Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Amazon ECR to Forward Logs to EventTracker

Publication Date:

November 30, 2021

Abstract

This guide provides instructions to configure/ retrieve the Amazon Elastic Container Registry (ECR) events using Amazon CloudTrail and Amazon EventBridge. After EventTracker is configured to collect and parse these logs then the dashboards and reports can be configured to monitor the Amazon ECR events.

Audience

This guide is intended for use by all EventTracker users responsible for investigating and managing network and cloud security. This guide assumes that you have EventTracker access and understanding of networking technologies and Amazon Web Services.

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 login 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.

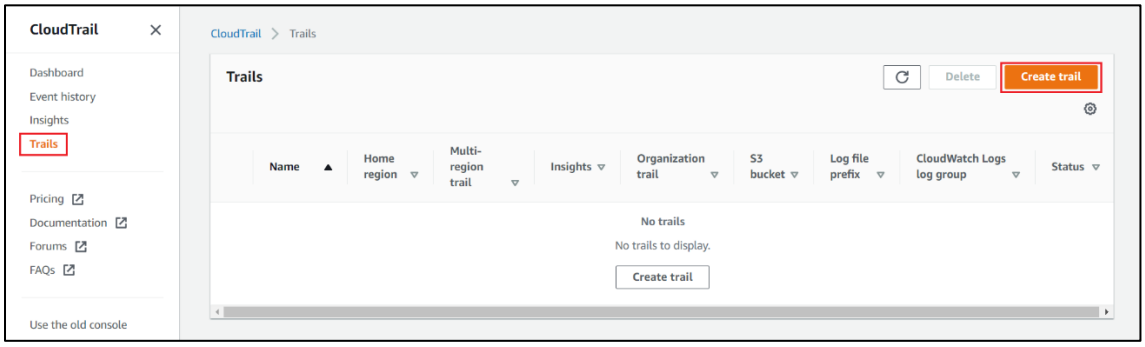
2. Prerequisites

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

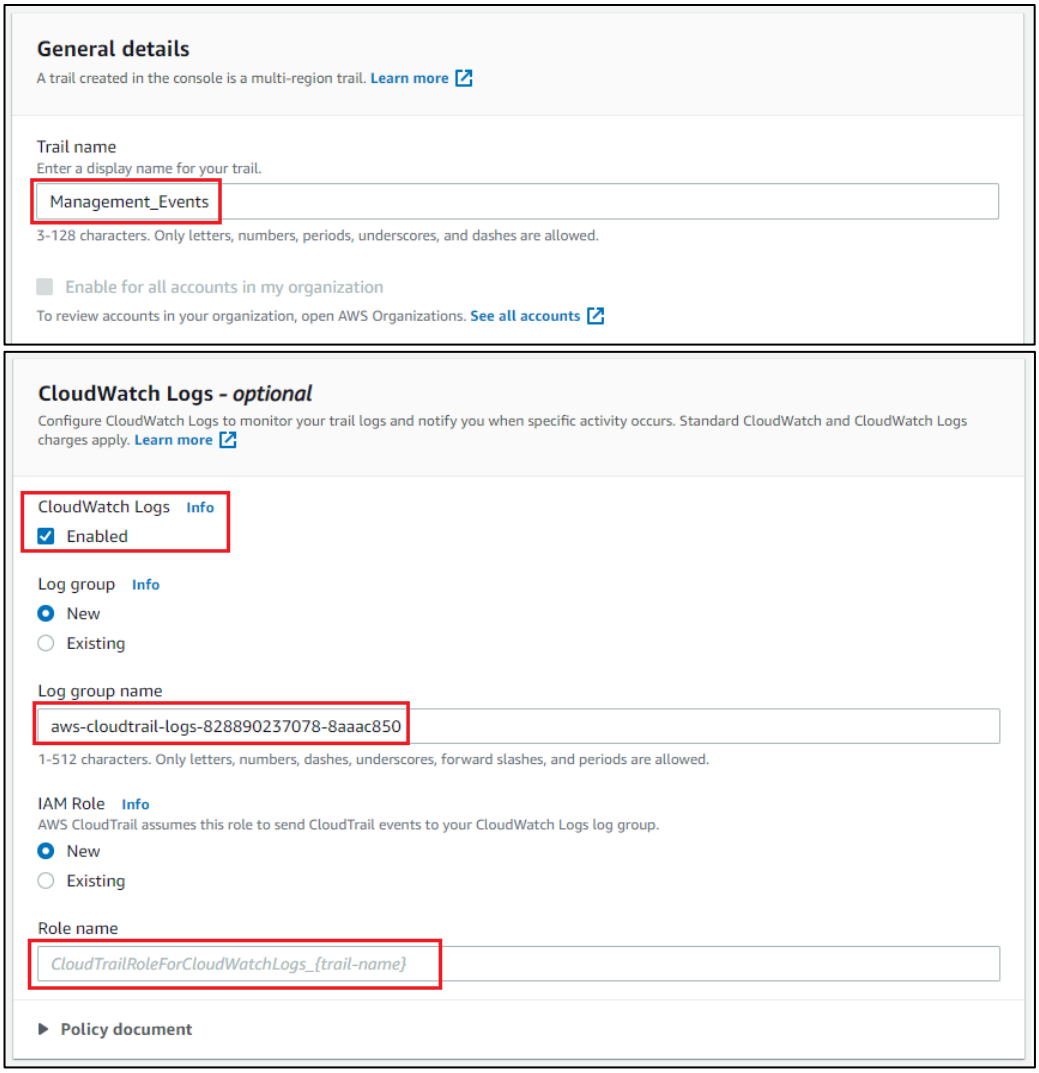
3. Integrating AWS CloudTrail with EventTracker

3.1 Enabling CloudTrail Logging

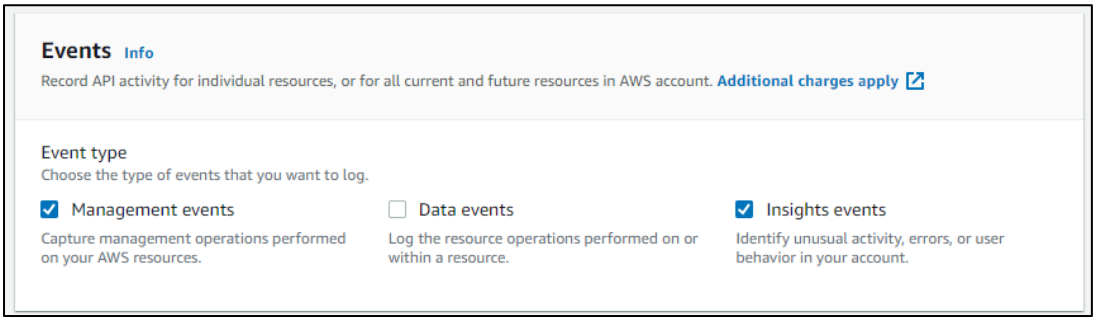
1. Login to AWS CloudTrail.
2. Navigate to the **Trails** section and click the **Create trail** button.



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



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



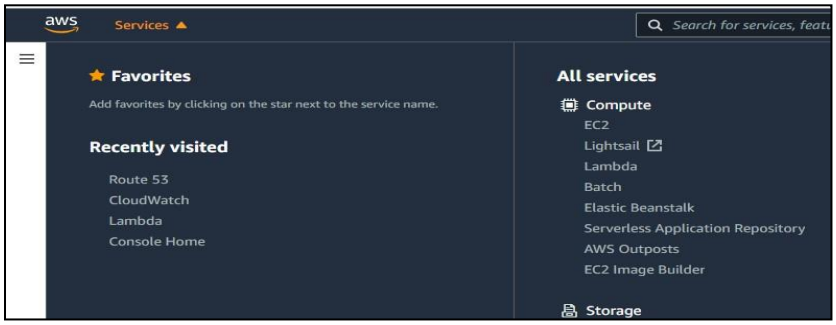
6. Click **Next** and review the setting and click **Create trail.**

It starts sending the CloudTrail logs to CloudWatch.

For forwarding the CloudTrail logs to EventTracker. We need to create a subscription filter for the log group which we have created in step 4. Follow the below instruction for integrating CloudWatch with EventTracker.

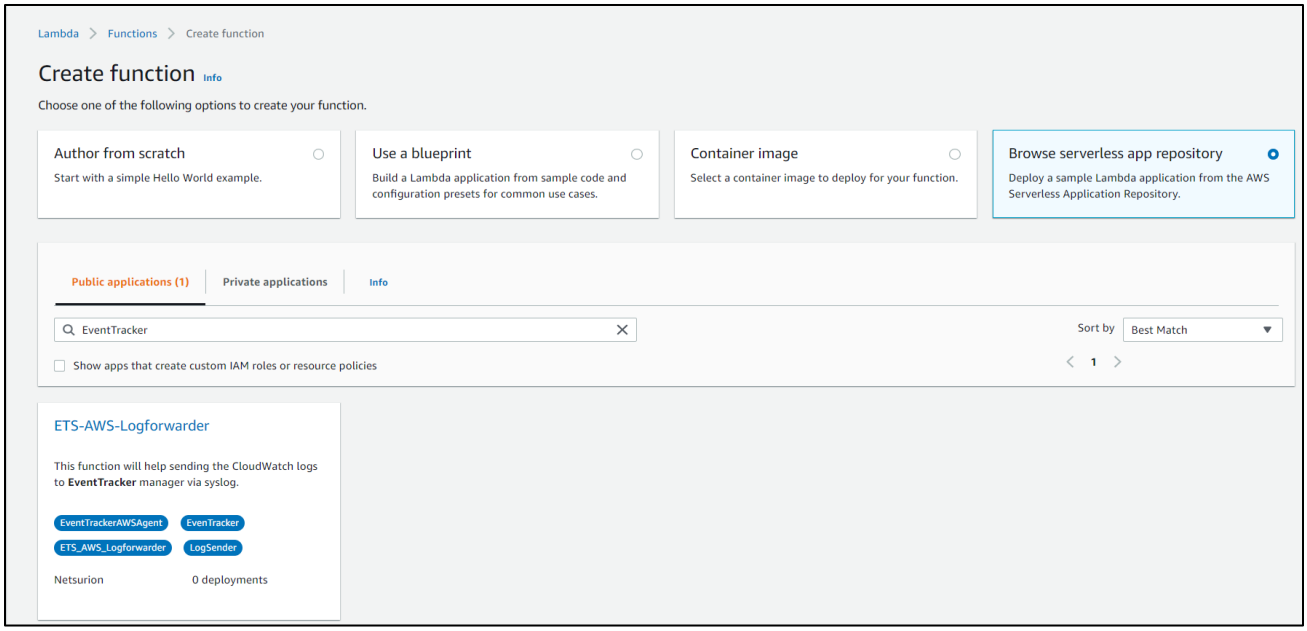
3.2 Implementing EventTracker Lambda function

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

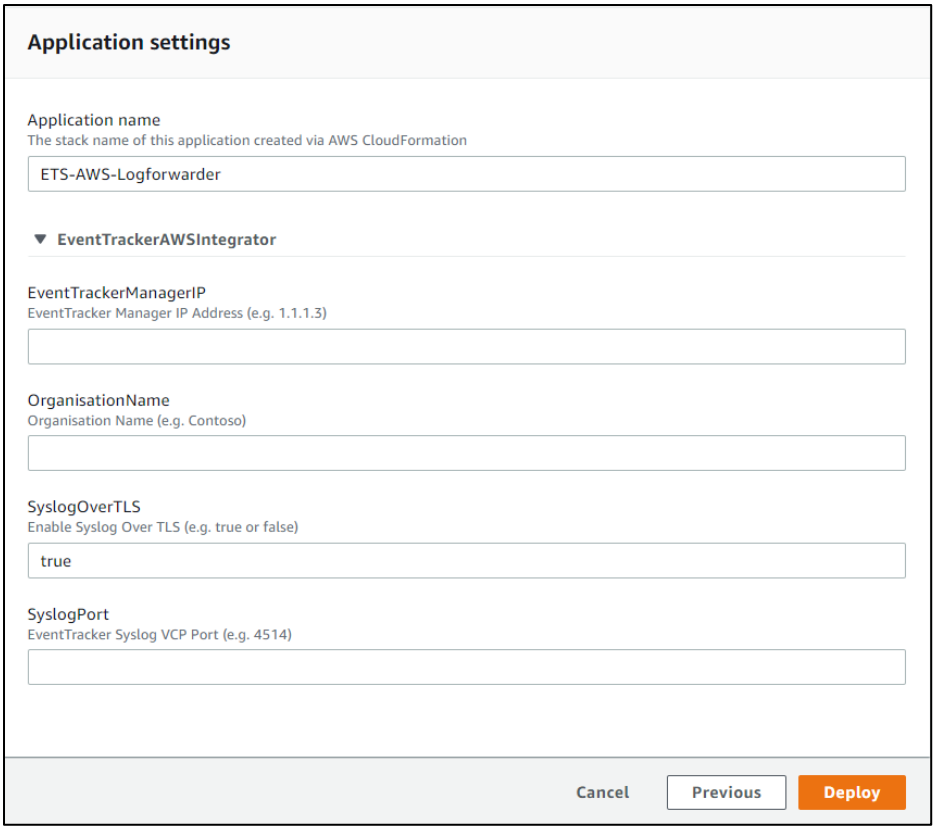


2. In the **Navigation** pane choose **Functions**, then click the **Create function**.

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



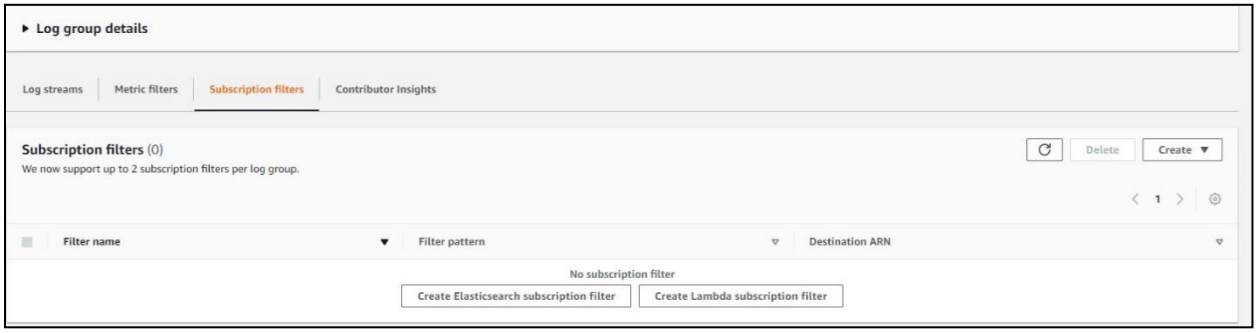
5. Fill in the details and click **Deploy**.



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 **log group**.
3. Click the **Log group** provided while creating **CloudTrail**.
4. Go to the **Subscription filter**.

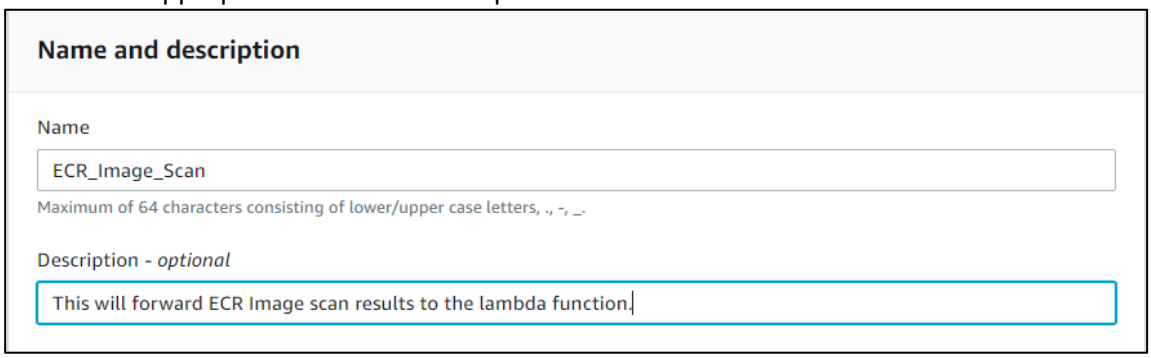


5. Click the **Create Lambda subscription filter**.
6. Under the lambda function, select the lambda function (created after deploying the application) created from the dropdown.
7. Enter subscription filter name, i.e., **CloudTrailTrigger**.
8. Click **Start streaming**.

3.4 Creating Rules in Amazon EventBridge

1. Click the **services** and select **EventBridge.**
2. In the navigation pane select **Rules,** further click the **Create Rule.**

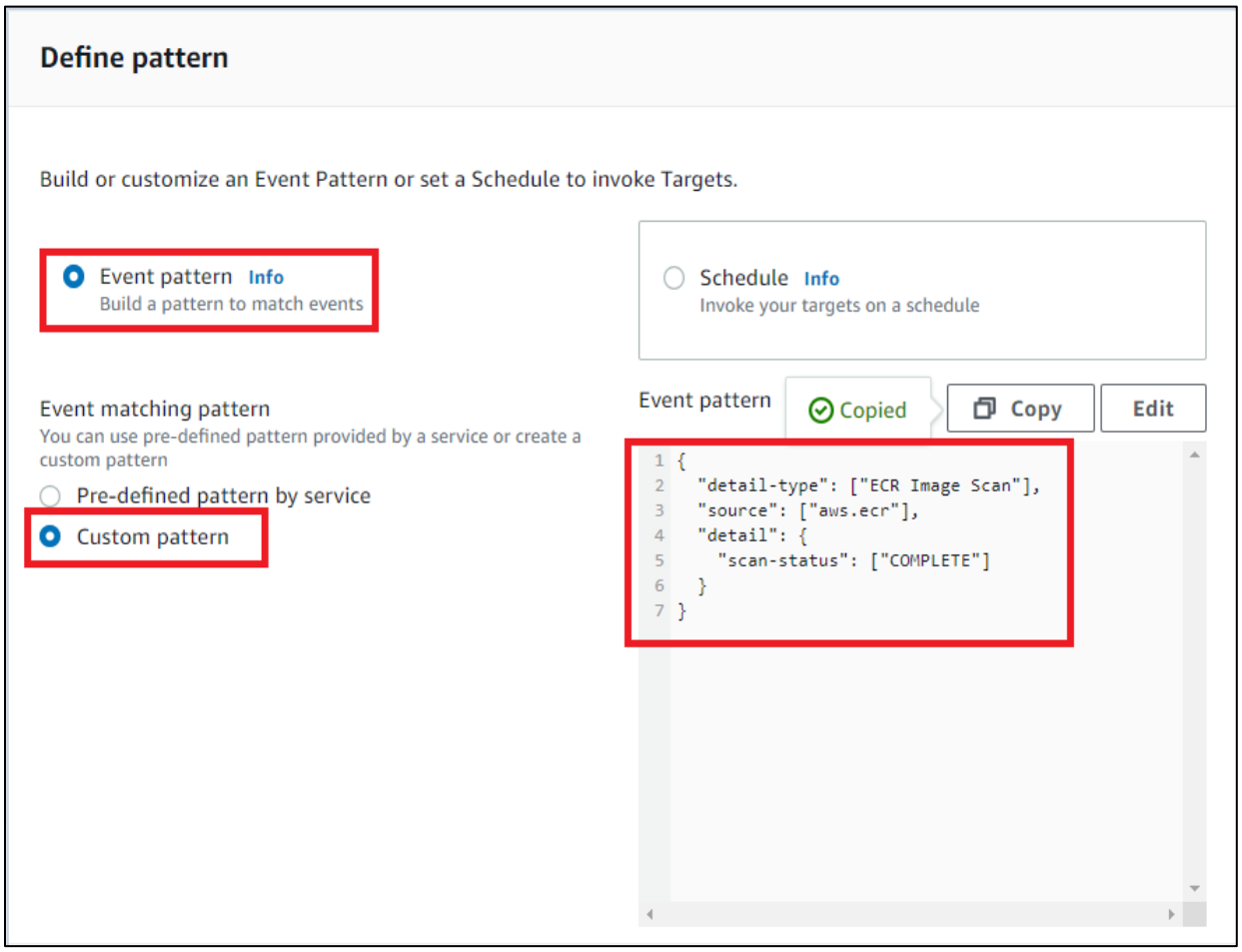
3. Add an appropriate name and description to the rule to be created.



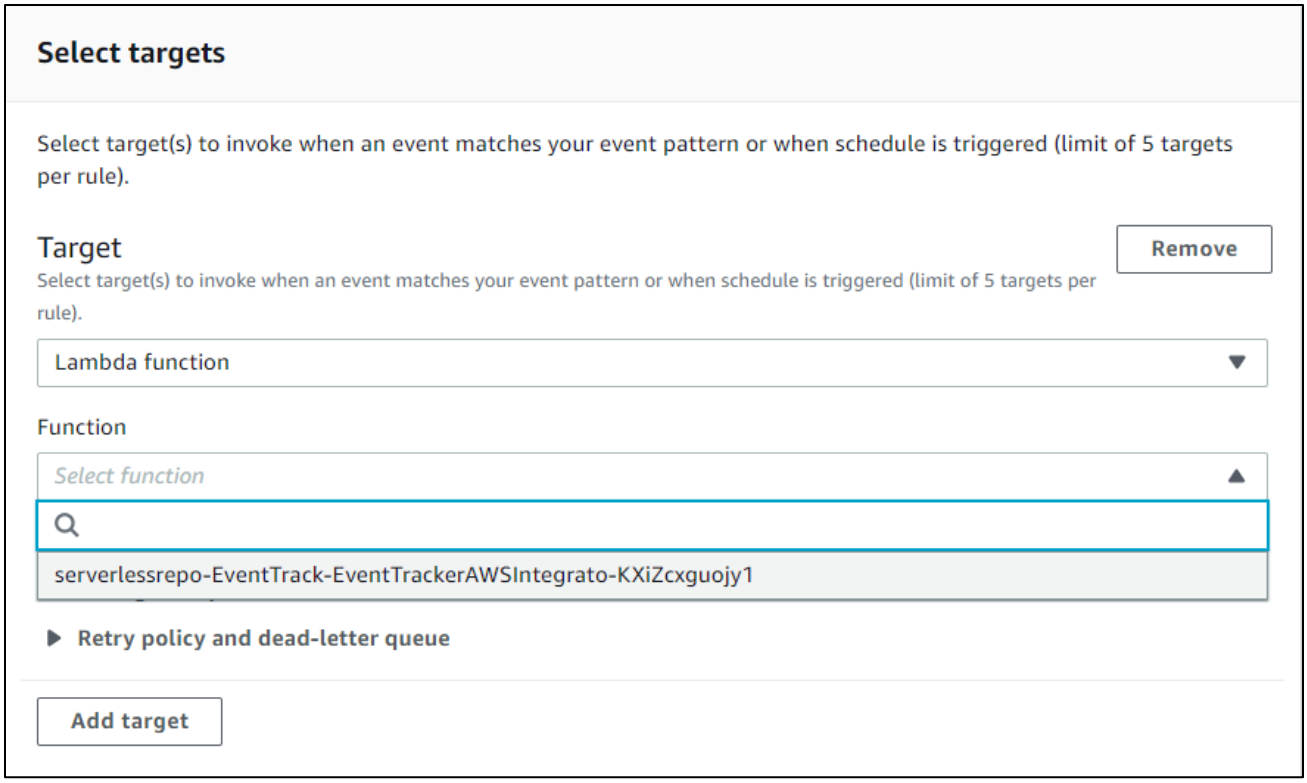
4. Under the **Define pattern** section select the **Event pattern** and **Custom pattern** options. Enter the following Event pattern below:

{

```
  "detail-type": ["ECR Image Scan"],
  "source": ["aws.ecr"],
  "detail": {
    "scan-status": ["COMPLETE"]
  }
}
```

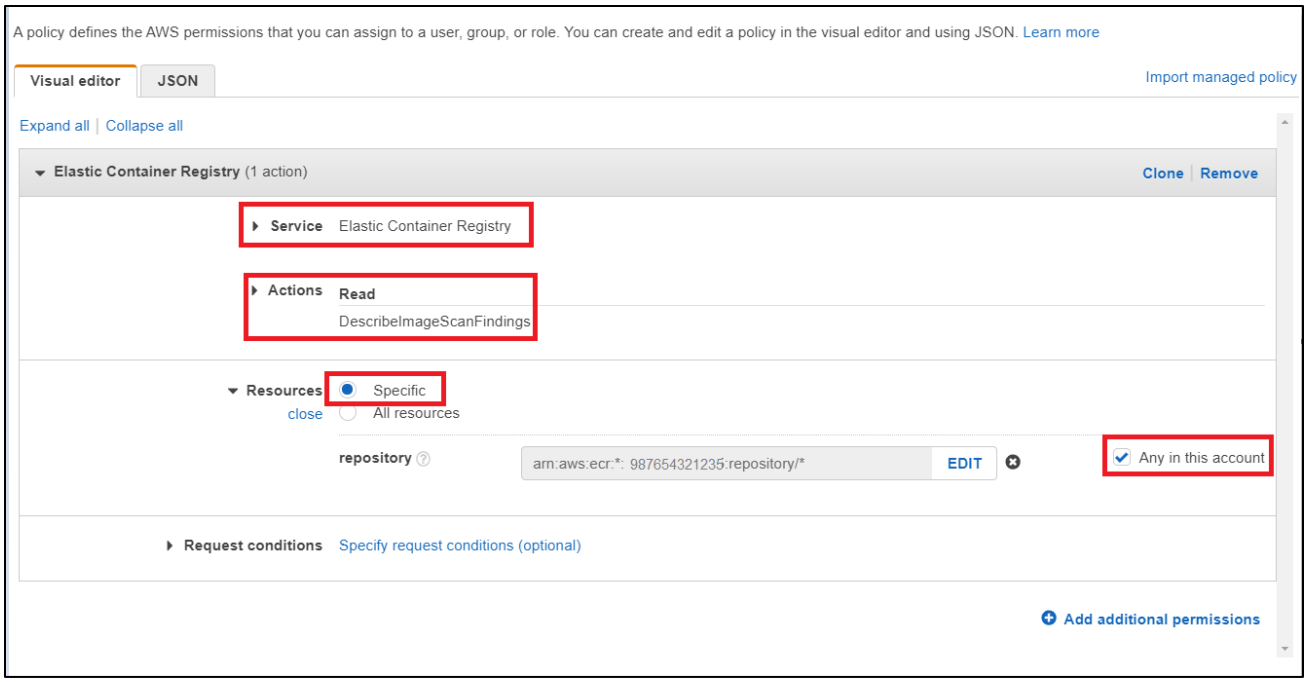


5. Under the **Select event bus** section, select "AWS default event bus" and make sure "Enable the rule on the selected event bus" is Active.
6. Under the **Select targets section** choose the lambda function and select the EventTracker lambda function as the target and click the **Add target.**



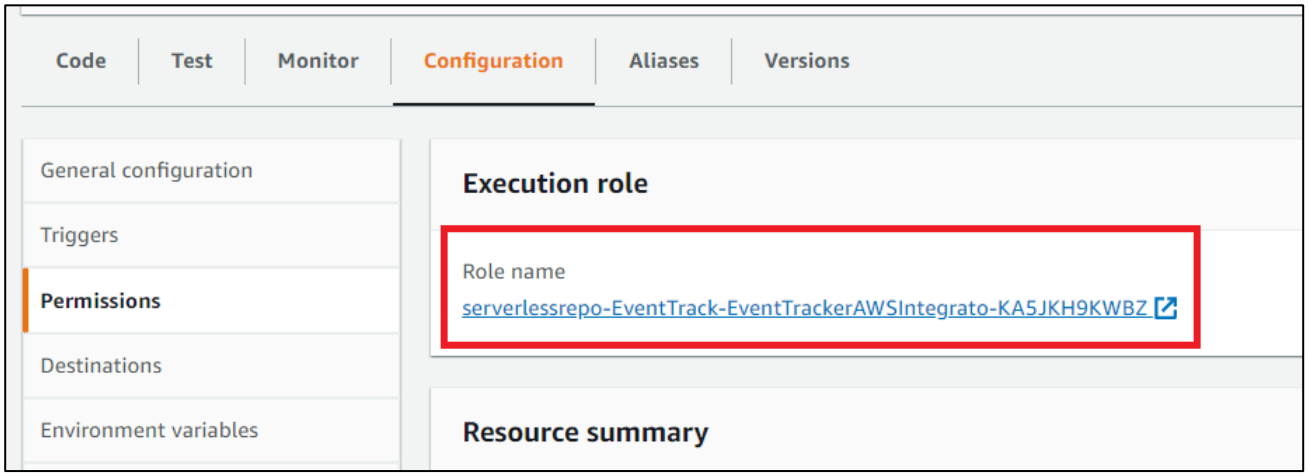
3.5 Attaching a policy to the Lambda function

1. Click the services and select **IAM**.
2. In the IAM navigation pane, select **Policies**, and further click the **Create Policy**.
3. Under the **Visual editor** tab, select **Service** as "Elastic Container Registry".
4. Under **Actions**, go to **Read** section and select the checkbox for **DescribeImageScanFindings**.

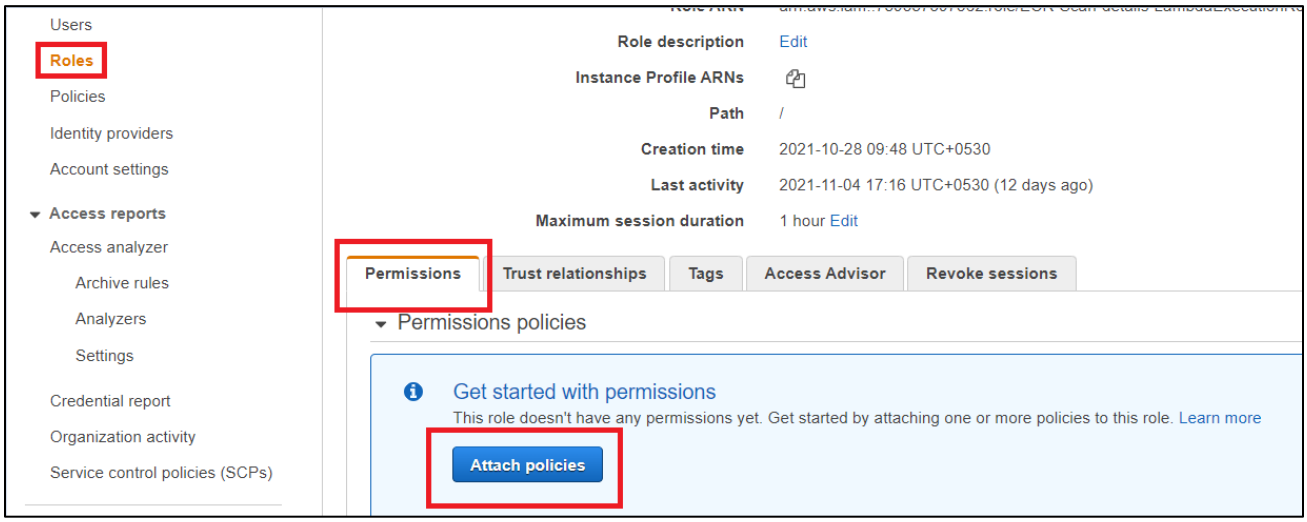


5. Under **Resources,** select the **Specific** radio button and the **Any in this account** checkbox.
6. Provide a suitable name and description to the policy and click the **Create policy**.
7. Once done, cross-check the policy created by doing a search in the policy page with the name with which it was created.

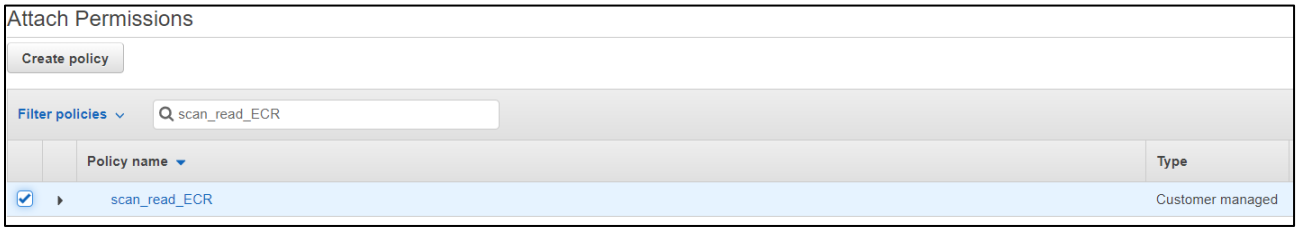
8. Go to the EventTracker lambda function in AWS Lambda, choose **Permissions** in the **Configuration** tab, and click the **Role** name, which will open the corresponding IAM page related to it.



9. Click the **Attach policies** in the permissions tab under **Roles**.



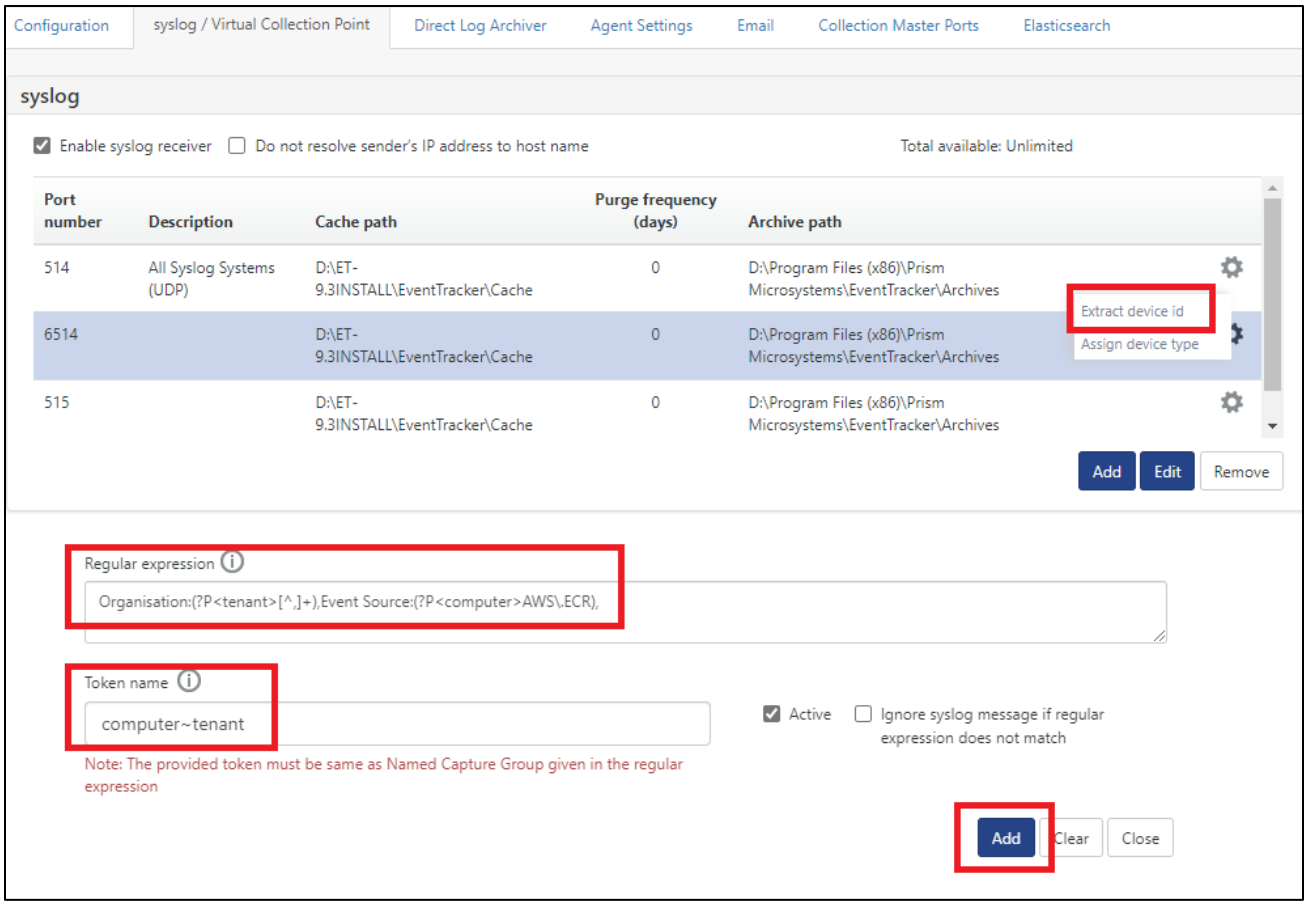
10. Type the name of the policy created in the previous steps, click the checkbox for it, and click the **Attach policy**, which will provide the **describeimagescanfinding** permission to the EventTracker lambda function.



4. System Extraction

1. Login to the **EventTracker Manager**.
2. Navigate to **Admin > Manager > syslog/Virtual Collection Point**.
3. Hover over the gear icon for getting the **Extract Id** option. Click the **Extract device Id** for extracting the system name using the below regexs:
4. Fill in the following details:
   (For Vulnerability scan)
   Regular expression: Organisation:(?P<tenant>[^,]+),Event Source:(?P<computer>AWS\.ECR),
   Token Name: computer~tenant

   (For CloudTrail logs)
   Regular expression: Organisation:(?P<Tenant>[^,]+).*?"eventSource":"(?P<Computer>[^"]+)
   Token Name: computer~tenant



5. Click the **Add** button for saving the extraction logic.

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