collects the events delivered to CloudTrail and filters them out to get some critical event types for creating reports, dashboards, and alerts. These are considered as Knowledge Packs and help to reduce the effort to manually log in to the AWS account and figuring what events are supposed to be critical. The events collected by EventTracker will include services like Amazon EC2 and Amazon VPC.

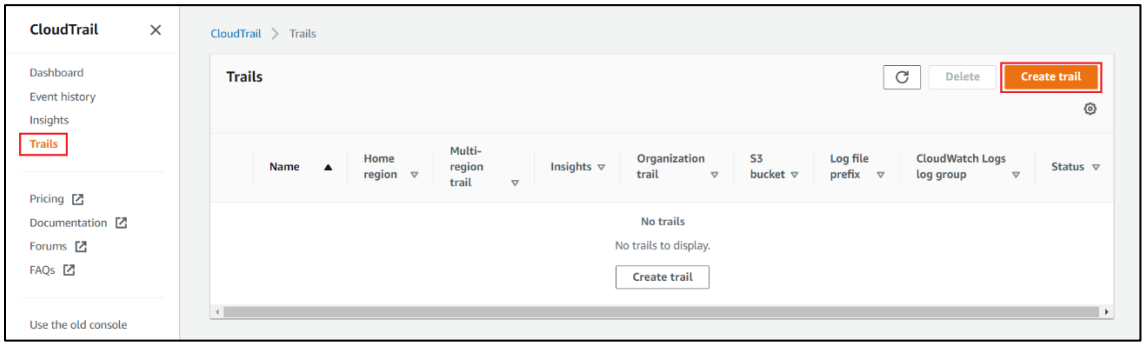
2. Prerequisites

- Users must have root-level access to the AWS console.
- EventTracker syslog VCP port should be NAT with the public IP address.

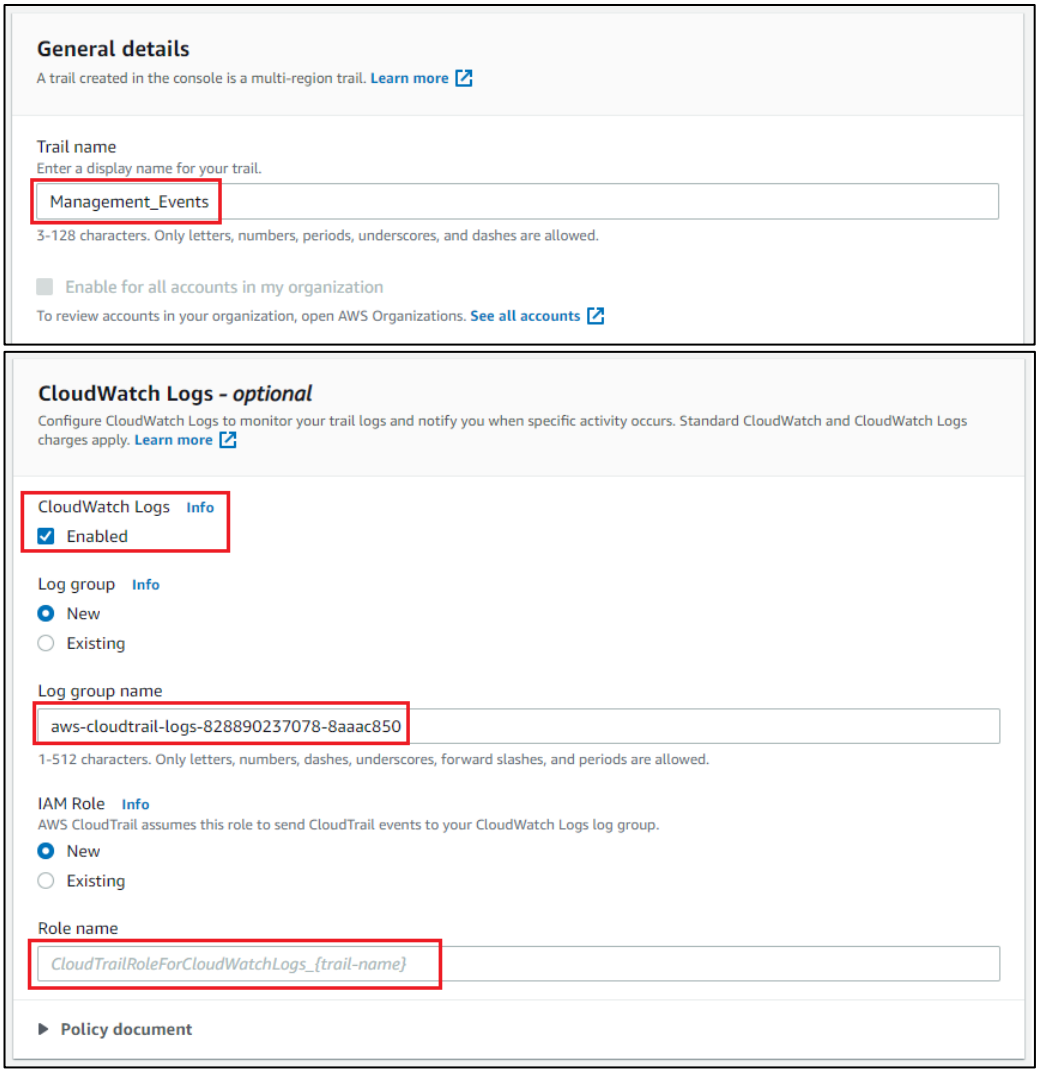
3. Integrating AWS CloudTrail with EventTracker

3.1 Enabling CloudTrail Logging

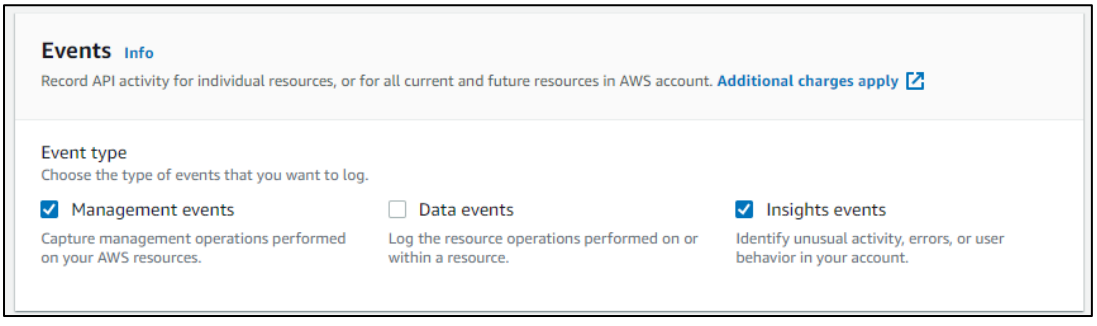
1. Log in to the AWS CloudTrail.
2. Navigate to the **Trails** section and click the **Create trail** button.



3. Provide the **Trail name** and enable the **CloudWatch Logs** option.



4. Provide the **Log group name** and **Role name.**
5. Click **Next** and select the **Management events** and **Insights events** in the Event type.



6. Click **Next** and review the setting and click **Create trail.**

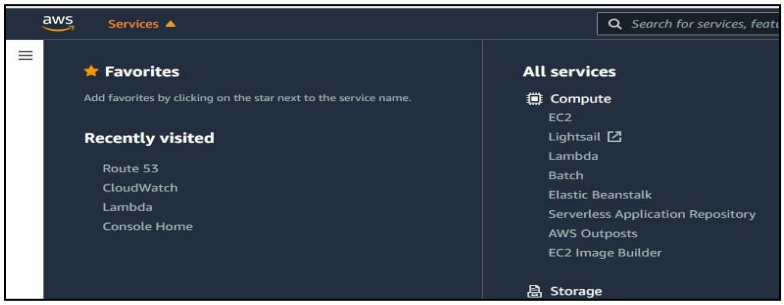
It starts sending the CloudTrail logs to CloudWatch.

For forwarding the CloudTrail logs to EventTracker. You need to create a subscription filter for the log group created in step 4.

Follow the below instruction for integrating the CloudWatch with EventTracker.

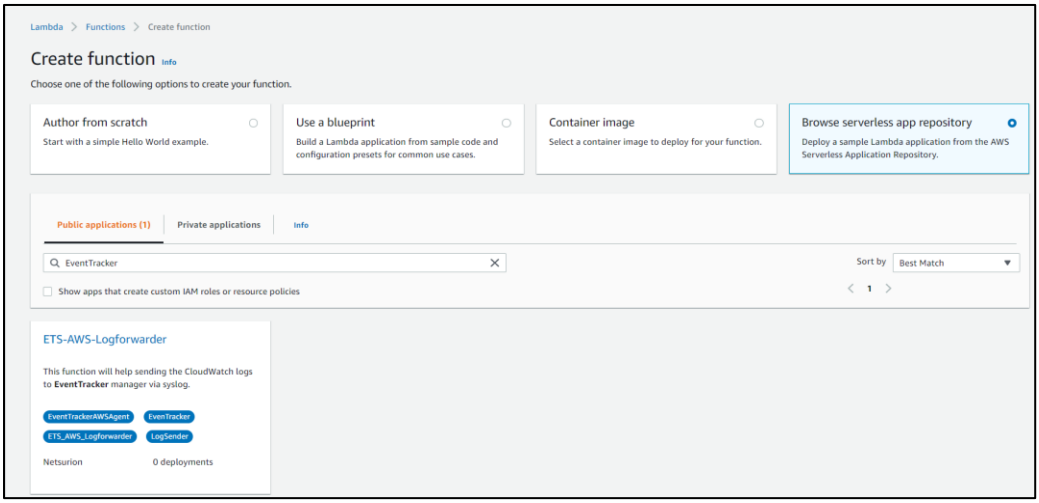
3.2 Implementing EventTracker Lambda function

1. Click **All Services** and select **Lambda.**

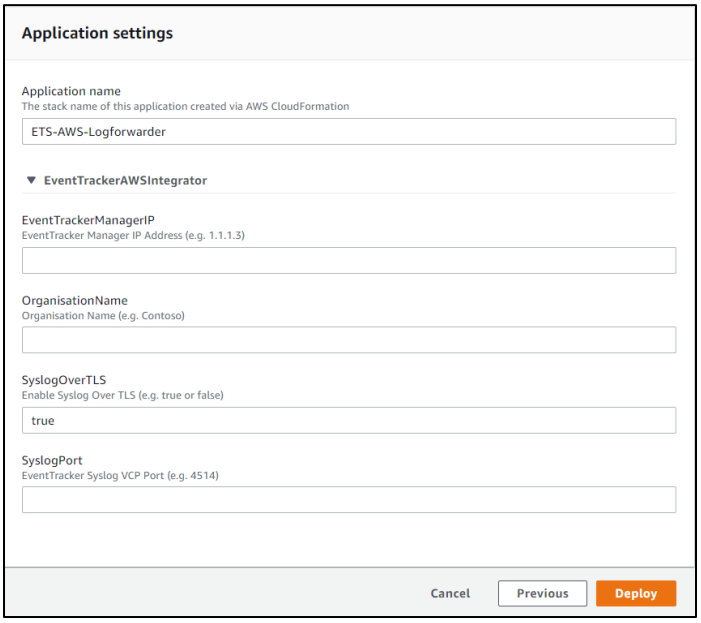


2. In the **Navigation** pane choose **Functions**, then click **Create function**.

3. Select **Browse serverless app repository.**
4. Search for **EventTracker** in the **Public applications** search bar.
   You will get the **ETS-AWS-Logforwarder** in the results.



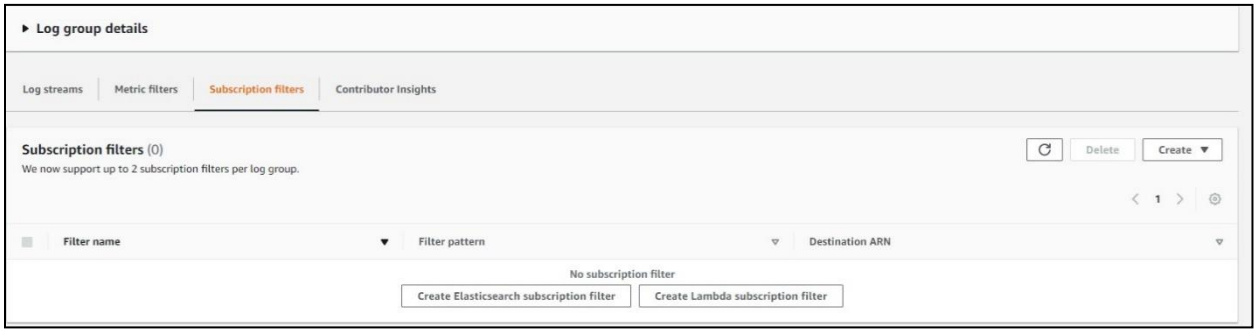
5. Fill in the details and click **Deploy**.



6. Enter the EventTracker **Public Manager IP address**.
7. Enable syslog over TLS as **True** or **False.**
8. Enter the syslog port.
9. After you click **Deploy**, a function is created.

3.3 Creating Subscription filters for CloudWatch

1. Click the **Services** and select **CloudWatch.**
2. In the navigation pane, choose the **Log group**.
3. Click the **Log group** provided while creating **CloudTrail**.
4. Go to the **Subscription filter**.



5. Click the **Create Lambda subscription filter**.
6. Under the lambda function, select the lambda function (created after deploying the application) created from the dropdown.
7. Enter the subscription filter name, i.e., **CloudTrailTrigger**.
8. Click **Start streaming**.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #23 among MSSP Alert's 2021 Top 250 MSSPs.

Contact Us

Corporate Headquarters

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

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support