Integration Guide

Integrating Amazon ECR

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.

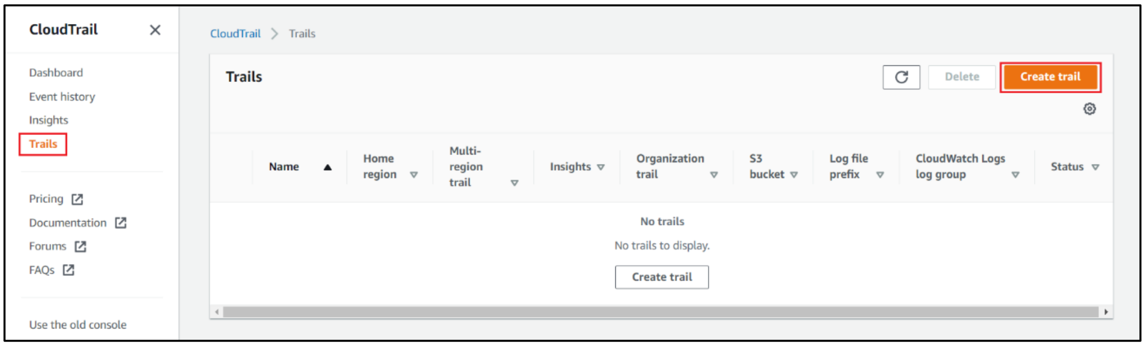
2. Prerequisites

- 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.

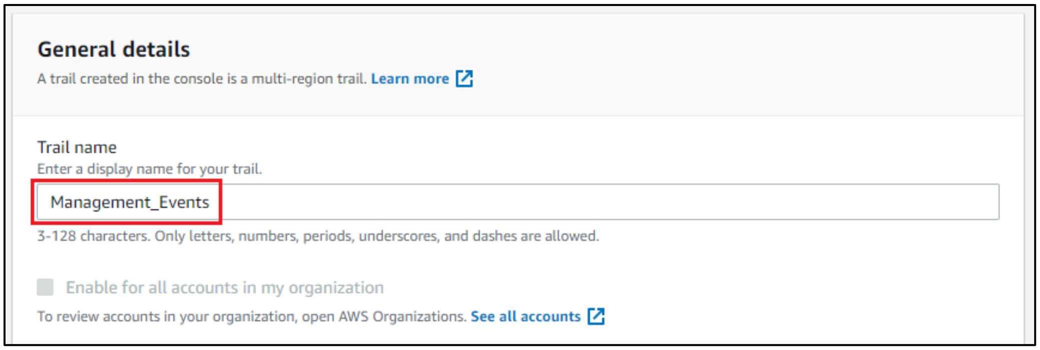


Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status

No trails

No trails to display.

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

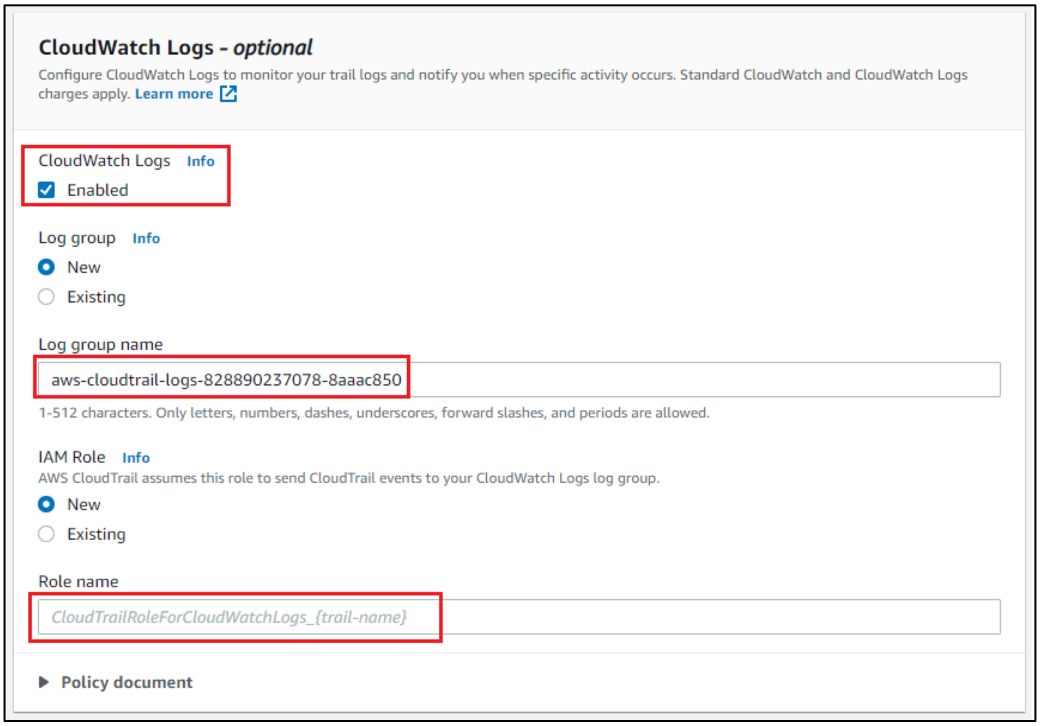
Enter a display name for your trail.

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

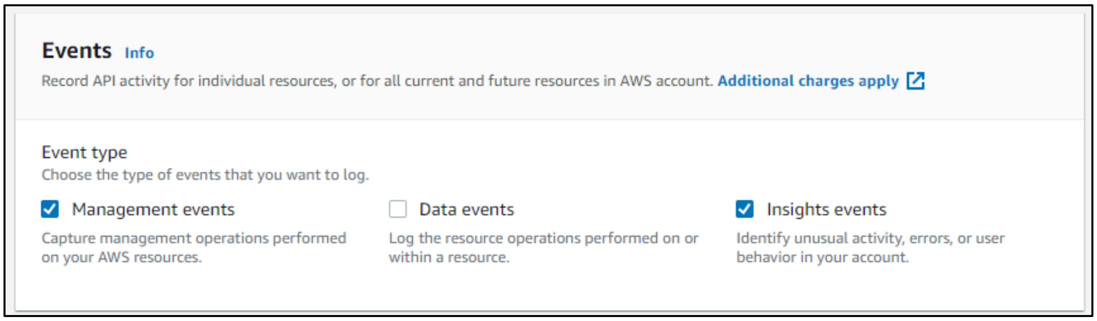
○ Existing

Role name

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

Capture management operations performed on your AWS resources.

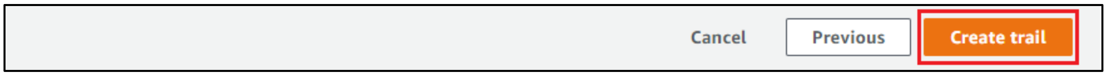
□ Data events

Log the resource operations performed on or within a resource.

☑ Insights events

Identify unusual activity, errors, or user behavior in your account.

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

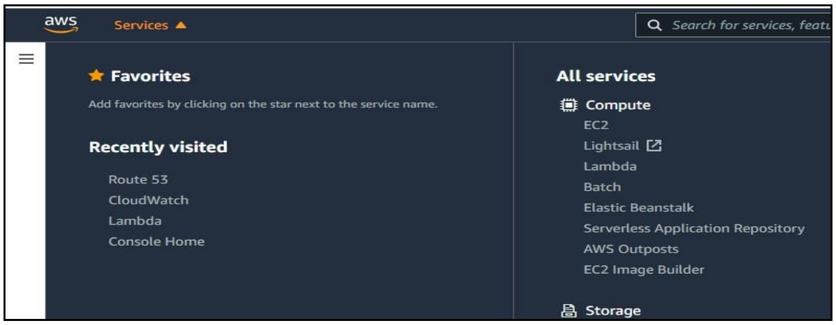


It starts sending the CloudTrail logs to CloudWatch.

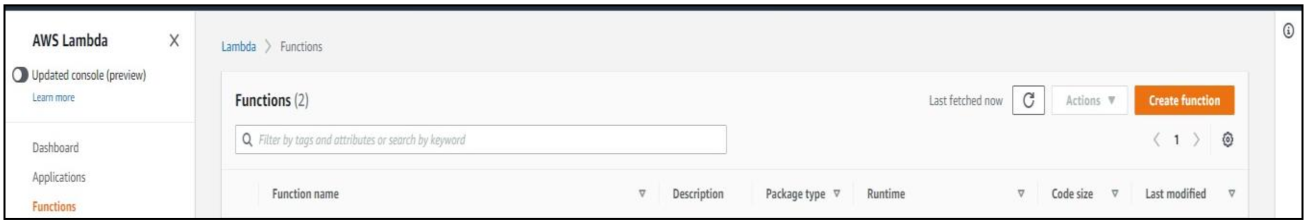
For forwarding the CloudTrail logs to EventTracker. You need to create a subscription filter for the log group which you have created in step 4. Follow the below instruction for integrating CloudWatch with EventTracker.

3.2 Implementing EventTracker Lambda function

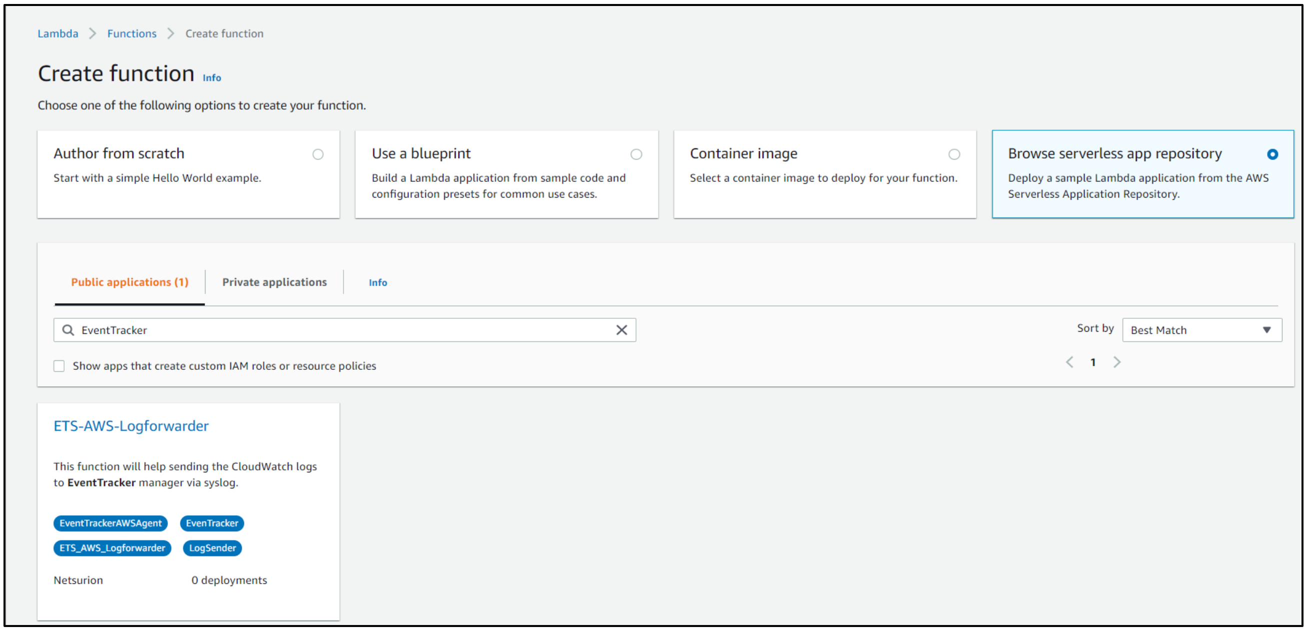
1. Click the **Services** and select **Lambda.**



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.



Lambda > Functions > Create function

Create function Info

Choose one of the following options to create your function.

○ Author from scratch — Start with a simple Hello World example.

○ Use a blueprint — Build a Lambda application from sample code and configuration presets for common use cases.

○ Container image — Select a container image to deploy for your function.

● Browse serverless app repository — Deploy a sample Lambda application from the AWS Serverless Application Repository.

EventTracker

Sort by Best Match

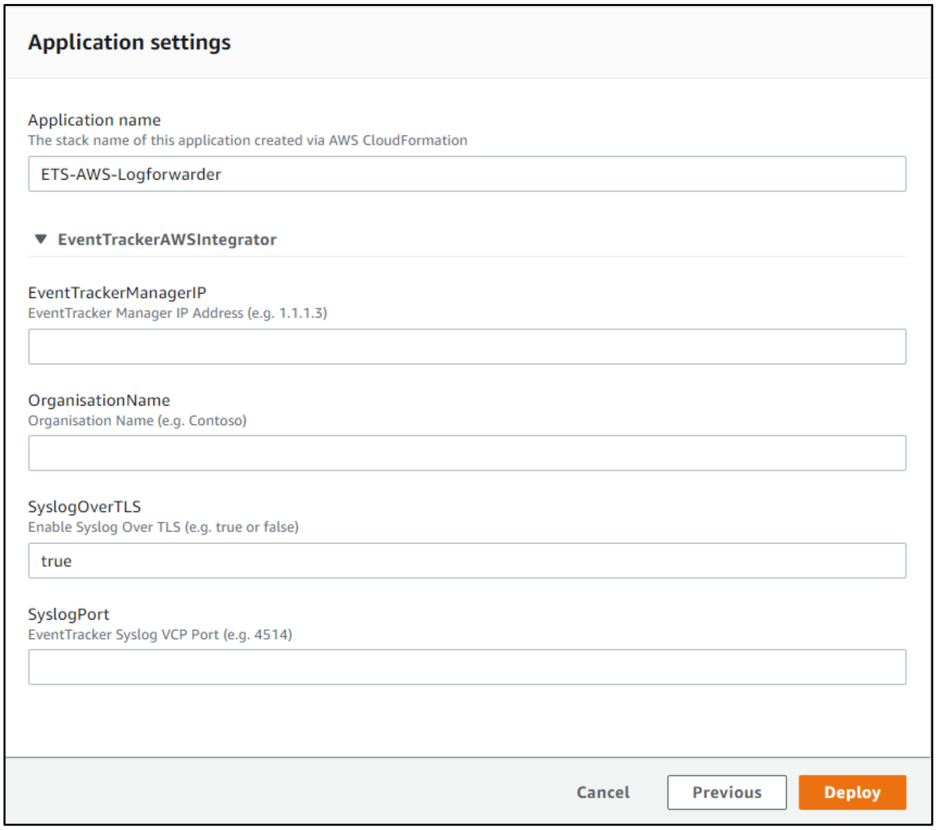
□ Show apps that create custom IAM roles or resource policies

ETS-AWS-Logforwarder

This function will help sending the CloudWatch logs to **EventTracker** manager via syslog.

Netsurion 0 deployments

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



Application settings

Application name
The stack name of this application created via AWS CloudFormation
ETS-AWS-Logforwarder

▼ EventTrackerAWSIntegrator

EventTrackerManagerIP
EventTracker Manager IP Address (e.g. 1.1.1.3)

OrganisationName
Organisation Name (e.g. Contoso)

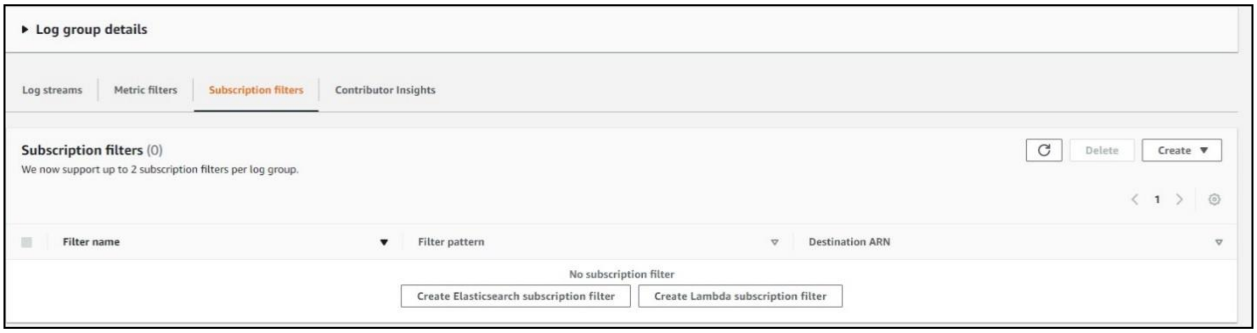
SyslogOverTLS
Enable Syslog Over TLS (e.g. true or false)
true

SyslogPort
EventTracker Syslog VCP Port (e.g. 4514)

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**.

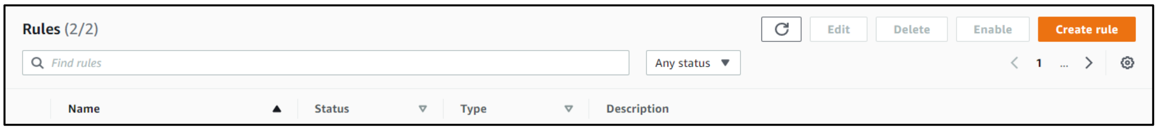


We now support up to 2 subscription filters per log group.

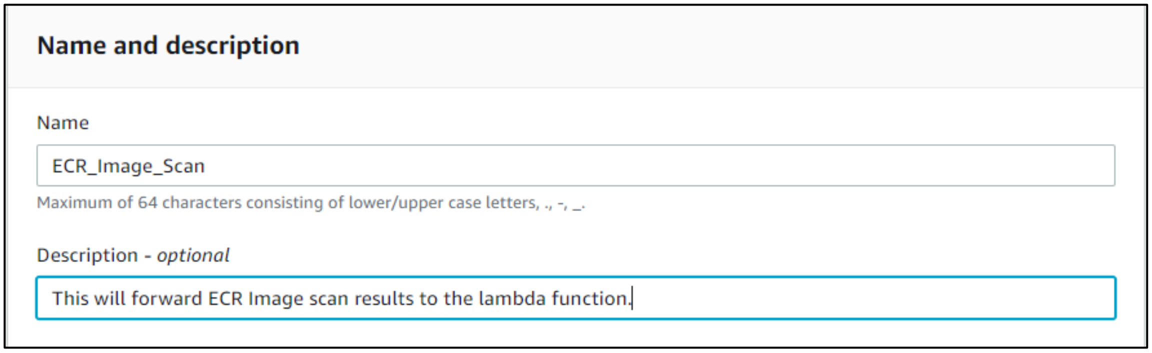
5. Click the **Create Lambda subscription filter**.
6. Under the lambda function, select the lambda function (created after deploying the application) created from the dropdown.
7. Enter subscription filter name, i.e., **CloudTrailTrigger**.
8. Click **Start streaming**.

3.4 Creating Rules in Amazon EventBridge

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



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



Name and description

Name

ECR_Image_Scan

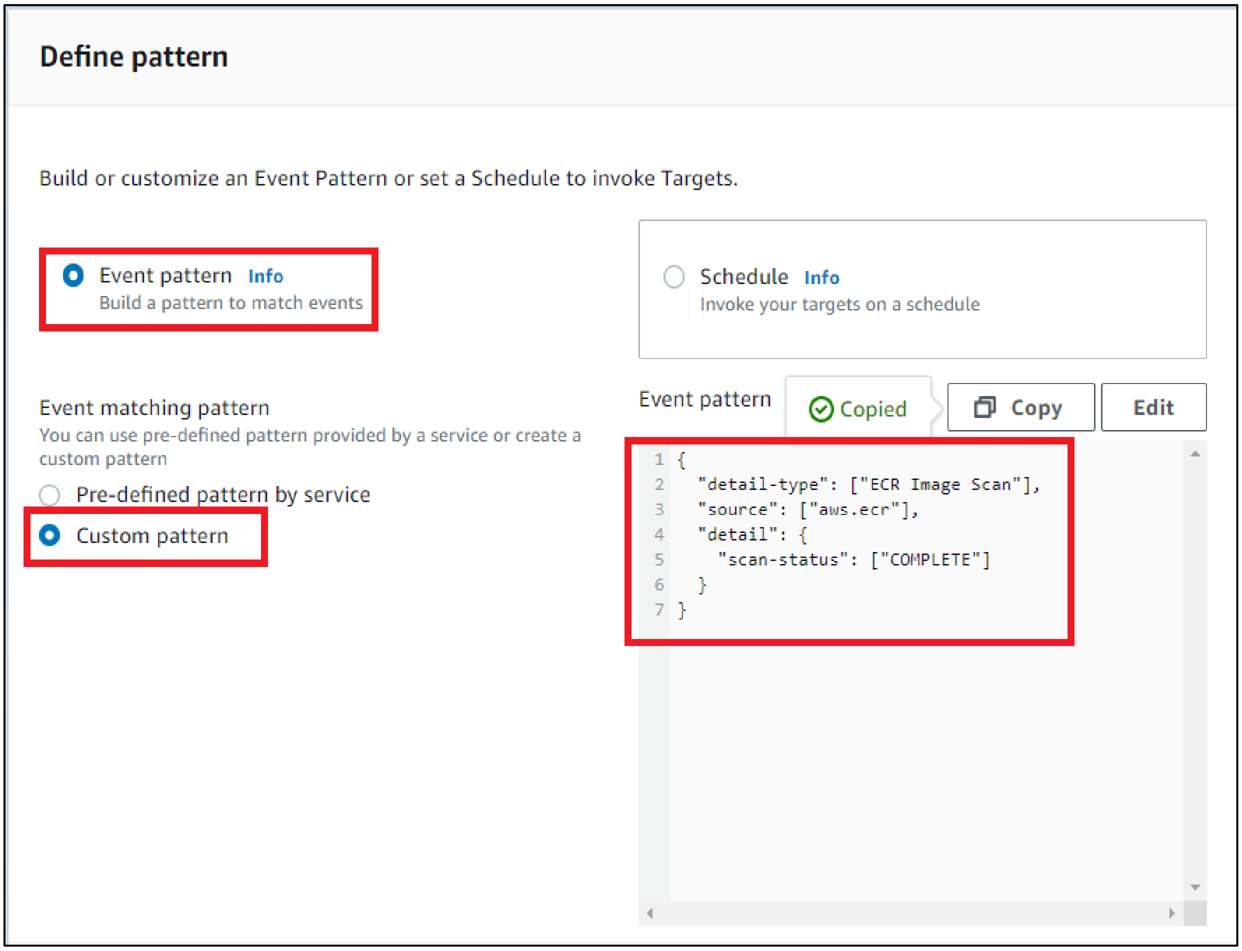
Maximum of 64 characters consisting of lower/upper case letters, ., -, _.

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 invoke Targets.

● Event pattern Info
Build a pattern to match events

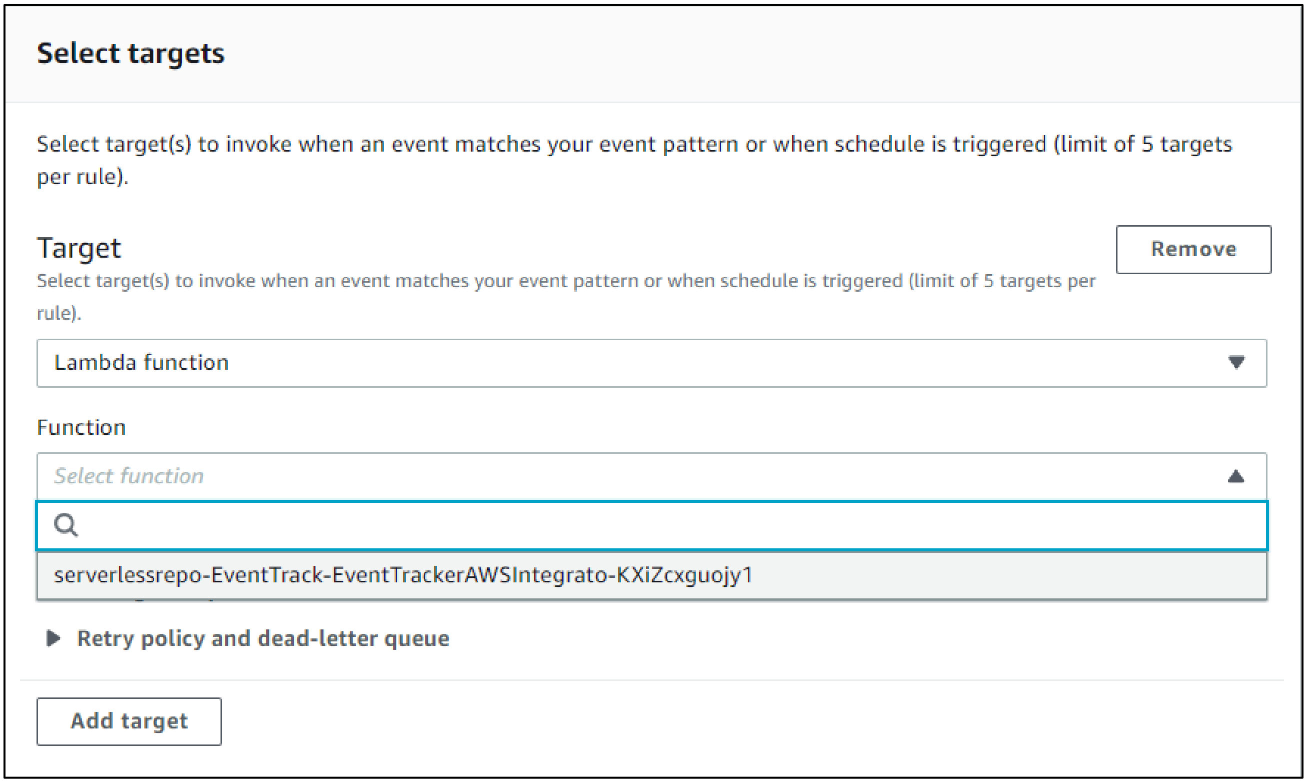
○ Schedule Info
Invoke your targets on a schedule

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

```
{
  "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.**



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).

Lambda function ▼

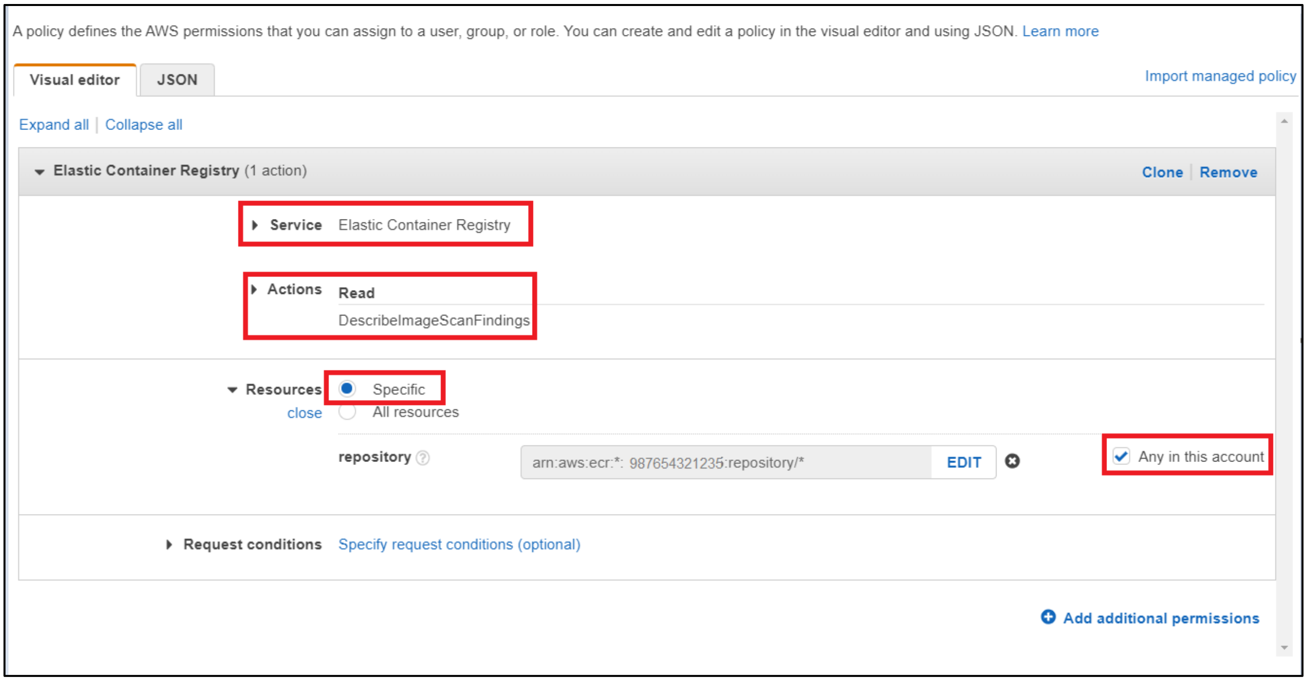
Function

Select function ▲

serverlessrepo-EventTrack-EventTrackerAWSIntegrato-KXiZcxguojy1

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 the **Read** section and select the checkbox for **DescribeImageScanFindings**.



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Elastic Container Registry (1 action)

Service: Elastic Container Registry

Actions: Read — DescribeImageScanFindings

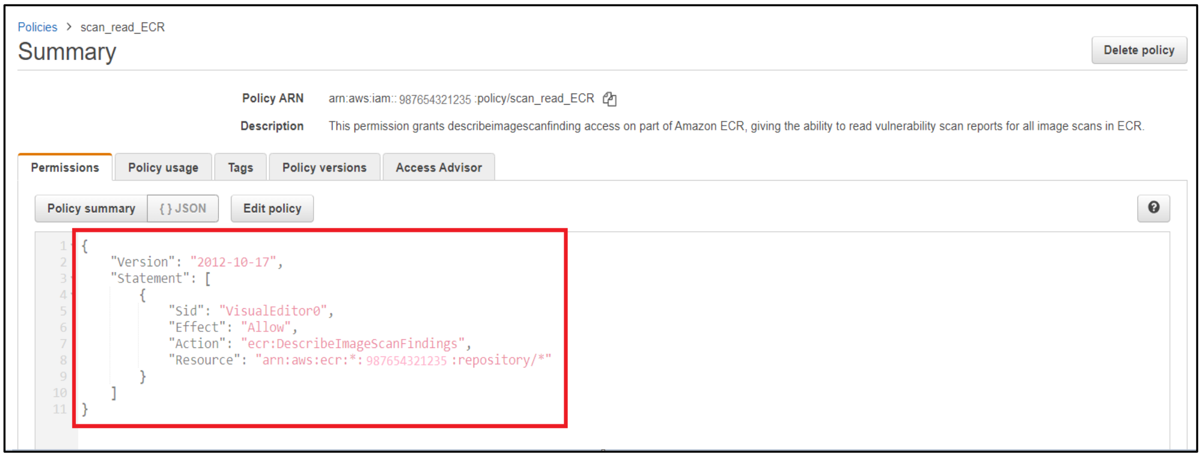
Resources: ● Specific ○ All resources

repository: arn:aws:ecr:*: 987654321235:repository/*

☑ Any in this account

Request conditions: Specify request conditions (optional)

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.

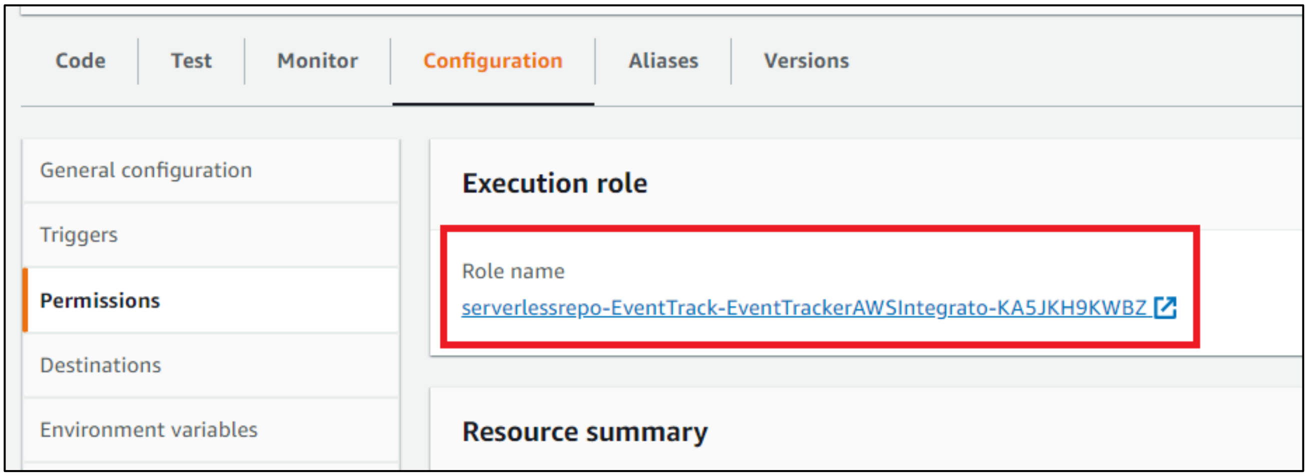


Policy ARN arn:aws:iam:: 987654321235 :policy/scan_read_ECR

Description This permission grants describeimagescanfinding access on part of Amazon ECR, giving the ability to read vulnerability scan reports for all image scans in ECR.

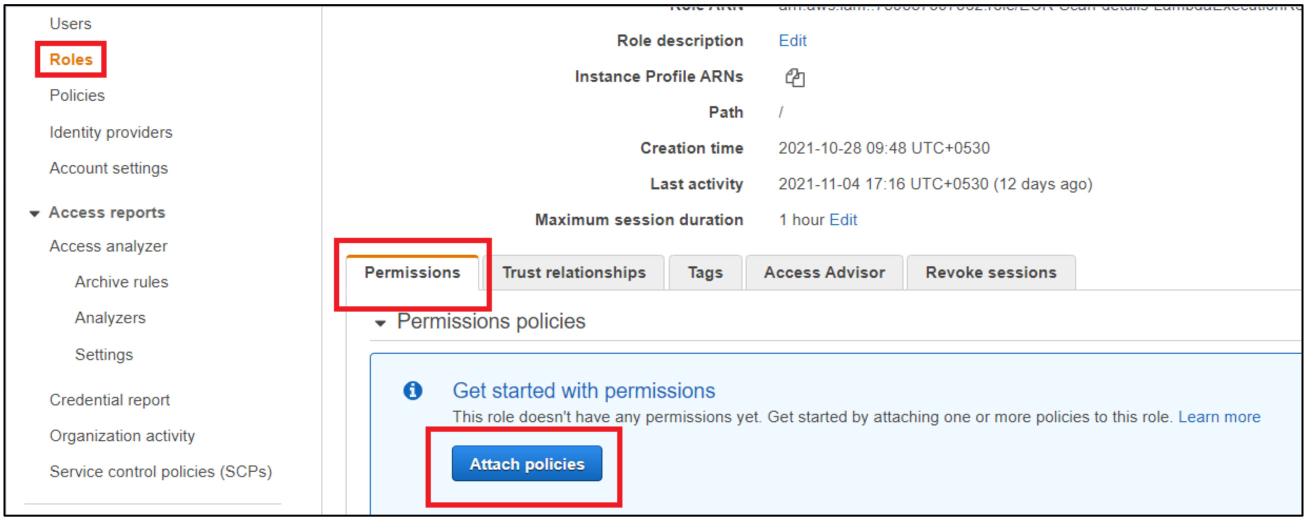
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ecr:DescribeImageScanFindings",
            "Resource": "arn:aws:ecr:*: 987654321235 :repository/*"
        }
    ]
}
```

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.



Role name
serverlessrepo-EventTrack-EventTrackerAWSIntegrato-KA5JKH9KWBZ

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

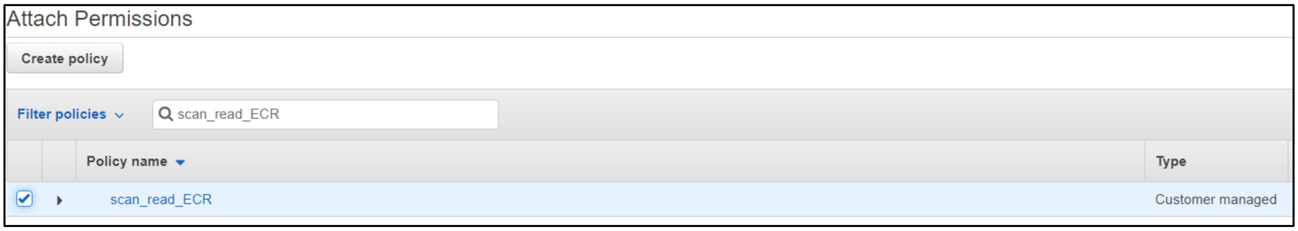


Role description: Edit
Instance Profile ARNs:
Path: /
Creation time: 2021-10-28 09:48 UTC+0530
Last activity: 2021-11-04 17:16 UTC+0530 (12 days ago)
Maximum session duration: 1 hour Edit

Get started with permissions

This role doesn't have any permissions yet. Get started by attaching one or more policies 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.

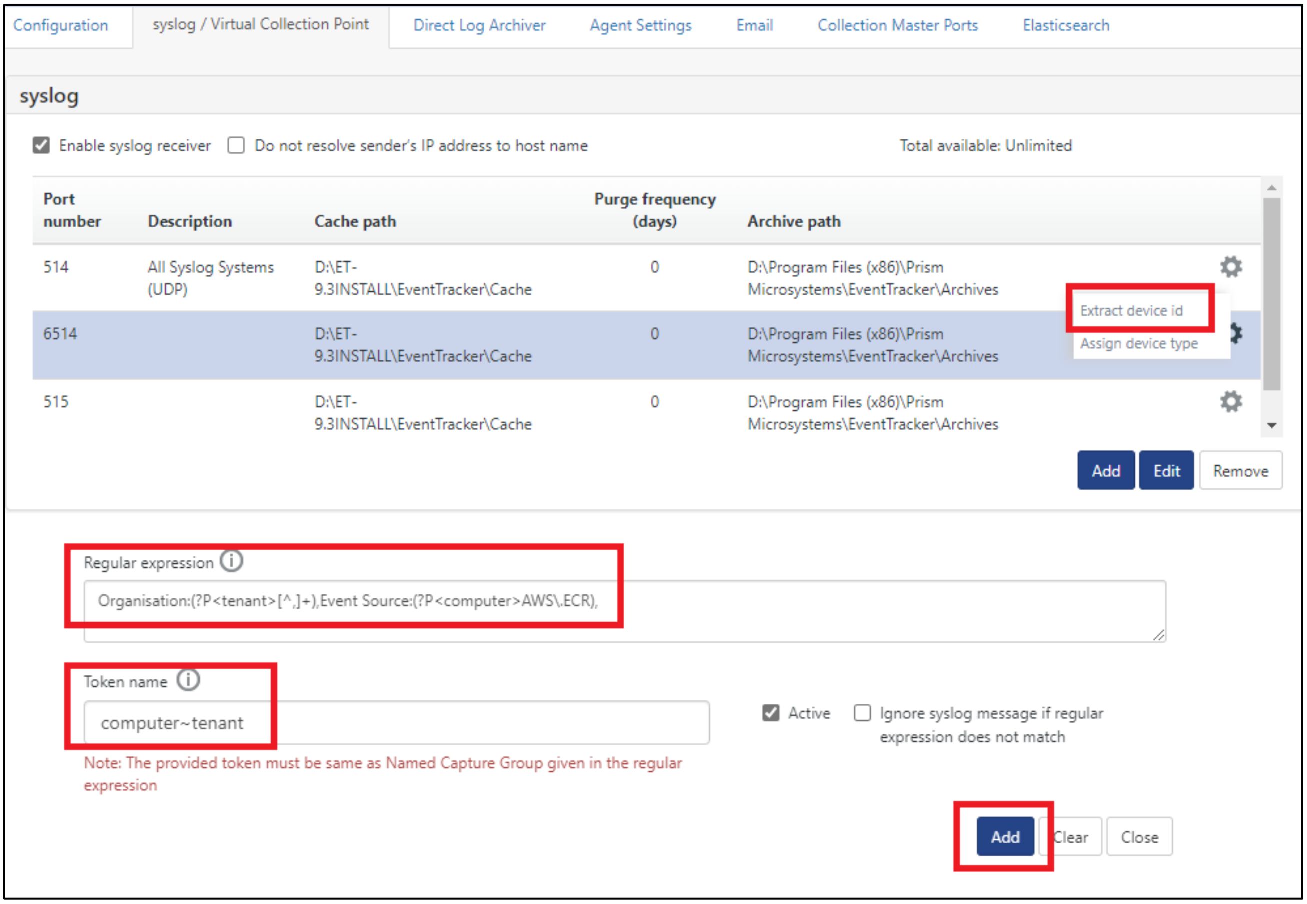


		Policy name	Type
☑	▸	scan_read_ECR	Customer managed

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:
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



syslog

☑ Enable syslog receiver ☐ Do not resolve sender's IP address to host name

Total available: Unlimited

Port number	Description	Cache path	Purge frequency (days)	Archive path
514	All Syslog Systems (UDP)	D:\ET-9.3INSTALL\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives
6514		D:\ET-9.3INSTALL\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives
515		D:\ET-9.3INSTALL\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

Regular expression

```
Organisation:(?P<tenant>[^,]+),Event Source:(?P<computer>AWS\.ECR),
```

Token name: computer~tenant

☑ Active ☐ Ignore syslog message if regular expression does not match

Note: The provided token must be same as Named Capture Group given in the regular expression

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

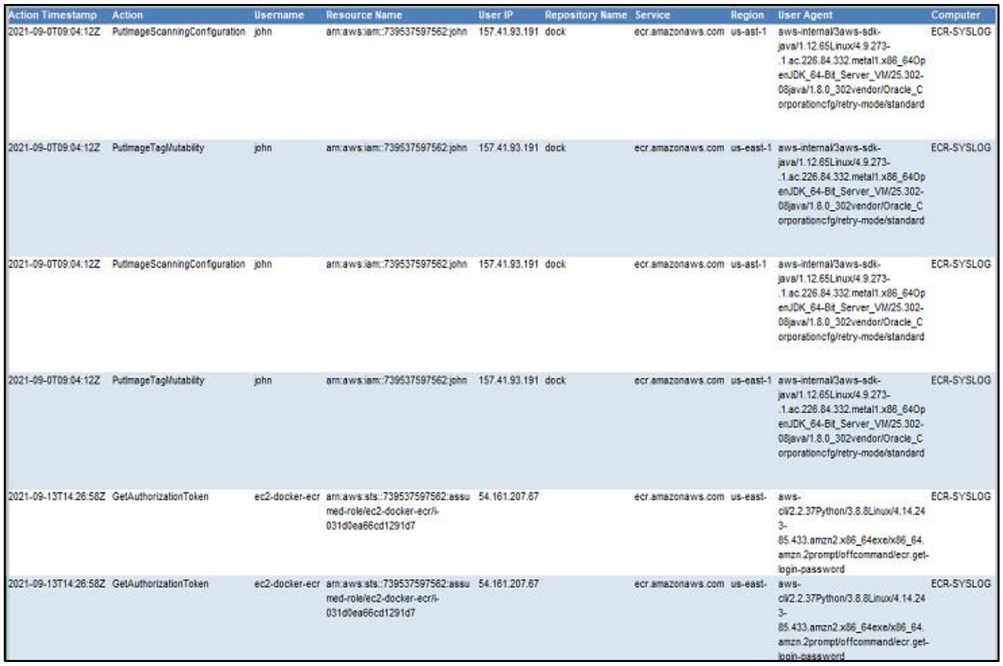
5. EventTracker Knowledge Pack

Once the logs are received by EventTracker, the Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support the services based on the CloudTrail logs:

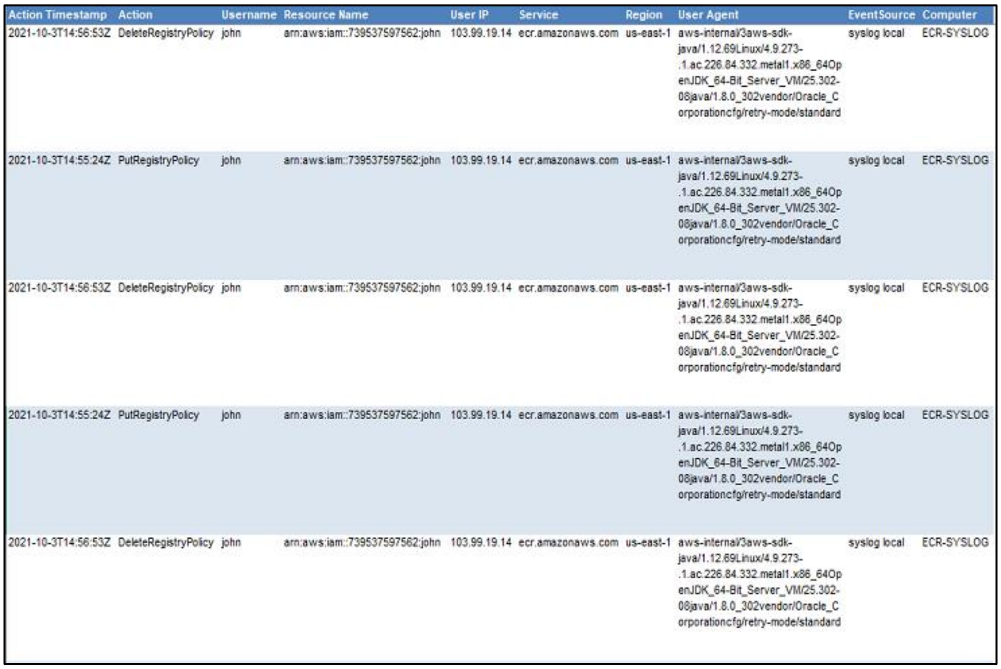
5.1 Flex Reports

- **Amazon ECR – Repository-related activities –** This report contains relevant information related to the repositories in Amazon ECR.



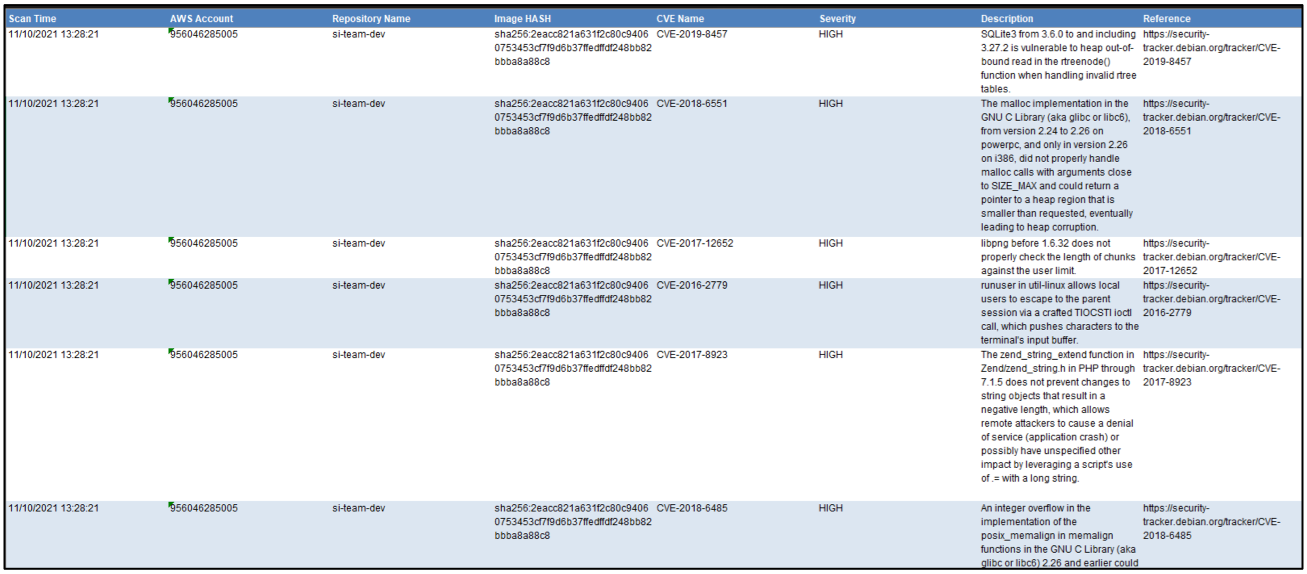
Action Timestamp	Action	Username	Resource Name	User IP	Repository Name	Service	Region	User Agent	Computer
2021-09-0T09:04:12Z	PutImageScanningConfiguration	john	arn:aws:iam::739537597562:john	157.41.93.191	dock	ecr.amazonaws.com	us-ast-1	aws-internal/3aws-sdk-java/1.12.65Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	ECR-SYSLOG
2021-09-0T09:04:12Z	PutImageTagMutability	john	arn:aws:iam::739537597562:john	157.41.93.191	dock	ecr.amazonaws.com	us-east-1	aws-internal/3aws-sdk-java/1.12.65Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	ECR-SYSLOG
2021-09-0T09:04:12Z	PutImageScanningConfiguration	john	arn:aws:iam::739537597562:john	157.41.93.191	dock	ecr.amazonaws.com	us-ast-1	aws-internal/3aws-sdk-java/1.12.65Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	ECR-SYSLOG
2021-09-0T09:04:12Z	PutImageTagMutability	john	arn:aws:iam::739537597562:john	157.41.93.191	dock	ecr.amazonaws.com	us-east-1	aws-internal/3aws-sdk-java/1.12.65Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	ECR-SYSLOG
2021-09-13T14:26:58Z	GetAuthorizationToken	ec2-docker-ecr	arn:aws:sts::739537597562:assumed-role/ec2-docker-ecr/i-031d0ea66cd1291d7	54.161.207.67		ecr.amazonaws.com	us-east-	aws-cli/2.2.37Python/3.8.8Linux/4.14.243-85.433.amzn2.x86_64exe/x86_64.amzn.2prompt/offcommand/ecr.get-login-password	ECR-SYSLOG
2021-09-13T14:26:58Z	GetAuthorizationToken	ec2-docker-ecr	arn:aws:sts::739537597562:assumed-role/ec2-docker-ecr/i-031d0ea66cd1291d7	54.161.207.67		ecr.amazonaws.com	us-east-	aws-cli/2.2.37Python/3.8.8Linux/4.14.243-85.433.amzn2.x86_64exe/x86_64.amzn.2prompt/offcommand/ecr.get-login-password	ECR-SYSLOG

- **Amazon ECR – Registry-related activities –** This report contains relevant information related to the registries in Amazon ECR.



Action Timestamp	Action	Username	Resource Name	User IP	Service	Region	User Agent	EventSource	Computer
2021-10-3T14:56:53Z	DeleteRegistryPolicy	john	arn:aws:iam::739537597562:john	103.99.19.14	ecr.amazonaws.com	us-east-1	aws-internal/3aws-sdk-java/1.12.69Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	syslog local	ECR-SYSLOG
2021-10-3T14:55:24Z	PutRegistryPolicy	john	arn:aws:iam::739537597562:john	103.99.19.14	ecr.amazonaws.com	us-east-1	aws-internal/3aws-sdk-java/1.12.69Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	syslog local	ECR-SYSLOG
2021-10-3T14:56:53Z	DeleteRegistryPolicy	john	arn:aws:iam::739537597562:john	103.99.19.14	ecr.amazonaws.com	us-east-1	aws-internal/3aws-sdk-java/1.12.69Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	syslog local	ECR-SYSLOG
2021-10-3T14:55:24Z	PutRegistryPolicy	john	arn:aws:iam::739537597562:john	103.99.19.14	ecr.amazonaws.com	us-east-1	aws-internal/3aws-sdk-java/1.12.69Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	syslog local	ECR-SYSLOG
2021-10-3T14:56:53Z	DeleteRegistryPolicy	john	arn:aws:iam::739537597562:john	103.99.19.14	ecr.amazonaws.com	us-east-1	aws-internal/3aws-sdk-java/1.12.69Linux/4.9.273-.1.ac.226.84.332.metal1.x86_64OpenJDK_64-Bit_Server_VM/25.302-08java/1.8.0_302vendor/Oracle_Corporationcfg/retry-mode/standard	syslog local	ECR-SYSLOG

- **Amazon ECR - Vulnerability scan –** This report shows relevant details related to the vulnerability scans performed by AWS when an image is pushed to an ECR repository.



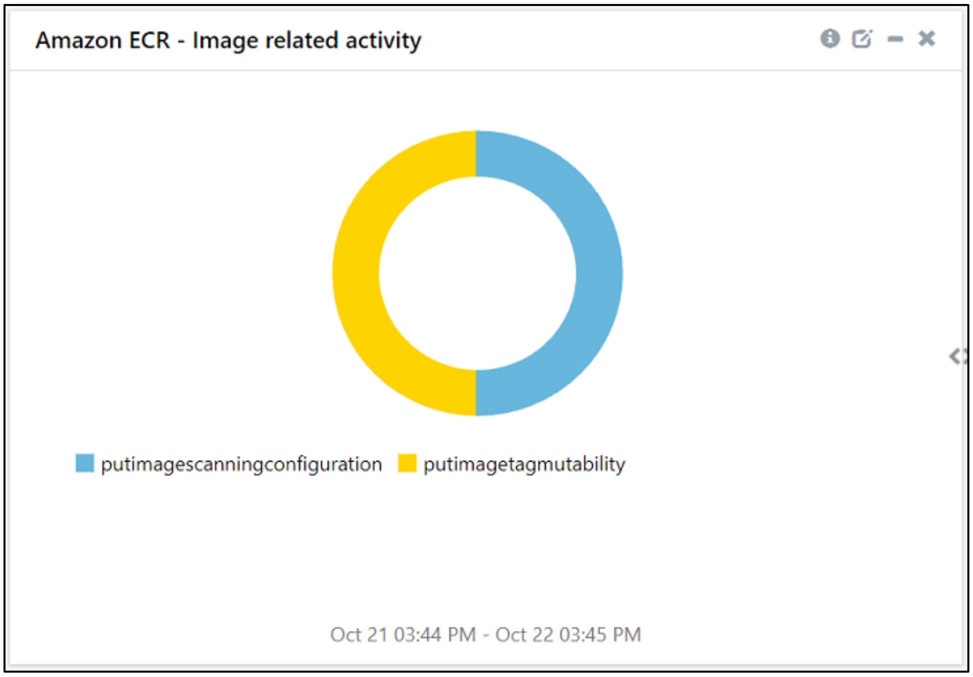
Scan Time	AWS Account	Repository Name	Image HASH	CVE Name	Severity	Description	Reference
11/10/2021 13:28:21	956046285005	si-team-dev	sha256:2eacc821a631f2c80c9406 0753453cf7f9d6b37ffedffdf248bb82 bbba8a88c8	CVE-2019-8457	HIGH	SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables.	https://security-tracker.debian.org/tracker/CVE-2019-8457
11/10/2021 13:28:21	956046285005	si-team-dev	sha256:2eacc821a631f2c80c9406 0753453cf7f9d6b37ffedffdf248bb82 bbba8a88c8	CVE-2018-6551	HIGH	The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.	https://security-tracker.debian.org/tracker/CVE-2018-6551
11/10/2021 13:28:21	956046285005	si-team-dev	sha256:2eacc821a631f2c80c9406 0753453cf7f9d6b37ffedffdf248bb82 bbba8a88c8	CVE-2017-12652	HIGH	libpng before 1.6.32 does not properly check the length of chunks against the user limit.	https://security-tracker.debian.org/tracker/CVE-2017-12652
11/10/2021 13:28:21	956046285005	si-team-dev	sha256:2eacc821a631f2c80c9406 0753453cf7f9d6b37ffedffdf248bb82 bbba8a88c8	CVE-2016-2779	HIGH	runuser in util-linux allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	https://security-tracker.debian.org/tracker/CVE-2016-2779
11/10/2021 13:28:21	956046285005	si-team-dev	sha256:2eacc821a631f2c80c9406 0753453cf7f9d6b37ffedffdf248bb82 bbba8a88c8	CVE-2017-8923	HIGH	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.	https://security-tracker.debian.org/tracker/CVE-2017-8923
11/10/2021 13:28:21	956046285005	si-team-dev	sha256:2eacc821a631f2c80c9406 0753453cf7f9d6b37ffedffdf248bb82 bbba8a88c8	CVE-2018-6485	HIGH	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could	https://security-tracker.debian.org/tracker/CVE-2018-6485

5.2 Alerts

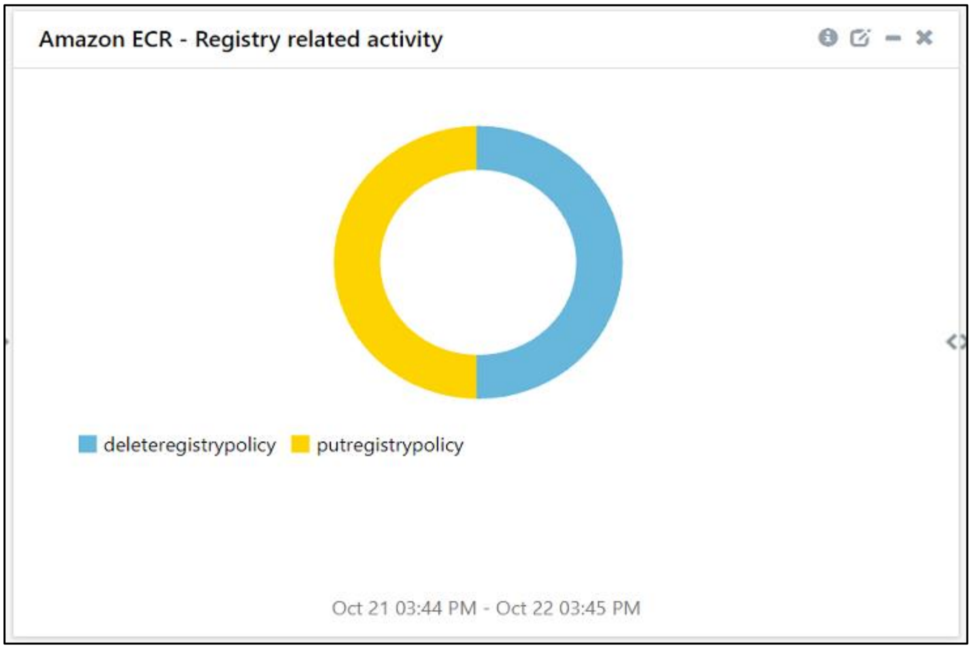
- **Amazon ECR: Forced repository deletion detected –** This alert is triggered when an ECR repository is deleted which has images present in it.
- **Amazon ECR: High priority lifecycle policy added –** This alert is triggered when a high priority lifecycle policy is added to a repository which may override the existing policies.
- **Amazon ECR: Image scan disabled –** This alert is triggered when an image scanning is changed from enabled to disabled for an ECR repository.
- **Amazon ECR: Image tag overwrite enabled -** This alert is triggered when an image tagging is changed from immutable to mutable, which disables the image overwrite protection.
- **Amazon ECR: Registry policy changes detected -** This alert is triggered when changes in the critical registry policies are detected.
- **Amazon ECR: Repository policy changes detected -** This alert is triggered when changes in the critical repository policies are detected.

5.3 Dashboards

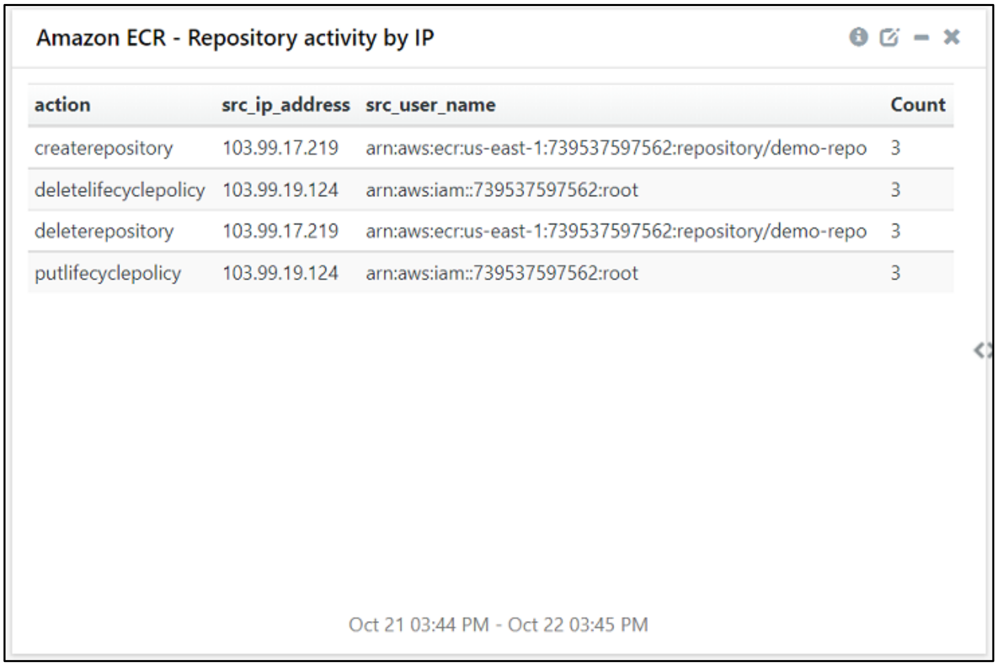
- **Amazon ECR – Image related Activity**


Amazon ECR - Image related activity
putimagescanningconfiguration
putimagetagmutability
Oct 21 03:44 PM - Oct 22 03:45 PM

- **Amazon ECR – Registry related Activity**


Amazon ECR - Registry related activity
deleteregistrypolicy
putregistrypolicy
Oct 21 03:44 PM - Oct 22 03:45 PM

- **Amazon ECR – Repository activity by IP Address**

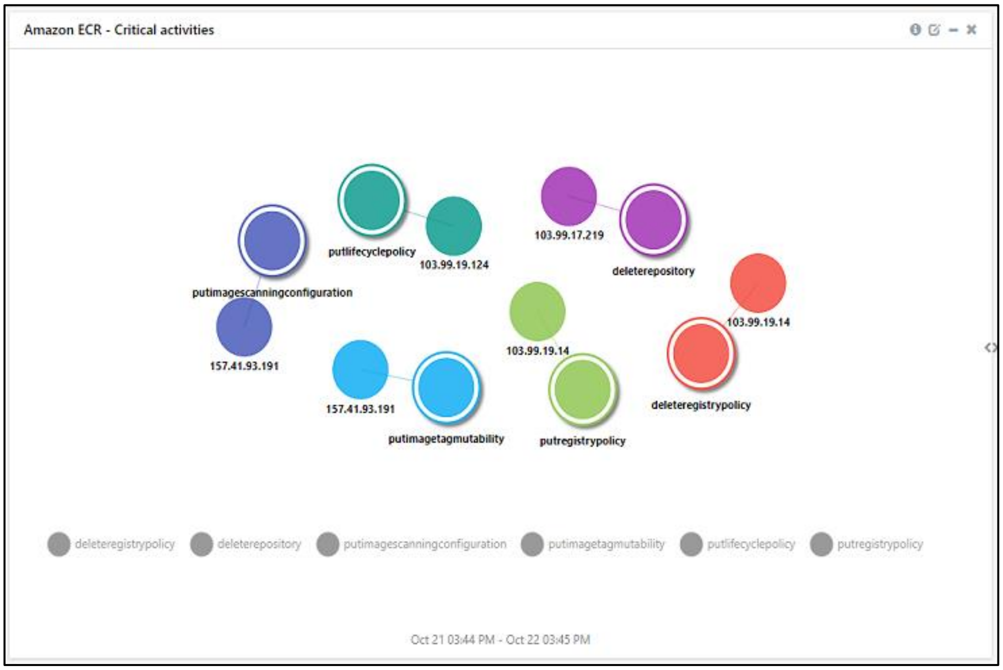


Amazon ECR - Repository activity by IP

action	src_ip_address	src_user_name	Count
createrepository	103.99.17.219	arn:aws:ecr:us-east-1:739537597562:repository/demo-repo	3
deletelifecyclepolicy	103.99.19.124	arn:aws:iam::739537597562:root	3
deleterepository	103.99.17.219	arn:aws:ecr:us-east-1:739537597562:repository/demo-repo	3
putlifecyclepolicy	103.99.19.124	arn:aws:iam::739537597562:root	3

Oct 21 03:44 PM - Oct 22 03:45 PM

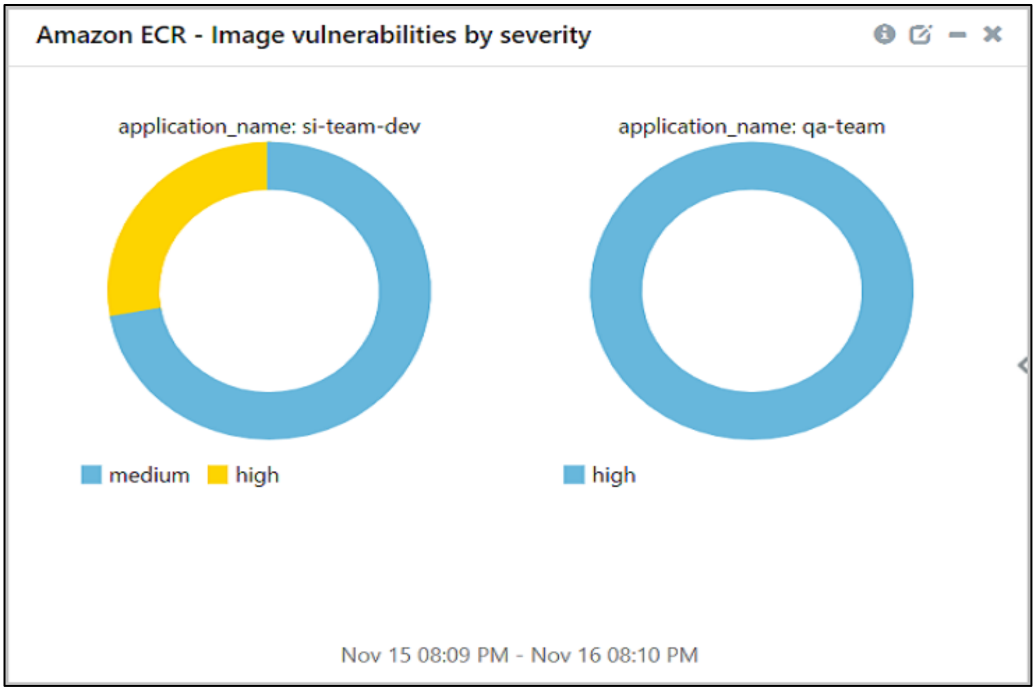
- **Amazon ECR – Critical Activities**



Amazon ECR - Critical activities

Oct 21 03:44 PM - Oct 22 03:45 PM

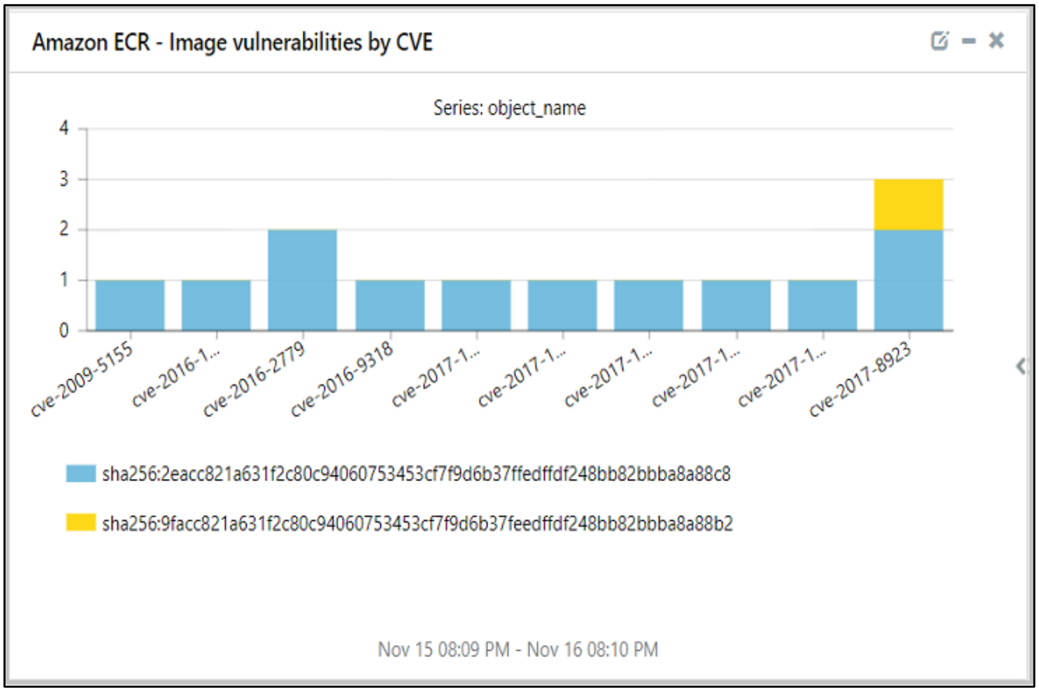
- **Amazon ECR – Image vulnerabilities by Severity**



Amazon ECR - Image vulnerabilities by severity

Nov 15 08:09 PM - Nov 16 08:10 PM

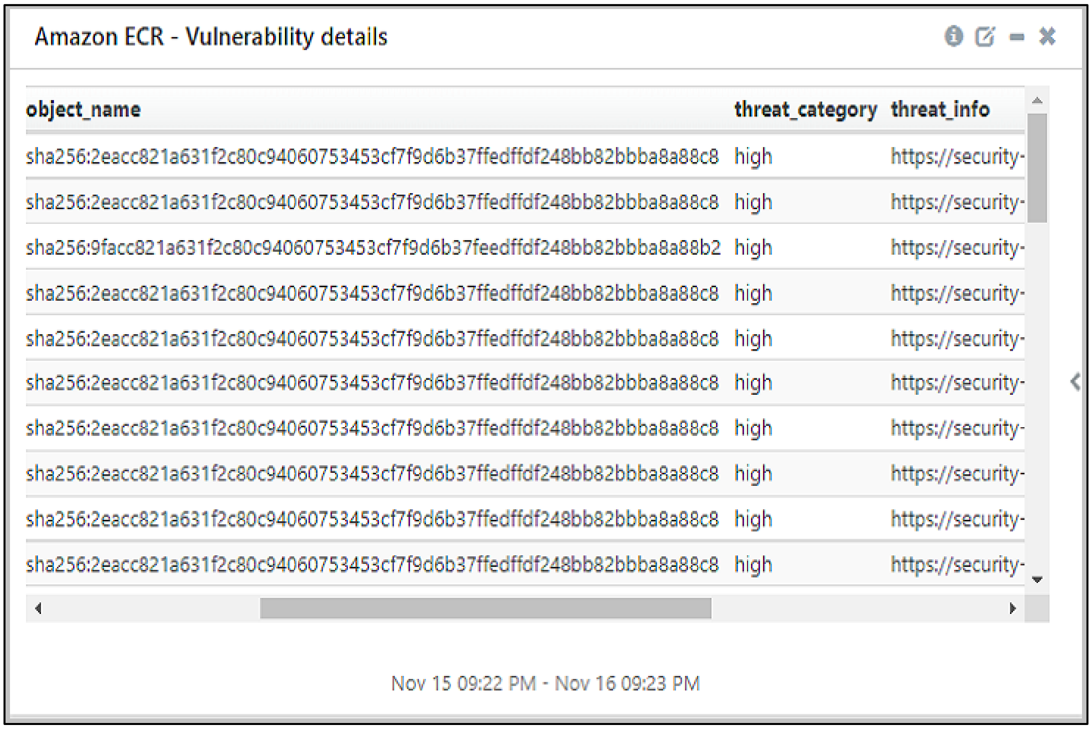
- **Amazon ECR – Image vulnerabilities by CVE**



Amazon ECR - Image vulnerabilities by CVE

Nov 15 08:09 PM - Nov 16 08:10 PM

- **Amazon ECR – Vulnerability Details**



Amazon ECR - Vulnerability details

object_name	threat_category	threat_info
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:9facc821a631f2c80c94060753453cf7f9d6b37feedffdf248bb82bbba8a88b2	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-
sha256:2eacc821a631f2c80c94060753453cf7f9d6b37ffedffdf248bb82bbba8a88c8	high	https://security-

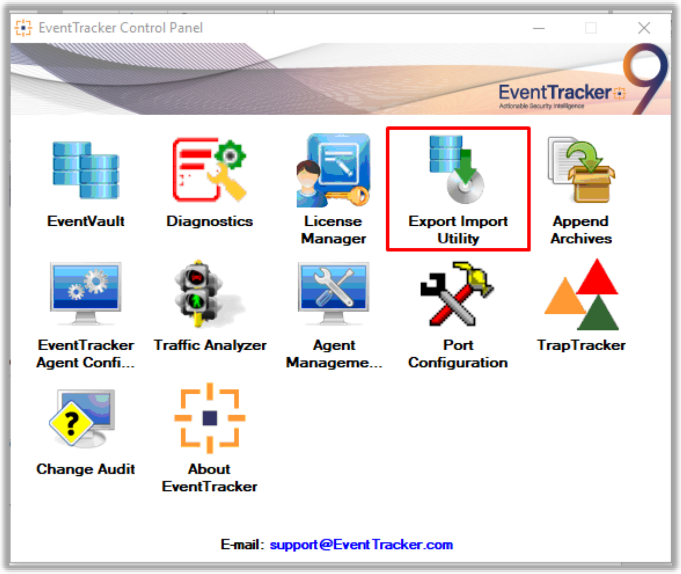
Nov 15 09:22 PM - Nov 16 09:23 PM

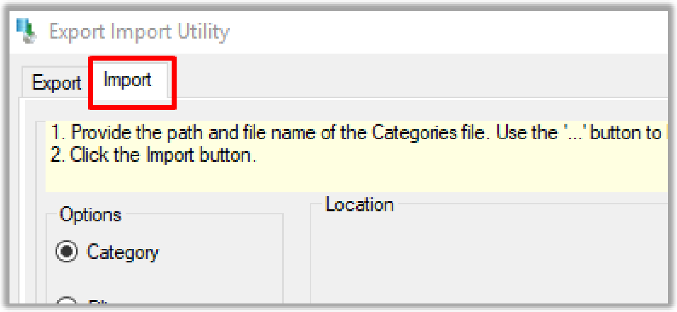
6. Importing Amazon ECR Knowledge Pack into EventTracker

NOTE: Import the Knowledge Pack items in the following sequence:

- Categories
- Alerts
- Token Values
- Knowledge Objects
- Flex Reports
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.



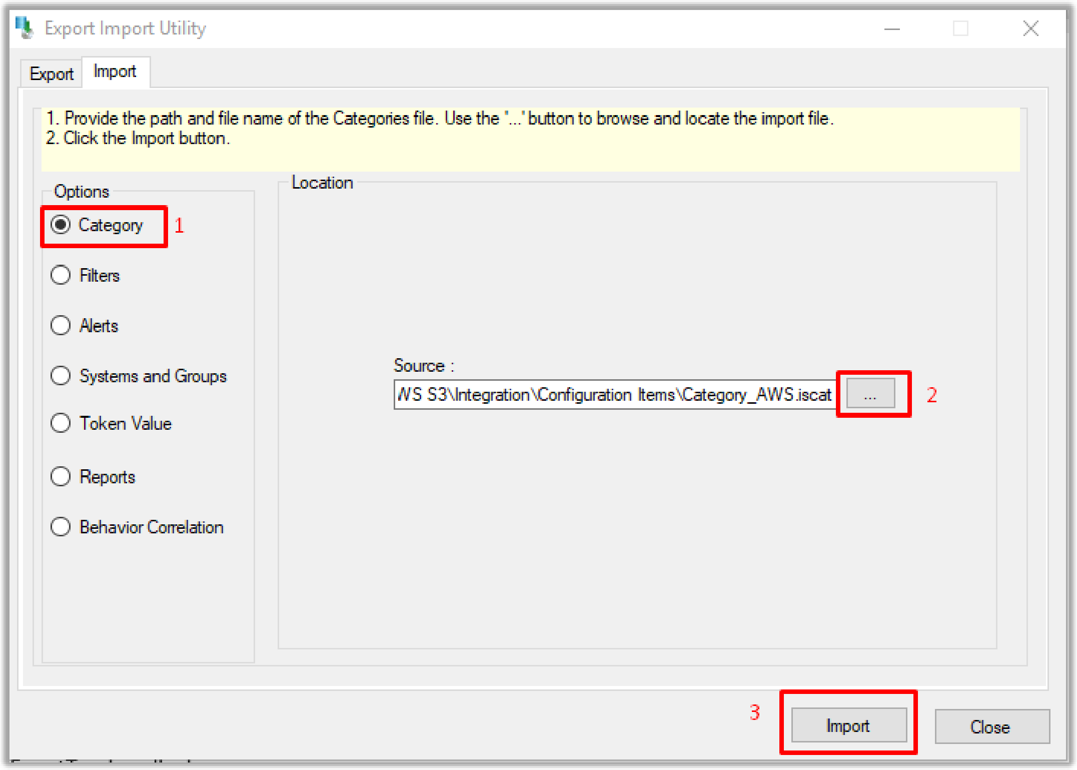


1. Provide the path and file name of the Categories file. Use the '...' button to
2. Click the Import button.

3. Click the **Import** tab.

6.1 Categories

1. Click the **Category** option, and then click the Browse ... button.
2. Navigate to the location having a file with the extension **".iscat"** and then click **Import.**

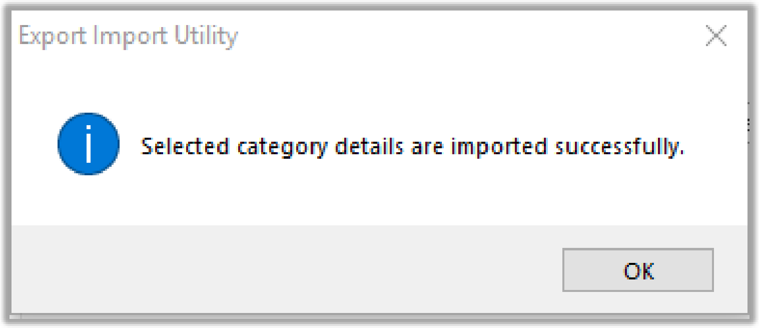


1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Source : WS S3\Integration\Configuration Items\Category_AWS.iscat

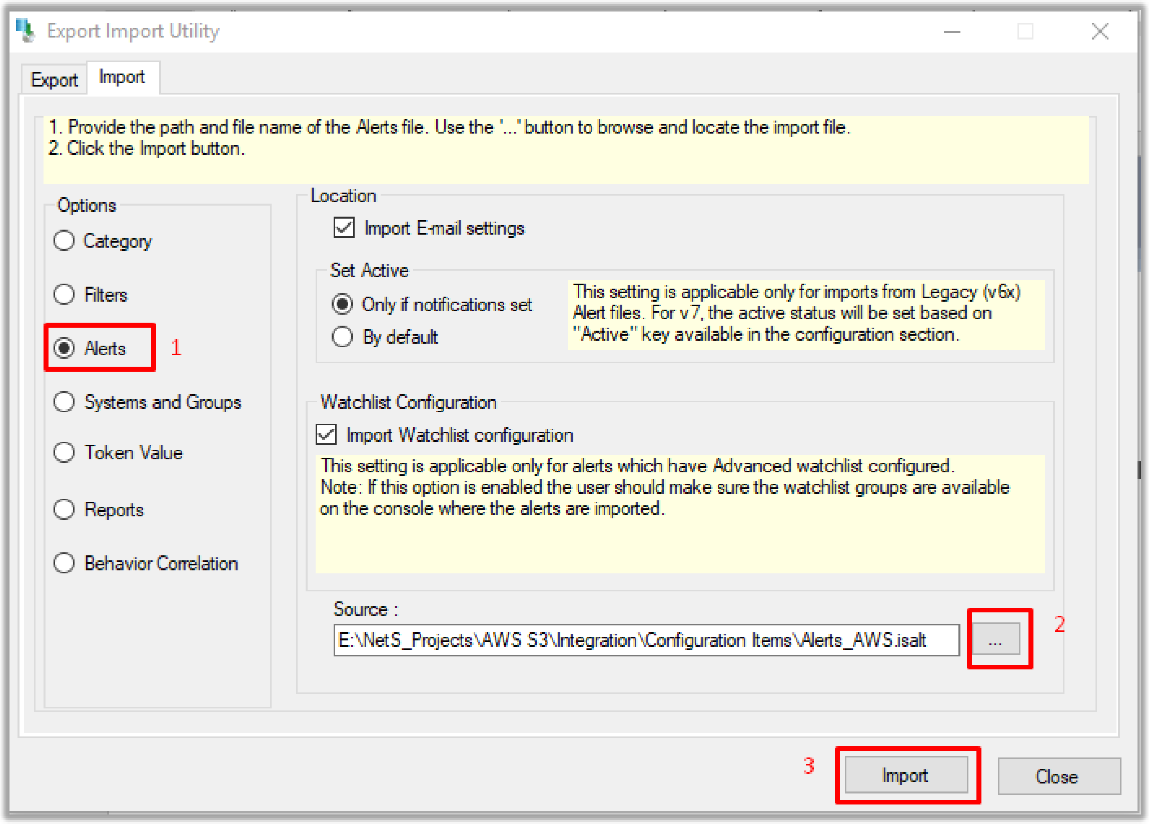
3. EventTracker displays a success message:



Selected category details are imported successfully.

6.2 Alerts

1. Click the **Alert** option, and then click the Browse ... button
2. Navigate to the location having a file with the extension **".isalt"** and then click **Import.**



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

☑ Import E-mail settings

● Only if notifications set
○ By default

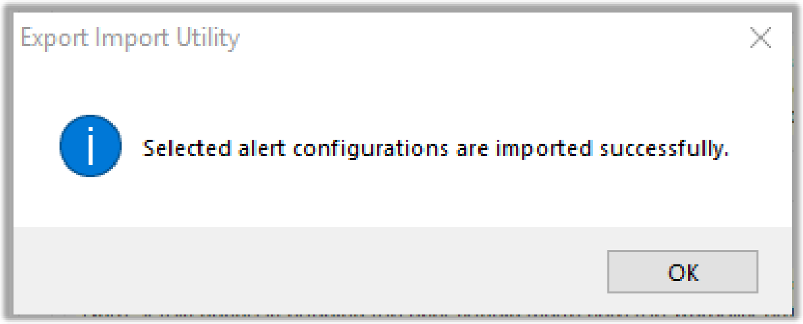
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : E:\NetS_Projects\AWS S3\Integration\Configuration Items\Alerts_AWS.isalt

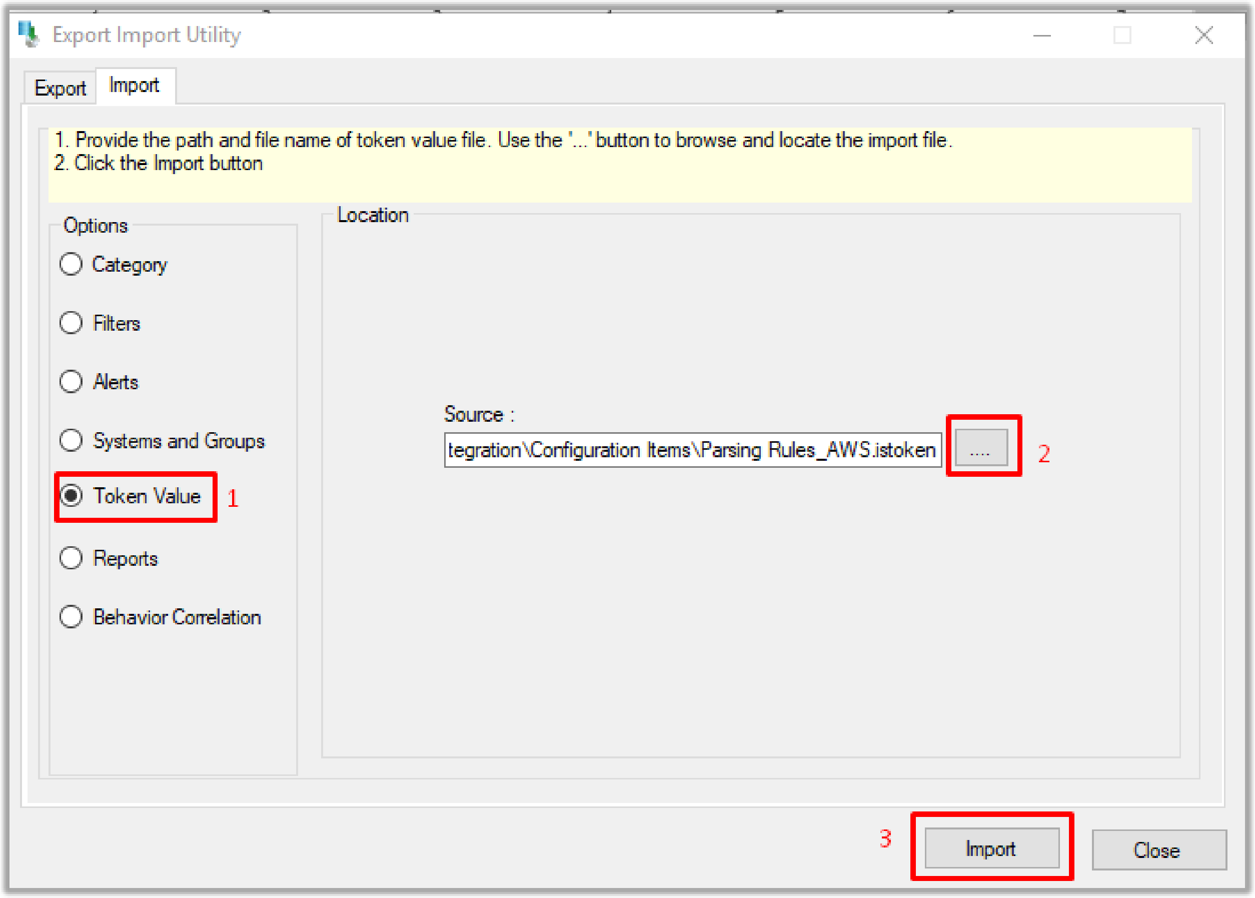
3. EventTracker displays a success message.



Selected alert configurations are imported successfully.

6.3 Token Values

1. In the EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Click the **Reports** option and choose **New (*.istoken).**
2. Navigate to the location having a file with the extension **".istoken**" and then click **Import**.

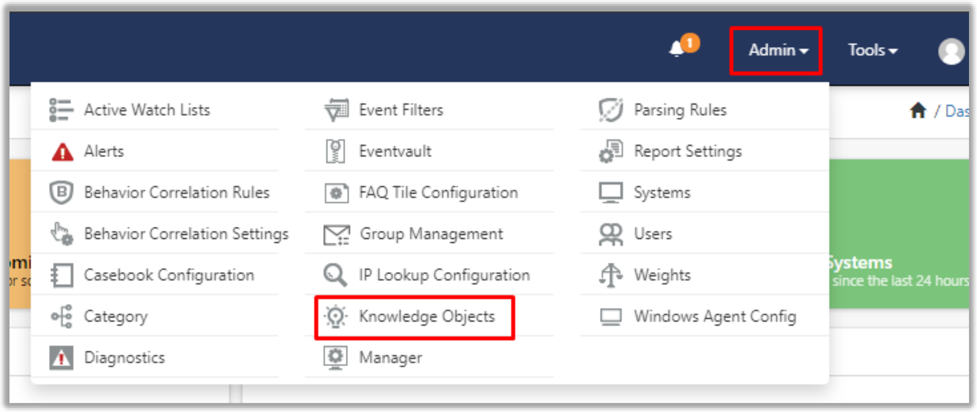


1. Provide the path and file name of token value file. Use the '...' button to browse and locate the import file.
2. Click the Import button

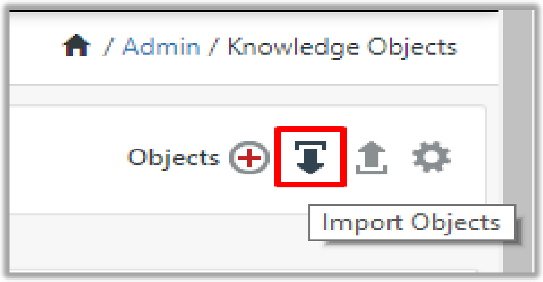
Source : tegration\Configuration Items\Parsing Rules_AWS.istoken ....

6.4 Knowledge Objects

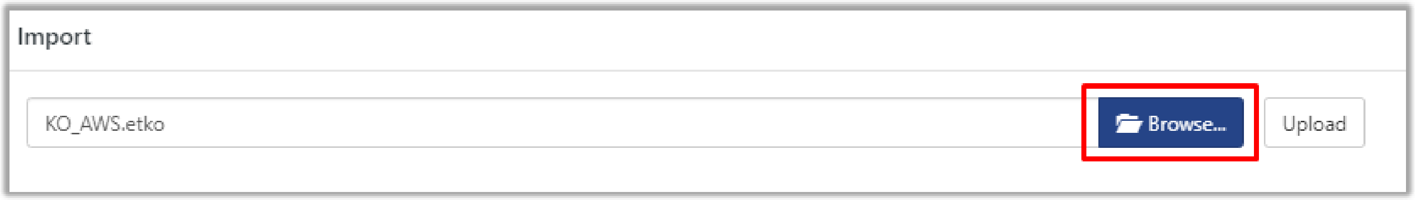
1. Click **Knowledge Objects** under the **Admin** option in the EventTracker page.



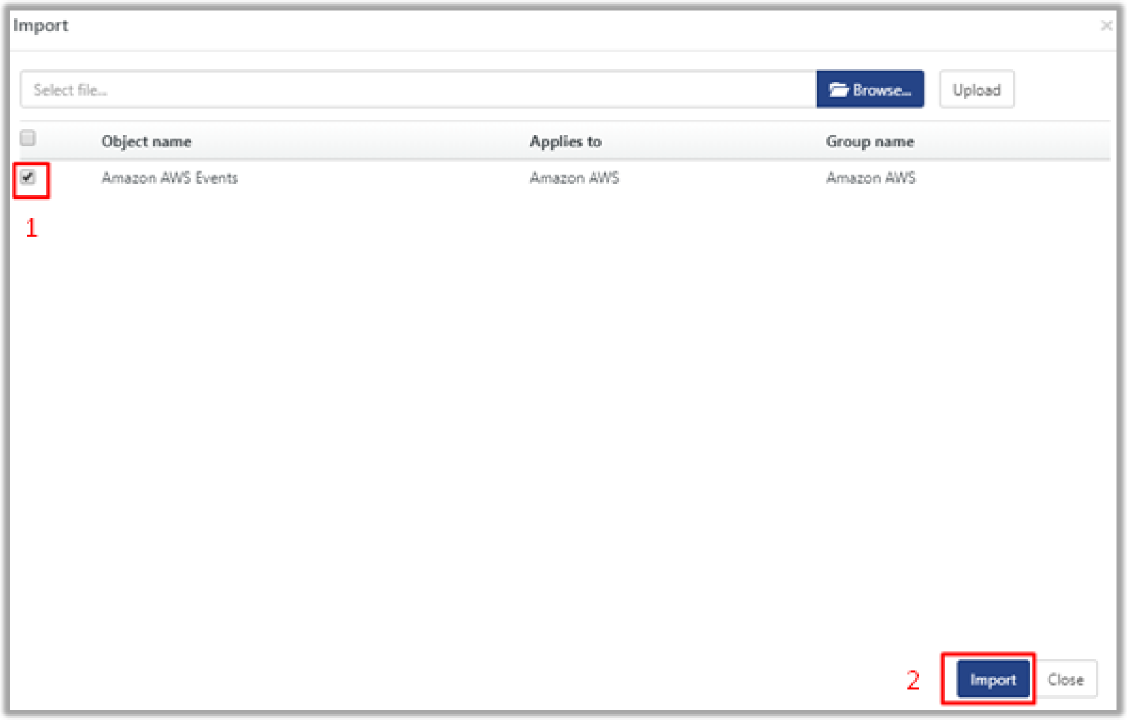
2. Click the **Import Object** icon.



3. A pop-up box will appear, click **Browse,** and navigate to the file path with the extension **".etko"** button.



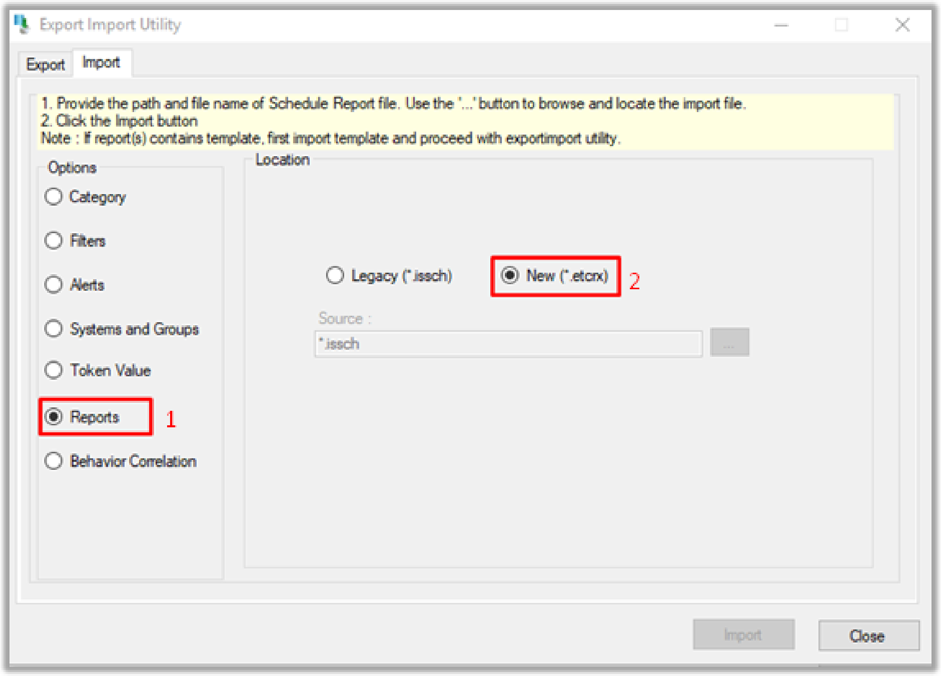
4. A list of available Knowledge Objects will appear. Select the relevant files and click **Import.**



☐	Object name	Applies to	Group name
☑	Amazon AWS Events	Amazon AWS	Amazon AWS

6.5 Flex Reports

1. In the EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Click the **Reports** option and choose "**New (*.etcrx)**".



Export Import Utility

Export | Import

1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

- ○ Category
- ○ Filters
- ○ Alerts
- ○ Systems and Groups
- ○ Token Value
- ● Reports
- ○ Behavior Correlation

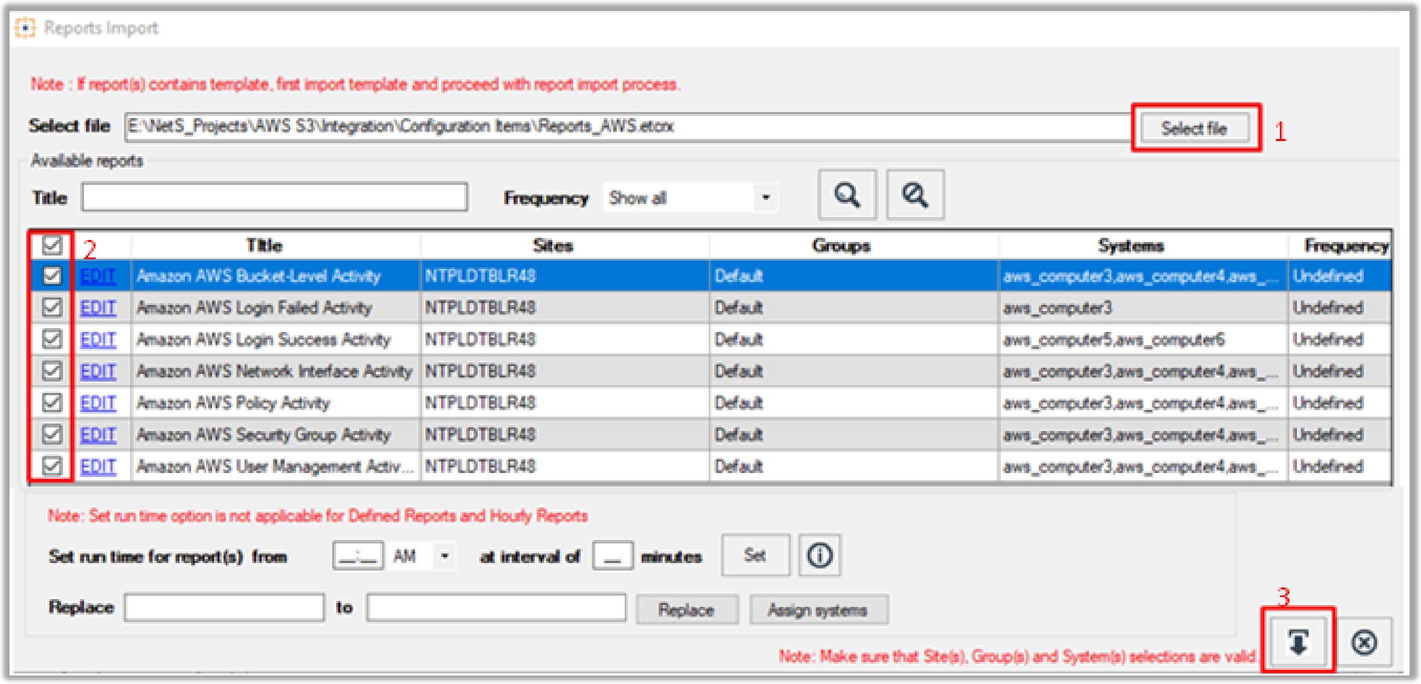
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

2. After you have selected the “**New (*.etcrx)**”, a new pop-up window will appear. Click the **Select File** button and navigate to the file path with a file having the extension **“.etcrx**”.

3. Select all the relevant files and then click the **Import** button ⤓.



Reports Import

Note : If report(s) contains template, first import template and proceed with report import process.

Select file E:\NetS_Projects\AWS S3\Integration\Configuration Items\Reports_AWS.etcrx

Available reports

Title

Frequency Show all

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	Amazon AWS Bucket-Level Activity	NTPLDTBLR48	Default	aws_computer3,aws_computer4,aws_...	Undefined
☑	EDIT	Amazon AWS Login Failed Activity	NTPLDTBLR48	Default	aws_computer3	Undefined
☑	EDIT	Amazon AWS Login Success Activity	NTPLDTBLR48	Default	aws_computer5,aws_computer6	Undefined
☑	EDIT	Amazon AWS Network Interface Activity	NTPLDTBLR48	Default	aws_computer3,aws_computer4,aws_...	Undefined
☑	EDIT	Amazon AWS Policy Activity	NTPLDTBLR48	Default	aws_computer3,aws_computer4,aws_...	Undefined
☑	EDIT	Amazon AWS Security Group Activity	NTPLDTBLR48	Default	aws_computer3,aws_computer4,aws_...	Undefined
☑	EDIT	Amazon AWS User Management Activ...	NTPLDTBLR48	Default	aws_computer3,aws_computer4,aws_...	Undefined

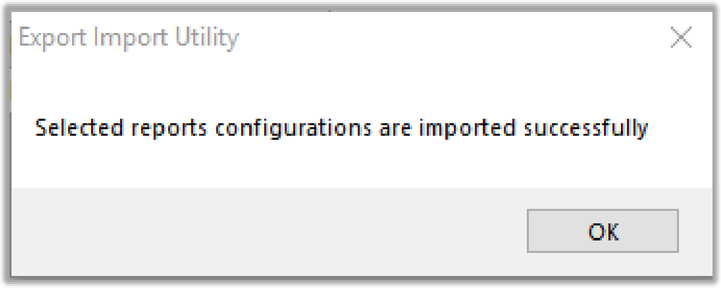
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM at interval of __ minutes

Replace to

Note: Make sure that Site(s), Group(s) and System(s) selections are valid

4. EventTracker displays a success message:

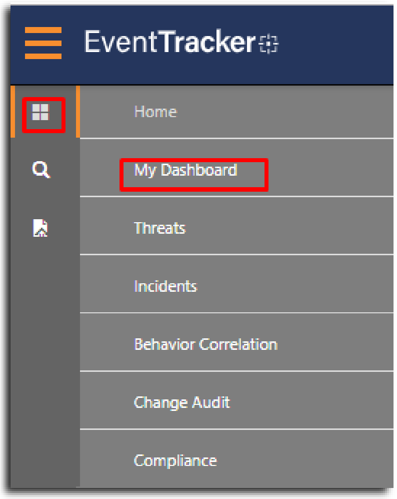


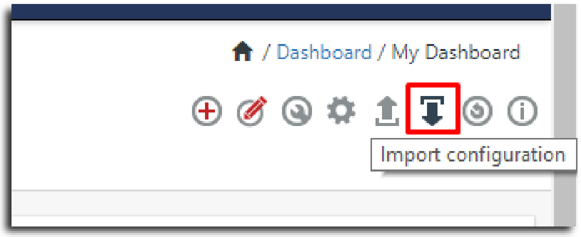
Export Import Utility

Selected reports configurations are imported successfully

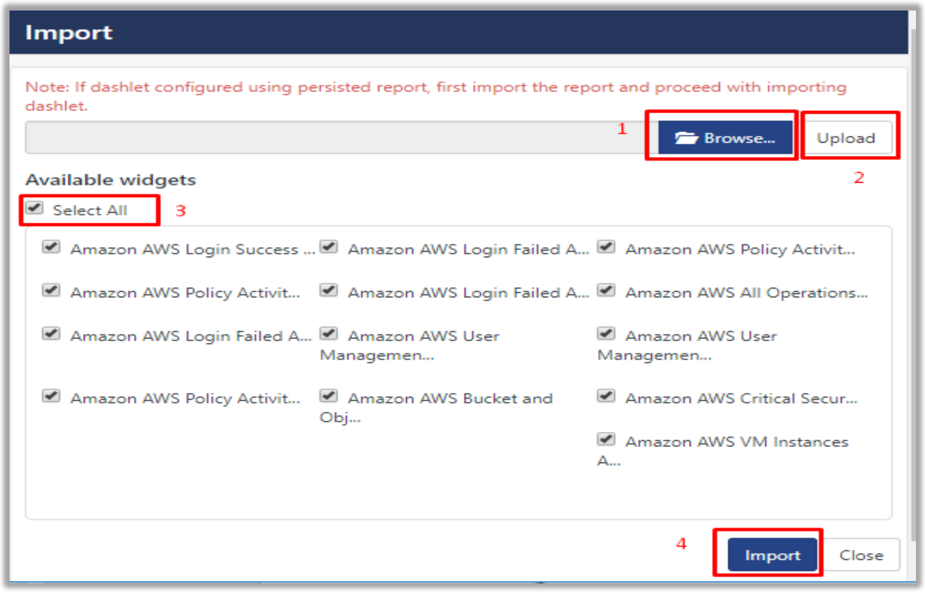
6.6 Dashboards

1. Login to **EventTracker**.
2. Navigate to **Dashboard** → **My Dashboard**.
3. In My Dashboard, click **Import Button.**





4. Select the **Browse** button and navigate to the file path where the dashboard file is saved and click the **Upload** button.
5. After completed, choose **Select All** and click **Import**.



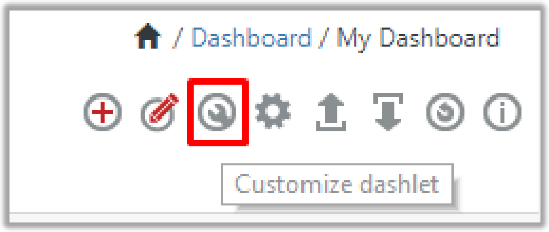
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Available widgets

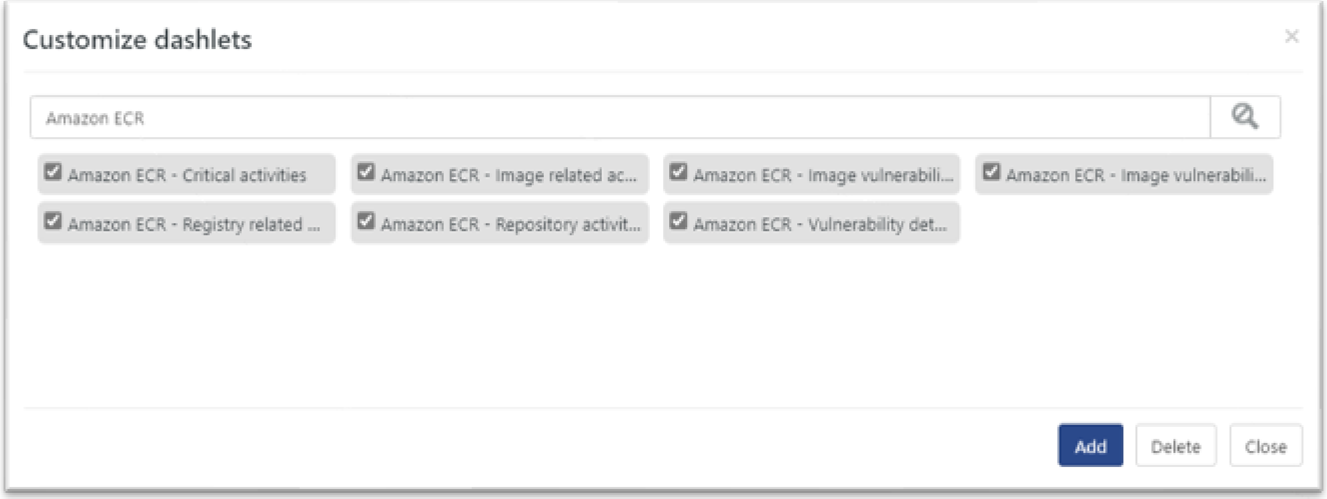
☑ Select All

☑ Amazon AWS Login Success ...
☑ Amazon AWS Login Failed A...
☑ Amazon AWS Policy Activit...
☑ Amazon AWS Policy Activit...
☑ Amazon AWS Login Failed A...
☑ Amazon AWS All Operations...
☑ Amazon AWS Login Failed A...
☑ Amazon AWS User Managemen...
☑ Amazon AWS User Managemen...
☑ Amazon AWS Policy Activit...
☑ Amazon AWS Bucket and Obj...
☑ Amazon AWS Critical Secur...
☑ Amazon AWS VM Instances A...

6. Click the **Customize dashlet** button as shown below:



7. Search for **Amazon ECR** in the Search bar and then select the Amazon ECR dashlets and then click the **Add** button.



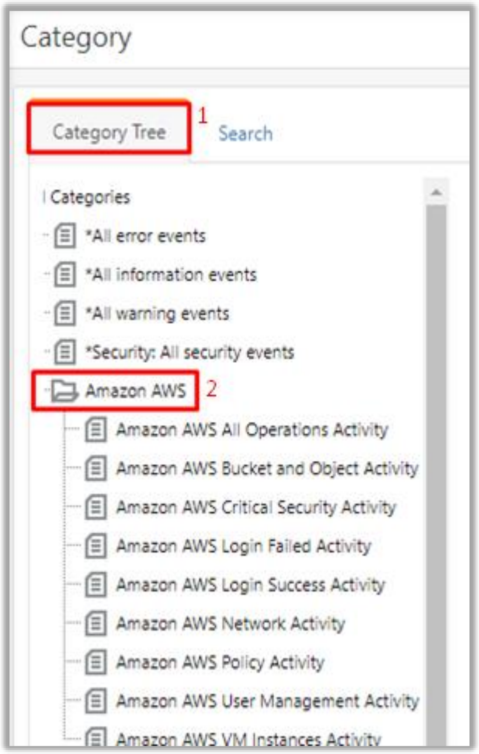
Amazon ECR

☑ Amazon ECR - Critical activities
☑ Amazon ECR - Image related ac...
☑ Amazon ECR - Image vulnerabili...
☑ Amazon ECR - Image vulnerabili...
☑ Amazon ECR - Registry related ...
☑ Amazon ECR - Repository activit...
☑ Amazon ECR - Vulnerability det...

7. Verifying Amazon ECR Knowledge Pack in EventTracker

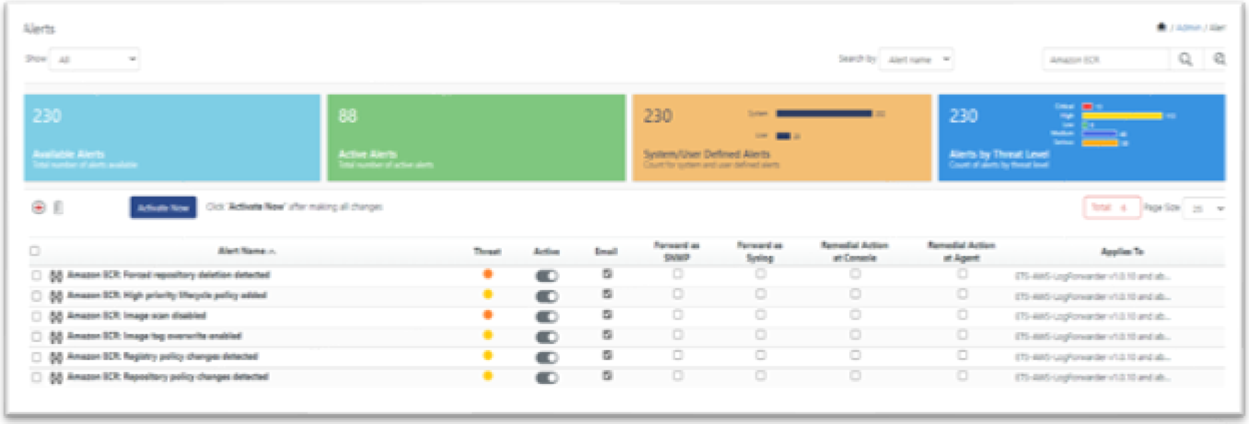
7.1 Categories

1. Login to **EventTracker**.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree** to view the imported categories, scroll down and expand the **Amazon AWS** group folder to view the imported categories:


Category
Category Tree
1
Search
Categories
*All error events
*All information events
*All warning events
*Security: All security events
Amazon AWS
2
Amazon AWS All Operations Activity
Amazon AWS Bucket and Object Activity
Amazon AWS Critical Security Activity
Amazon AWS Login Failed Activity
Amazon AWS Login Success Activity
Amazon AWS Network Activity
Amazon AWS Policy Activity
Amazon AWS User Management Activity
Amazon AWS VM Instances Activity

7.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In the search box enter **Amazon ECR** and then click the **Search** button.
3. EventTracker displays all the alerts related to **Amazon ECR.**



Alerts

Show All

Search by Alert name

Amazon ECR

230 Available Alerts Total number of alerts available

88 Active Alerts Total number of active alerts

230 System/User Defined Alerts Count for system and user defined alerts

230 Alerts by Threat Level Count of alerts by threat level

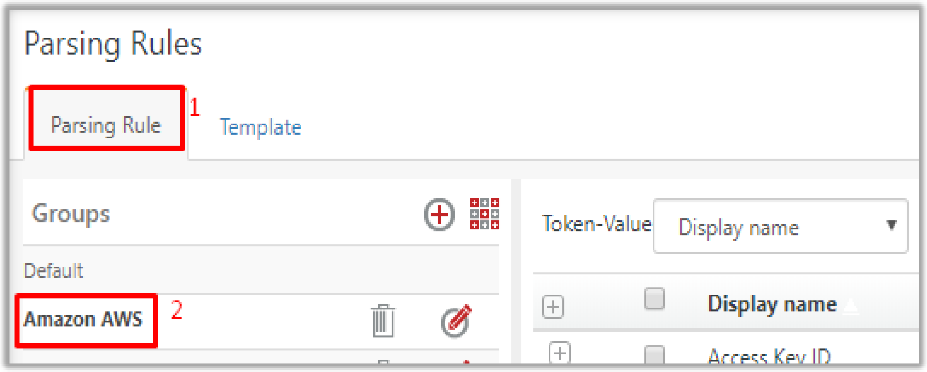
Activate Now Click 'Activate Now' after making all changes

Total 6 Page Size 25

	Alert Name	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	Amazon ECR: Forced repository deletion detected	●	●	☑	□	□	□	□	ETS-AWS-LogForwarder v1.0.10 and ab...
□	Amazon ECR: High priority lifecycle policy added	●	●	☑	□	□	□	□	ETS-AWS-LogForwarder v1.0.10 and ab...
□	Amazon ECR: Image scan disabled	●	●	☑	□	□	□	□	ETS-AWS-LogForwarder v1.0.10 and ab...
□	Amazon ECR: Image tag overwrite enabled	●	●	☑	□	□	□	□	ETS-AWS-LogForwarder v1.0.10 and ab...
□	Amazon ECR: Registry policy changes detected	●	●	☑	□	□	□	□	ETS-AWS-LogForwarder v1.0.10 and ab...
□	Amazon ECR: Repository policy changes detected	●	●	☑	□	□	□	□	ETS-AWS-LogForwarder v1.0.10 and ab...

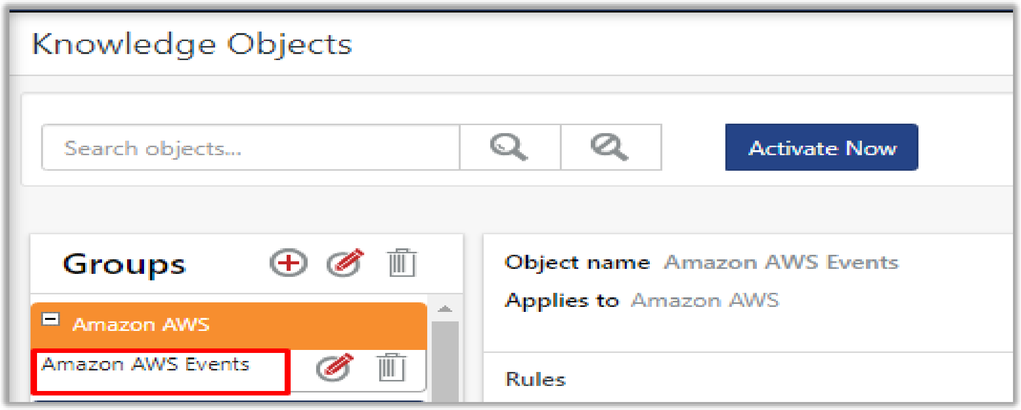
7.3 Token Values

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules.**
2. In the **Parsing Rules** tab, click the **Amazon AWS** group folder to view the imported Token Values.



7.4 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **Amazon AWS Events and Amazon ECR Scan** group folders to view the imported Knowledge Objects.

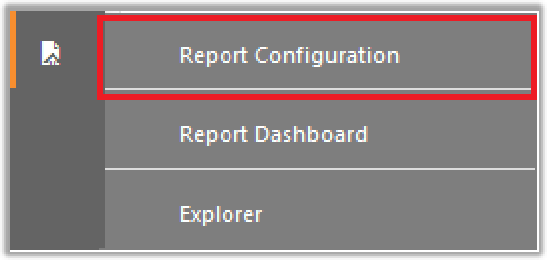


Object name Amazon AWS Events

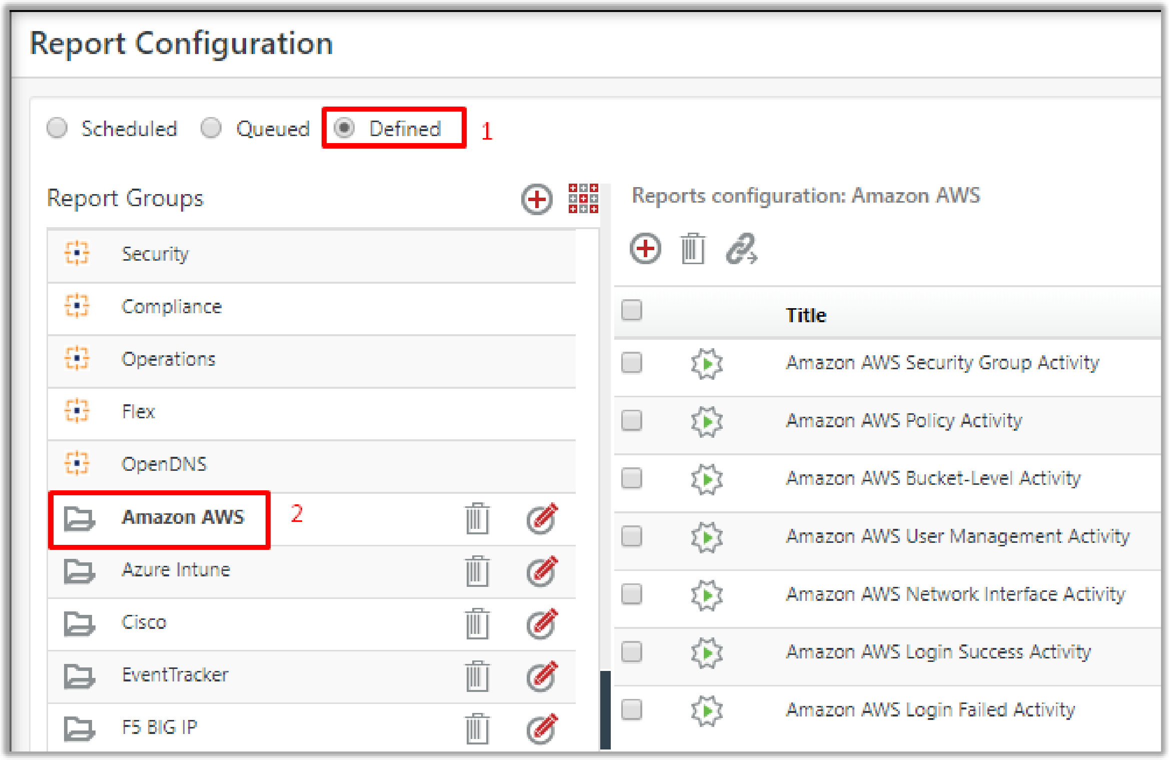
Applies to Amazon AWS

7.5 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.



2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Amazon AWS** group folder to view the imported reports.



Report Configuration

○ Scheduled ○ Queued ● Defined 1

Report Groups

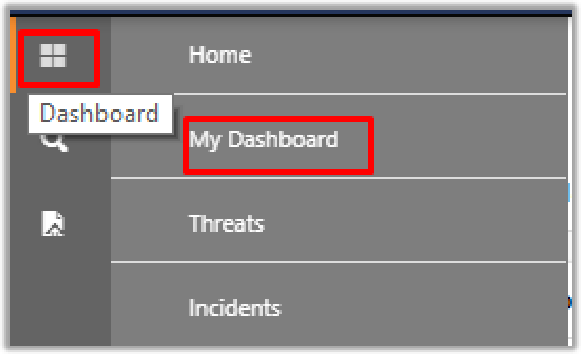
Security
Compliance
Operations
Flex
OpenDNS
Amazon AWS 2
Azure Intune
Cisco
EventTracker
F5 BIG IP

Reports configuration: Amazon AWS

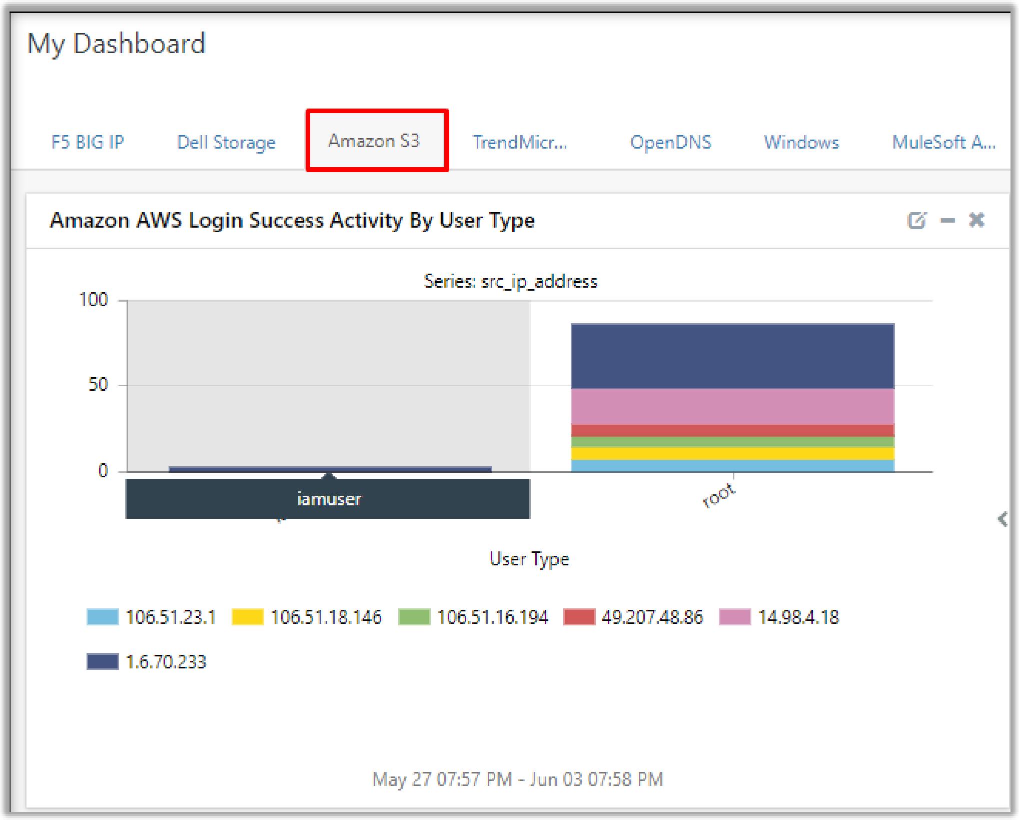
□		Title
□		Amazon AWS Security Group Activity
□		Amazon AWS Policy Activity
□		Amazon AWS Bucket-Level Activity
□		Amazon AWS User Management Activity
□		Amazon AWS Network Interface Activity
□		Amazon AWS Login Success Activity
□		Amazon AWS Login Failed Activity

7.6 Dashboards

1. In the EventTracker web interface, click the **Home** Button ⊞ and select **My Dashboard**.



2. In the **Amazon AWS** dashboard, you should now be able to view the following screen.



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 MSPs 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