

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

Τa	ble	e of Contents	3
1.	(Overview	4
2.	F	Prerequisites	4
3.	I	Integrating AWS CloudTrail with EventTracker	4
	3.1	Enabling CloudTrail Logging	4
	3.2	Implementing EventTracker Lambda function	6
	3.3	3 Creating Subscription filters for CloudWatch	8
	3.4	Creating Rules in Amazon EventBridge	8
	3.5	Attaching a policy to the Lambda function	10
4.	S	System Extraction	12
	Ab	out Netsurion	14
	Со	ntact Us	14



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 <u>AWS console</u>.
- 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 <u>AWS CloudTrail</u>.
- 2. Navigate to the Trails section and click the Create trail button.

CloudTrail ×	CloudTrail > Trails
Dashboard Event history Insights	Trails C Delete Create trail
Trails	Name Home region Multi- region Organization trail S3 Log file CloudWatch Logs Status St
Documentation 🗹 Forums 🖸 FAQs 🗹	No trails No trails to display. Create trail
Use the old console	4F

3. Provide the Trail name and enable CloudWatch Logs.

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-828890237078-8aaac850 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
CloudTrailRoleForCloudWatchLogs_{trail-name} Policy document

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

Events Info Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply 🔀						
Event type Choose the type of events that you want to log.						
Management events	Data events	Insights events				
Capture management operations performed on your AWS resources.	Log the resource operations performed on or within a resource.	Identify unusual activity, errors, or user behavior in your account.				

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

	Cancel	Previous	Create trail	
It starts condinates ClaudTrail lags to ClaudMatch				

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.

aws	Services 🔺	Q Search for services, feature
	★ Favorites Add favorites by clicking on the star next to the service name. Recently visited Route 53 CloudWatch Lambda Console Home	All services Compute EC2 Lightsail [2] Lambda Batch Elastic Beanstalk Serverless Application Repository AWS Outposts EC2 Image Builder
		a storage

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

AWS Lambda ×	Lambda > Functions											١
Learn more	Functions (2)					Last fetched now	C	Actions	¥.	Create function		
Dashboard	Q Filter by tags and attributes or search by keyword									$\langle 1 \rangle$	0	
Applications Functions	Function name	⊽	Description	Package type ⊽	Runtime		⊽	Code size	⊽	Last modified	⊽	

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

Lambda > Functions > Create function Create function Info Choose one of the following options to create your funct	ion.		
Author from scratch O Start with a simple Hello World example.	Use a blueprint OBUII a Lambda application from sample code and configuration presets for common use cases.	Container image O	Browse serverless app repository O Deploy a sample Lambda application from the AWS Serverless Application Repository.
Public applications (1) Private applications Q. EventTracker	Info X		Sort by Best Match ▼ < 1 > >
ETS-AWS-Logforwarder This function will help sending the CloudWatch logs to EventTracker manager via syslog. EventTracker. (TS_AWS_Logforwarder) (LogSender) Netsurion 0 deployments			

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

pplication settings
pplication name ne stack name of this application created via AWS CloudFormation
ETS-AWS-Logforwarder
EventTrackerAWSIntegrator
ventTrackerManagerIP ventTracker Manager IP Address (e.g. 1.1.1.3)
rganisationName rganisation Name (e.g. Contoso)
yslogOverTLS nable Syslog Over TLS (e.g. true or false)
true
yslogPort rentTracker Syslog VCP Port (e.g. 4514)
Cancel Previous 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.

► Log group details			
Log streams Metric filters Subscription filters Contributor	Insights		
Subscription filters (0) We now support up to 2 subscription filters per log group.			C Delete Create ▼ < 1 >
Filter name	Filter pattern	♥ Destination ARN	⊽
	No subs	ription filter	
	Create Elasticsearch subscription filte	r Create Lambda subscription filter	

- 5. Click the Create Lambda subscription filter.
- 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**.

Rules (2/2)				C Edit Delete Enable Create rule
Q Find rules			Any status 🔻	< 1 > 💿
Name	▲ Status	⊽ Туре	▽ Description	

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

Name and description
Name
ECR_Image_Scan
Maximum of 64 characters consisting of lower/upper case letters, ., -,
Description - optional
This will forward ECR Image scan results to the lambda function.

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"]
}
```

Define pattern	
Build or customize an Event Pattern or set a Schedule to in	voke Targets.
• Event pattern Info Build a pattern to match events	Schedule Info Invoke your targets on a schedule
 Event matching pattern You can use pre-defined pattern provided by a service or create a custom pattern Pre-defined pattern by service Custom pattern 	Event pattern Copied Copied Edit 1 { 2 "detail-type": ["ECR Image Scan"], 3 "source": ["aws.ecr"], 4 "detail": { 5 "scan-status": ["COMPLETE"] 6 } 7 }

- 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**.

Select targets						
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).						
Target Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).	Remove					
Lambda function	•					
Function						
Select function						
Q						
serverlessrepo-EventTrack-EventTrackerAWSIntegrato-KXiZcxguojy1						
Retry policy and dead-letter queue						
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.

A policy defines the	e AWS permis	sions that you o	can assign to a user, grou	p, or role. You can create and edit a policy in the visual ed	itor and using JSON. L	earn more
Visual editor	JSON					Import managed policy
Expand all Colla	apse all					^ ^
	tainer Registi	ry (1 action)				Clone Remove
		 Service 	Elastic Container Regis	try		
		 Actions 	Read DescribelmageScanFin	dings		
		 Resources close 	Specific All resources			
			repository ③	arn:aws:ecr:*: 987654321235:repository/*	EDIT	 Any in this account
	▶ Reque	est conditions	Specify request condition	ons (optional)		
						Add additional permissions



- 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.

Policies > scan_read_ECR Summary	Delete policy
Policy ARN arr.:aws.iam:: 987854321235 :policy/scan_read. Description This permission grants describeimagescanfind Permissions Policy usage Tags Policy versions Access Advisor	ECR 🖉
<pre>Policy summary {}JSON Edit policy { "Version": "2012-10-17", "Statement": [{ "Statement": [{ "Statement": [</pre>	

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.

Code Test Monitor	Configuration Aliases Versions			
General configuration	Execution role			
Triggers Permissions	Role name serverlessrepo-EventTrack-EventTrackerAWSIntegrato-KA5JKH9KWBZ.			
Destinations				
Environment variables	Resource summary			

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



Lisors			itore / itali	un.awo.lam.roo		cun details cambdackeeditoning	
	Role description			Edit	Edit		
Roles		Instance Pr	ofile ARNs	Ch			
Policies	Dath						
Identity providers		_		'			
Account settings	Creation time Last activity Maximum session duration			2021-10-28 09:48	2021-10-28 09:48 UTC+0530 2021-11-04 17:16 UTC+0530 (12 days ago)		
, coount countigo				2021-11-04 17:16			
✓ Access reports				1 hour Edit			
Access analyzer							
Archive rules	Permissions	Trust relationships	Tags	Access Advisor	Revoke sessions		
Analyzers	✓ Permissions policies						
Settings							
Credential report Organization activity Service control policies (SCPs)	Get This At	started with permis role doesn't have any pe tach policies	ssions ermissions y	et. Get started by attac	ching one or more polici	es to this role. Learn more	

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.

Atta	ich	Permiss	ions			
Cre	Create policy					
Filt	Filter policies v Q scan_read_ECR					
	Policy name 👻					
	•	scan_r	ead_ECR	Customer managed		

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:
- 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

Configuration	syslog / Virtual Colle	ction Point	Direct Log Archiver	Agent Settings	Email	Collection Master Ports	Elasticsearch	
syslog								
Enable sys	slog receiver 🗌 Do no	t resolve send	ler's IP address to host na	me	Total available: Unlimited			
Port number	Description	Cache pat	h	Purge frequency (days)	Archiv	e path		*
514	All Syslog Systems (UDP)	D:\ET- 9.3INSTALI	\EventTracker\Cache	0	D:\Prog Micros	gram Files (x86)\Prism ystems\EventTracker\Archives	Sutract davice id	\$
6514		D:\ET- 9.3INSTALI	\EventTracker\Cache	0	D:\Prog Micros	gram Files (x86)\Prism ystems\EventTracker\Archives	Assign device type	*
515		D:\ET- 9.3INSTALI	\EventTracker\Cache	0	D:\Prog Micros	gram Files (x86)\Prism ystems\EventTracker\Archives		₽.
							Add Edit	Remove
Regula	ar expression (i)			_				
Orga	Organisation:(?P <tenant>[^,]+),Event Source:(?P<computer>AWSECR),</computer></tenant>							
Token name () computer~tenant Note: The provided token must be same as Named Capture Group given in the regular expression					Active Ignore syslog message if regular expression does not match			
						Ac	dd Clear Close	

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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #23 among <u>MSSP Alert's 2021 Top 250 MSSPs</u>.

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