Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrate AWS CloudTrail

Publication Date:

April 19, 2021

© Copyright Netsurion. All Rights Reserved.

Abstract

This guide provides instructions to configure/ retrieve Amazon Web services (AWS) events using Amazon CloudTrail**.** This will include services like Amazon Elastic Compute Cloud (EC2) and Amazon Virtual Private Cloud (VPC). Once EventTracker is configured to collect and parse these logs, dashboard, and reports can be configured to monitor Amazon CloudTrail logs.

Audience

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

© Copyright Netsurion. All Rights Reserved.

Table of Contents

Table of Contents 3

1. Overview 4

2. Prerequisites 4

3. Integrating AWS CloudTrail with EventTracker 4

   3.1 Enabling CloudTrail Logging 4

   3.2 Implementing EventTracker Lambda function 6

   3.3 Creating Subscription filters for CloudWatch 7

4. EventTracker Knowledge Pack 8

   4.1 Flex Reports 8

   4.2 Alerts 10

   4.3 Dashboards 11

5. Importing Amazon AWS Knowledge Pack into EventTracker 17

   5.1 Categories 18

   5.2 Alerts 18

   5.3 Token Value 19

   5.4 Knowledge Object 20

   5.5 Flex Reports 21

   5.6 Dashboard 23

6. Verifying Amazon AWS Knowledge Pack in EventTracker 25

   6.1 Categories 25

   6.2 Alerts 25

   6.3 Token Value 26

   6.4 Knowledge Object 26

   6.5 Flex Reports 27

   6.6 Dashboard 27

   About Netsurion 29

   Contact Us 29

© Copyright Netsurion. All Rights Reserved.

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 a history of AWS API calls for your account, including 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 API calls made on behalf of Amazon EC2 and Amazon VPC.

EventTracker collects the events delivered to CloudTrail and filters it out to get some critical event types for creating reports, dashboards, and alerts. These are considered as knowledge Packs and helps to reduce the effort to manually login to 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.

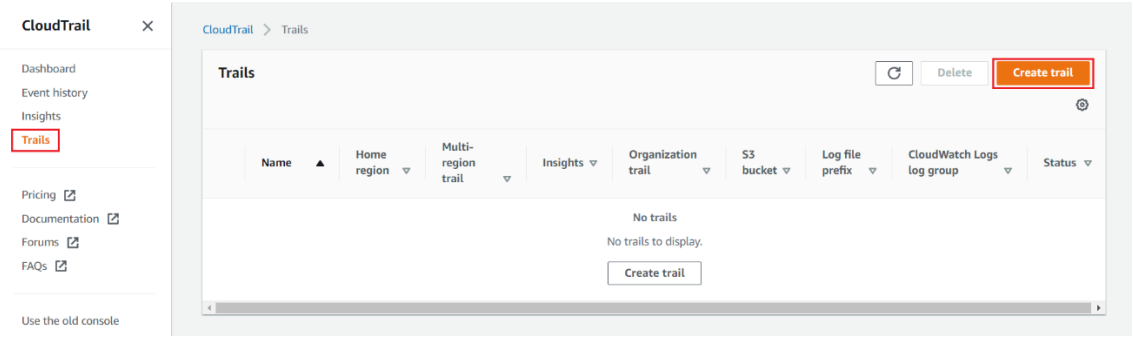
2. Prerequisites

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

3. Integrating AWS CloudTrail with EventTracker

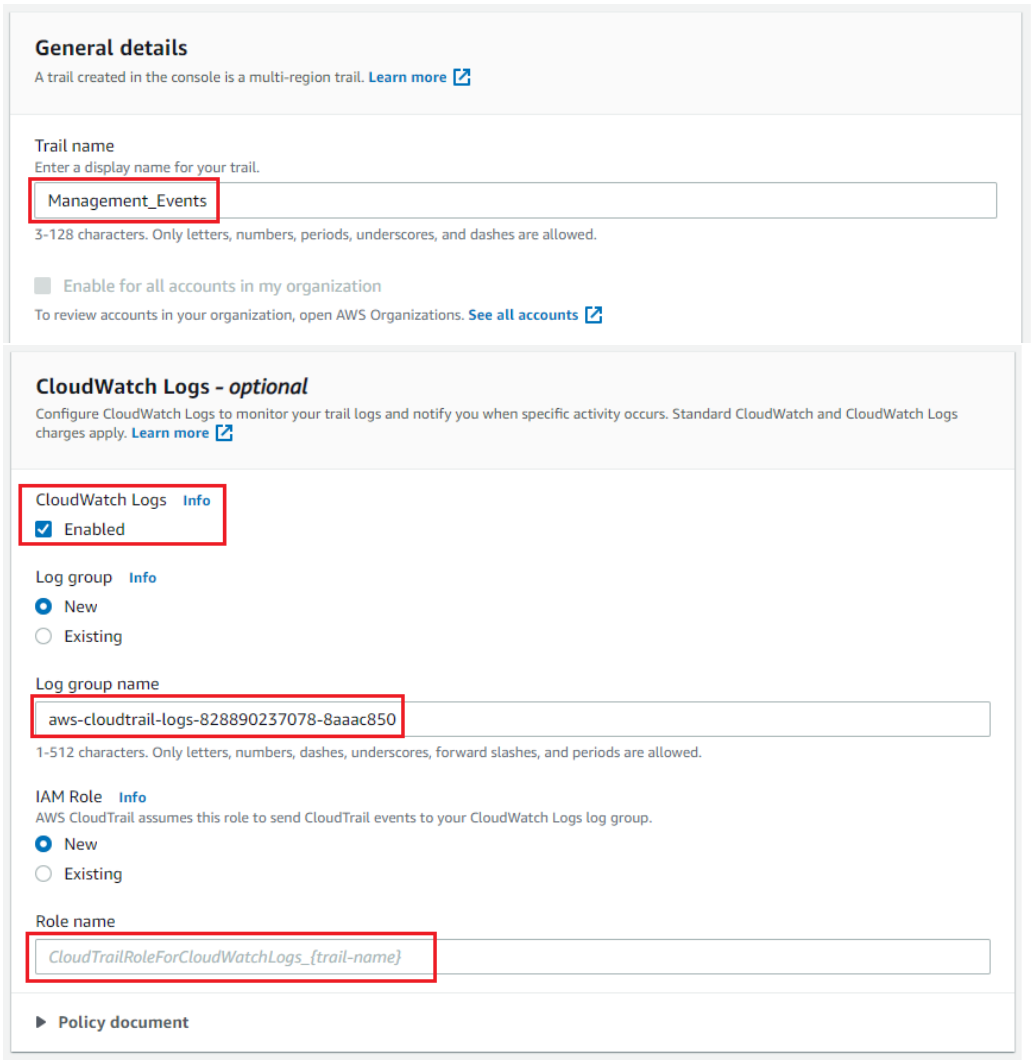
3.1 Enabling CloudTrail Logging

1. Login to AWS CloudTrail.
2. Navigate to **Trails** section and click on **create trail** button.

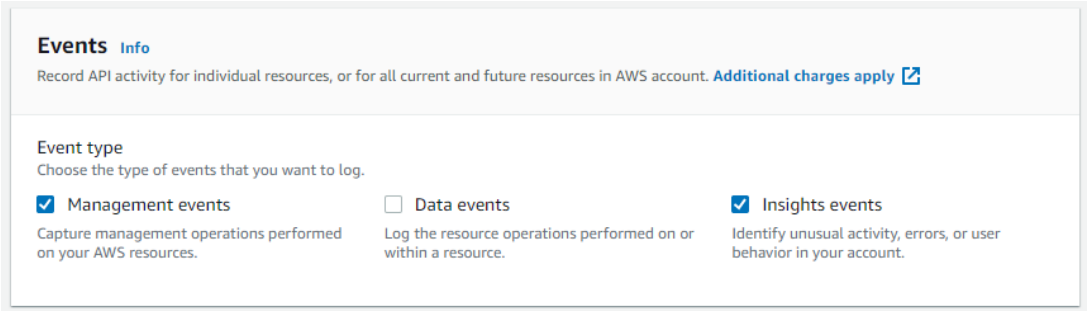


3. Provide the **Trail name** and enable **CloudWatch Logs.**

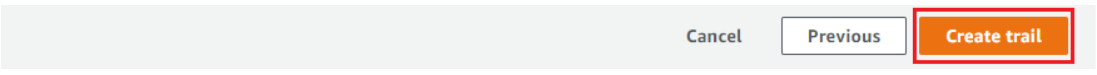
© Copyright Netsurion. All Rights Reserved.



4. After enabling CloudWatch logs, provide **Log group name** and **Role name.**
5. Click **Next** and select **Management events** and **Insights events** Event type.



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



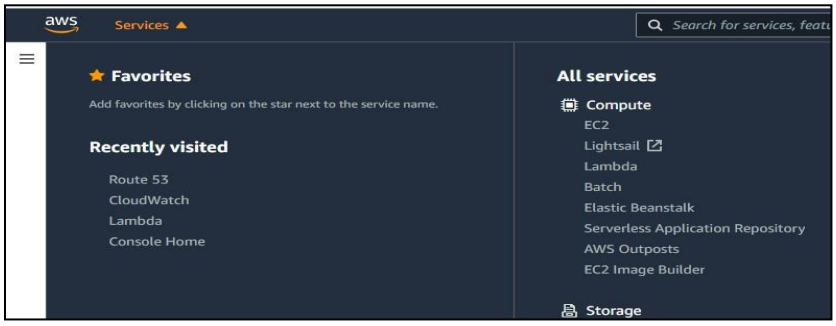
© Copyright Netsurion. All Rights Reserved.

It starts sending CloudTrail logs to CloudWatch.

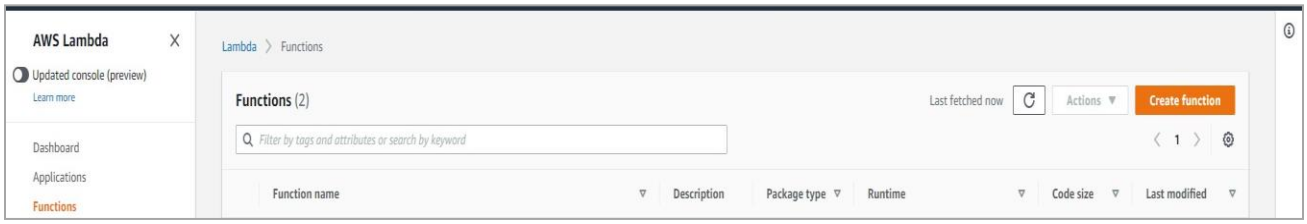
For forwarding CloudTrail logs to EventTracker. We need to create subscription filter for log group which we have created in step 4. Follow below instruction for integrating CloudWatch with EventTracker.

3.2 Implementing EventTracker Lambda function

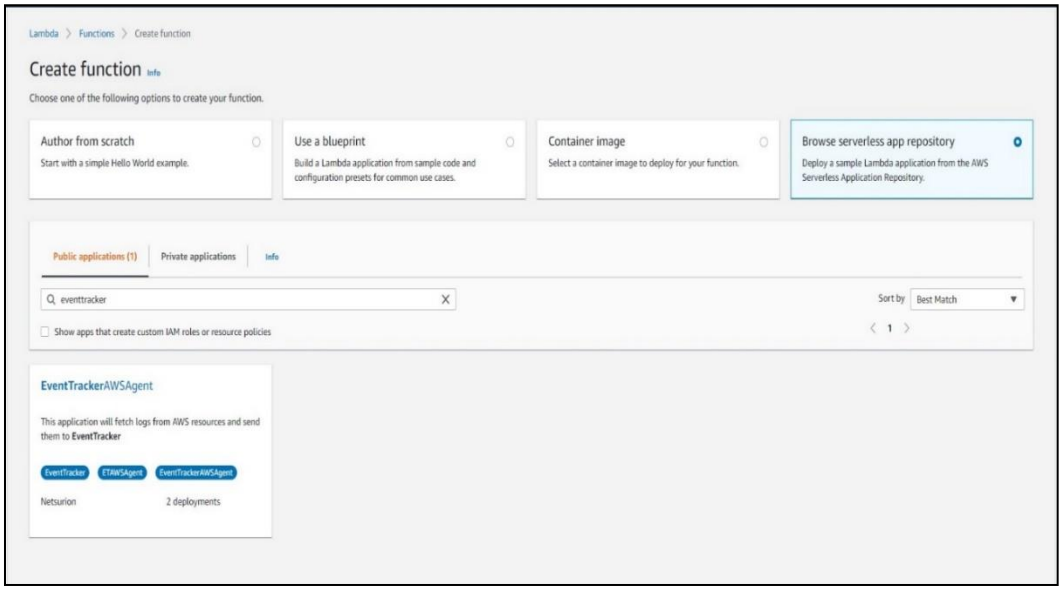
1. Click on **services** and select **lambda.**



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

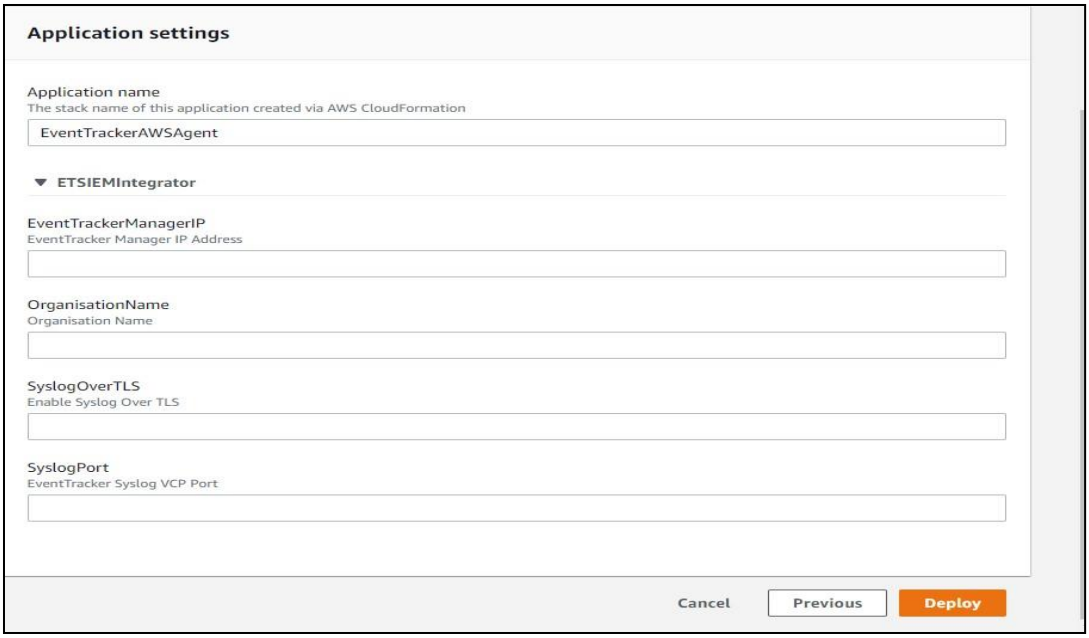


3. Select **Browse serverless app repository.**
4. Search **EventTracker** in public applications. You will get the **EventtrackerAWSAgent** in results.



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

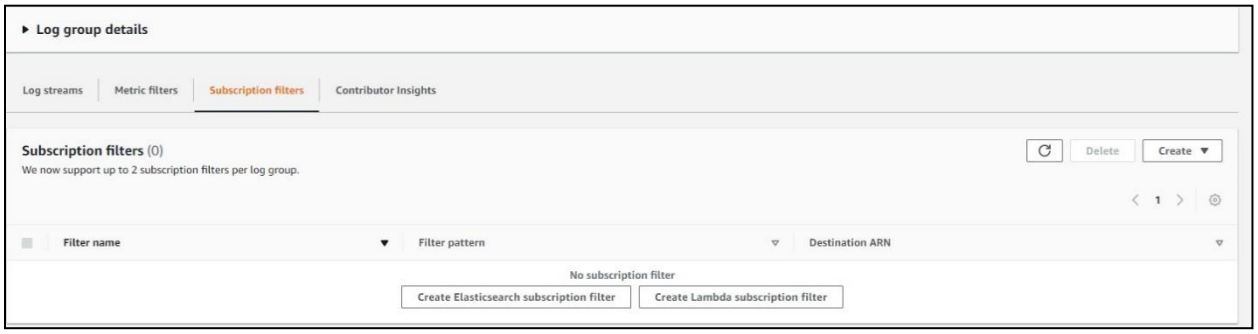
© Copyright Netsurion. All Rights Reserved.



6. Enter the EventTracker Public Manager IP.
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 on **services** and select **CloudWatch.**
2. In the navigation pane, choose **log group**.
3. Click on the **log group** provided while creating **CloudTrail**.
4. Go to **subscription filter**.



5. Click on **Create Lambda subscription filter**.
6. Under 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 on **start streaming**.

© Copyright Netsurion. All Rights Reserved.

4. EventTracker Knowledge Pack

Once logs are received by EventTracker, knowledge packs can be configured into EventTracker.

The following knowledge packs are available in EventTracker to support **Amazon CloudTrail**.

4.1 Flex Reports

- **Amazon AWS Login Failed Activity** – This report will generate a detailed view of failed or unauthorized logins to the AWS management console.

LogTime	Computer	Source IP Address	Login Status	Error Message	Login URL
05/22/2019 04:56:31 PM	AWS_COMPUTER3	17.13.182.226	Failure	Failed authentication	https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true
05/22/2019 04:56:31 PM	AWS_COMPUTER3	17.13.182.226	Failure	Failed authentication	https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true
05/22/2019 04:56:31 PM	AWS_COMPUTER3	11.19.182.226	Failure	Failed authentication	https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true
05/22/2019 04:56:31 PM	AWS_COMPUTER3	14.8.4.15	Failure	Failed authentication	https://console.aws.amazon.com/support/home?state=hashArgs%23%2Fcase%2Fcreate%3FissueType%3Dtechnical&isauthcode=true
05/22/2019 04:56:32 PM	AWS_COMPUTER3	14.8.4.15	Failure	Failed authentication	https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true

- **Amazon AWS Login Success Activity** – This report will generate a detailed view of the successful user login or authentication to the AWS management console.

LogTime	Computer	User Name	Source IP Address	Login Status	Region	Login URL
05/27/2019 07:18:13 PM	AWS_COMPUTER5	Karen	12.6.70.233	Success	us-east-1	https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true
05/28/2019 11:32:30 AM	AWS_COMPUTER5	Jacob	12.6.70.112	Success	us-east-1	https://s3.console.aws.amazon.com/s3/buckets/awslogs1192/?region=us-east-1&state=hashArgs%23&tab=overview&isauthcode=true
05/28/2019 11:32:31 AM	AWS_COMPUTER5	Mary	12.6.70.33	Success	us-east-1	https://console.aws.amazon.com/console/home?nc2=h_ct&src=header-signin&state=hashArgs%23&isauthcode=true
05/28/2019 11:32:31 AM	AWS_COMPUTER5	Brenden	12.6.70.34	Success	us-east-1	https://console.aws.amazon.com/console/home?nc2=h_ct&src=header-signin&state=hashArgs%23&isauthcode=true

- **Amazon AWS Network Interface Activity** – This report will generate a detailed view of the activity related to Network Interface create, delete, reset, modify, detach, attach, etc.

© Copyright Netsurion. All Rights Reserved.

LogTime	Computer	User Type	Requested Action	Source IP Address	Interface Description	Subnet ID	Network Interface ID
05/28/2019 11:33:02 AM	AWS_COMPUTER5	Root	CreateNetworkInterface	12.6.70.33	testinterface	subnet-1186b679	
05/28/2019 11:33:05 AM	AWS_COMPUTER5	Root	DeleteNetworkInterface	12.6.70.33			eni-063cc300302e1bef3
05/29/2019 12:03:22 PM	AWS_COMPUTER5	Root	DeleteNetworkInterface	12.6.70.33			eni-063cc300302e1bef3
05/29/2019 12:06:10 PM	AWS_COMPUTER5	Root	DeleteNetworkInterface	12.6.70.33			eni-063cc300302e1bef3
05/29/2019 12:06:10 PM	AWS_COMPUTER5	Root	CreateNetworkInterface	12.6.70.33	testinterface	subnet-1186b679	eni-063cc300302e1bef3
05/29/2019 12:08:32 PM	AWS_COMPUTER5	Root	DeleteNetworkInterface	12.6.70.33			eni-063cc300302e1bef3
05/29/2019 12:08:32 PM	AWS_COMPUTER5	Root	CreateNetworkInterface	12.6.70.33	testinterface	subnet-1186b679	eni-063cc300302e1bef3
05/31/2019 02:02:16 PM	AWS_COMPUTER5	Root	CreateNetworkInterface	AWS Internal	Route 53 Resolver: rslvr-out-630e81a12d844356b:rni-a15abdee88fc4ad0a	subnet-1186b679	eni-0c4b759618a5cd247

- **Amazon AWS User Management Activity** – This report will generate a detailed view of the activities related to user or group create, delete, add, remove, etc.

LogTime	Computer	User Type	Account ID	Region	Source IP Address	Requested Action	User Name	Group Name	User ARN
05/27/2019 05:39:07 PM	AWS_COMPUTER5	Root	247856xxxxxx	us-east-1	12.6.70.233	RemoveUserFromGroup	Karen	mygg	
05/27/2019 05:39:07 PM	AWS_COMPUTER5	Root	247856xxxxxx	us-east-1	12.6.70.233	AddUserToGroup	Karen	mygg	
05/28/2019 11:32:35 AM	AWS_COMPUTER5	Root	247856xxxxxx	us-east-1	12.6.70.234	AddUserToGroup	John	CloudWatch	
05/28/2019 11:32:35 AM	AWS_COMPUTER5	Root	247856xxxxxx	us-east-1	12.6.70.235	AddUserToGroup	Mike	Read_only	
05/28/2019 11:32:35 AM	AWS_COMPUTER5	Root	247856xxxxxx	us-east-1	12.6.70.236	DeleteUser	Mike		
05/28/2019 11:32:35 AM	AWS_COMPUTER5	Root	247856xxxxxx	us-east-1	12.6.70.237	CreateUser	Mike		arn:aws:iam::200836103659:user/Mike
05/28/2019 11:32:36 AM	AWS_COMPUTER5	Root	247856xxxxxx	us-east-1	12.6.70.238	CreateUser	John		arn:aws:iam::200836103659:user/John

- **Amazon AWS Bucket-Level Activity** – This report will generate a detailed view of the activities related to the Amazon S3 bucket. This includes CreateBucket, PutBucketPolicy, ListBuckets, etc.

LogTime	Computer	User Type	Account ID	Source IP Address	Region	Requested Action	Bucket Name	Error Code	Bucket Policy
05/27/2019 05:27:02 PM	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.233	us-east-2	GetBucketEncryption	awslogs1192	ServerSideEncryptionConfigurationNotFoundError	
05/27/2019 05:27:02 PM	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.234	us-east-2	GetBucketPublicAccessBlock	awslogs1192	NoSuchPublicAccessBlockConfiguration	
05/27/2019 05:27:03 PM	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.235	us-east-2	GetBucketEncryption	logs1990	ServerSideEncryptionConfigurationNotFoundError	
05/29/2019 12:03:12 PM	AWS_COMPUTER5	Root	2008361xxxxx	172.18.144.11	us-east-2	CreateBucket	awslogs1192		
05/28/2019 11:32:27 AM	AWS_COMPUTER5	IAMUser	2008361xxxxx	14.98.42.12	us-west-2	GetBucketLocation	nse-sec-cloudtrail-central	AccessDenied	
05/28/2019 02:30:54 PM	AWS_COMPUTER5	Root	2008361xxxxx	172.18.144.11	us-east-2	PutBucketPolicy	awslogs1192		Sid = AWSCloud

- **Amazon AWS Policy Activity** – This report will generate a detailed view of the activities related to policy, i.e. AttachUserPolicy, GetPolicy, DetachRolePolicy, CreatePolicy, etc.

© Copyright Netsurion. All Rights Reserved.

Event DateTime	Computer	User Type	Account ID	Source IP Address	Service Name	Region	Requested Action	PolicyARN	User Name
2019-05-27T08:31:08Z	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.233	iam.amazonaws.com	us-east-1	AttachUserPolicy	arn:aws:iam::200836103659:policy/testpolicy	John
2019-05-27T08:31:40Z	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.234	iam.amazonaws.com	us-east-1	AttachUserPolicy	arn:aws:iam::200836103659:policy/testpolicy	Karen
2019-05-27T08:27:37Z	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.235	iam.amazonaws.com	us-east-1	DetachUserPolicy	arn:aws:iam::aws:policy/IAMUserChangePassword	Mike

- **Amazon AWS Security Group Activity** – This report will generate a detailed view of the activities related to the security groups, i.e. CreateSecurityGroup, AuthorizeSecurityGroupIngress, DeleteSecurityGroup, etc.

Event DateTime	Computer	User Type	Account ID	Source IP Address	Region	Requested Action	Group Name	Group ID	IP Permissions
2019-05-27T08:38:59Z	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.233	us-east-2	CreateSecurityGroup	testsecuritygroup	sg-0de88643e4f2d752a	
2019-05-27T08:39:11Z	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.234	us-east-2	DeleteSecurityGroup		sg-0de88643e4f2d752a	
2019-05-27T08:37:25Z	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.235	us-east-2	AuthorizeSecurityGroupIngress		sg-1ee4b571	items =
2019-05-27T08:38:11Z	AWS_COMPUTER5	Root	2008361xxxxx	12.6.70.236	us-east-2	RevokeSecurityGroupIngress		sg-1ee4b571	items =

4.2 Alerts

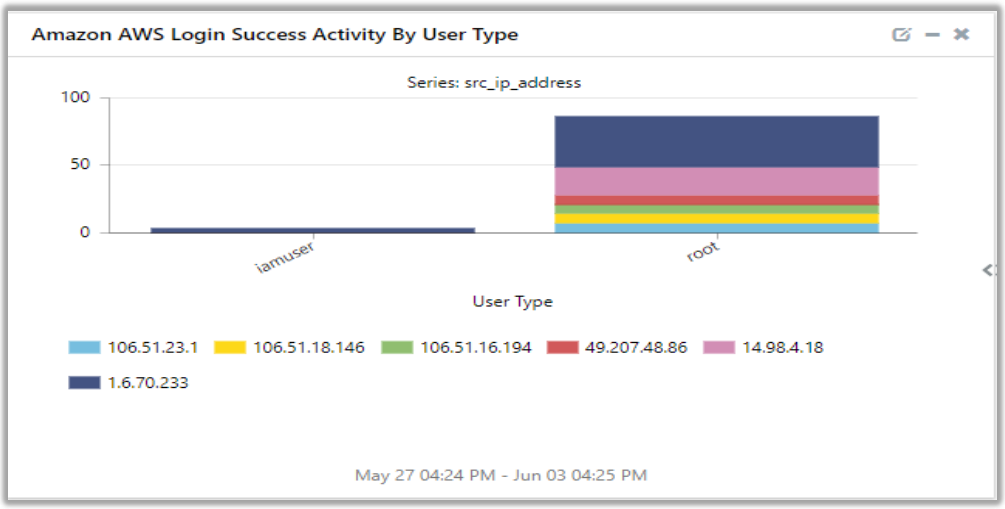
- **Amazon AWS Network Interface Deleted** – This alert will be triggered if there is any activity related to VPC network interface deletion.
- **Amazon S3 User Deleted** – This alert will be triggered if a user gets deleted.
- **AWS CIS Control AWS Config configuration changed** - This alert will be triggered when the configuration is changed in the AWS Config. It will help ensure sustained visibility of configuration items within the AWS account.
- **AWS CIS Control AWS Management Console authentication failures** - This alert will be triggered in the event of any failed or unauthorized login attempt to the AWS management console.
- **AWS CIS Control changes to Network Access Control Lists (NACL) detected** - This alert will be triggered in the event of any changes to Network Access Control Lists is detected. Monitoring changes to NACLs will help ensure that the AWS resources and services are not unintentionally exposed.
- **AWS CIS Control Changes to network gateways detected** - This alert will be triggered in the event of any changes to the network gateway is detected. Monitoring changes to network gateways will help ensure that all ingress/egress traffic traverses the VPC border via a controlled path.
- **AWS CIS Control CloudTrail configuration changed** - This alert will be triggered in the event of any CloudTrail configuration is changed. Monitoring changes to CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account.
- **AWS CIS Control Disabling or scheduled deletion of customer created CMKs** - This alert will be triggered in the event of any disabling or scheduled deletion of customer created CMKs. Monitoring changes to CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account.

© Copyright Netsurion. All Rights Reserved.

- **AWS CIS Control IAM policy changed** - This alert will be triggered in the event of any IAM policy changed. Monitoring changes to IAM policies will help ensure authentication and authorization controls remain intact.
- **AWS CIS Control Management Console signed-in without MFA** - This alert will be triggered in the event of any user signed-in without MFA. Monitoring for single-factor console logins will increase visibility into accounts that are not protected by MFA.
- **AWS CIS Control Route table changed** - This alert will be triggered in the event of any Route table changed. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path.
- **AWS CIS Control S3 bucket policy changed** - This alert will be triggered in the event of the s3 bucket policy changed. Monitoring changes to the S3 bucket policies may reduce the time to detect and correct permissive policies on sensitive S3 buckets.
- **AWS CIS Control Security group changed** - This alert will be triggered in the event of the s3 bucket policy changed. Monitoring changes to the security group will help ensure that resources and services are not unintentionally exposed.
- **AWS CIS Control Unauthorized API calls** - This alert is triggered in the event of unauthorized API calls detected. Monitoring unauthorized API calls will help reveal application errors and may reduce the time to detect malicious activity.
- **AWS CIS Control Usage of root account detected** - This alert will be triggered in the event of root account usage detected. Monitoring for root account logins will provide visibility into the use of a fully privileged account and an opportunity to reduce the use of it.
- **AWS CIS Control VPC configuration changed** - This alert will be triggered in the event of VPC changed. Monitoring changes to IAM policies will help ensure authentication and authorization controls remain intact.

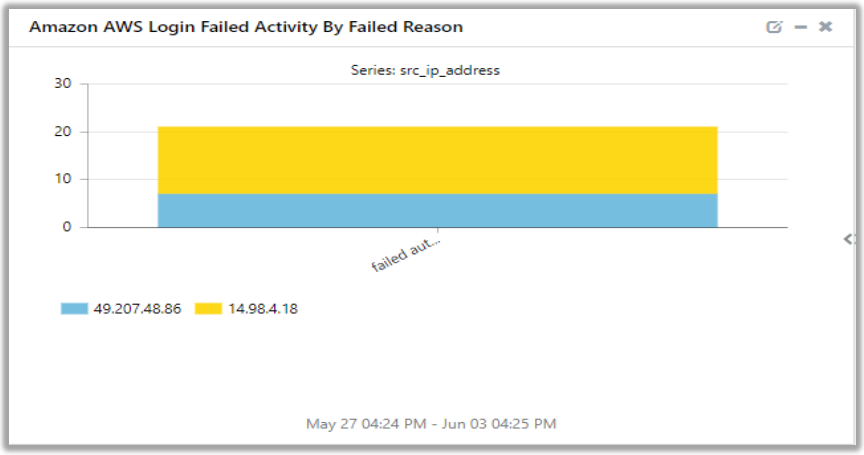
4.3 Dashboards

- **Amazon AWS Login Success Activity By User Type.**

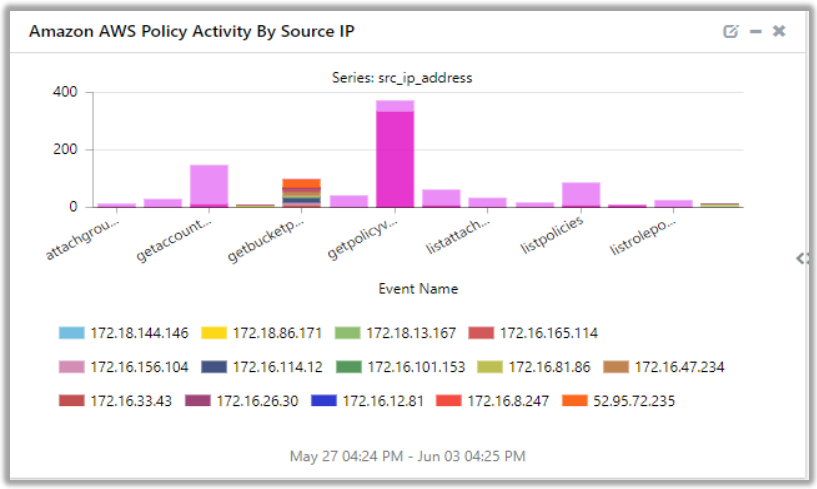


© Copyright Netsurion. All Rights Reserved.

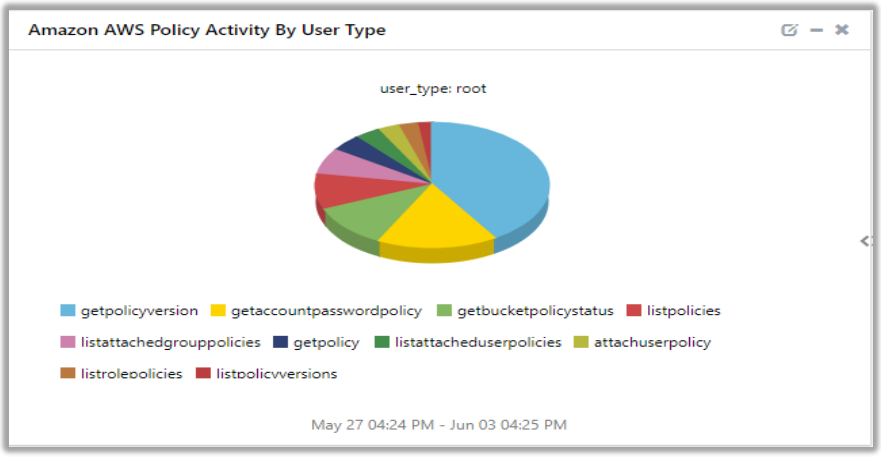
- **Amazon AWS Login Failed Activity By Failed Reason**.



- **Amazon AWS Policy Activity By Source IP**.

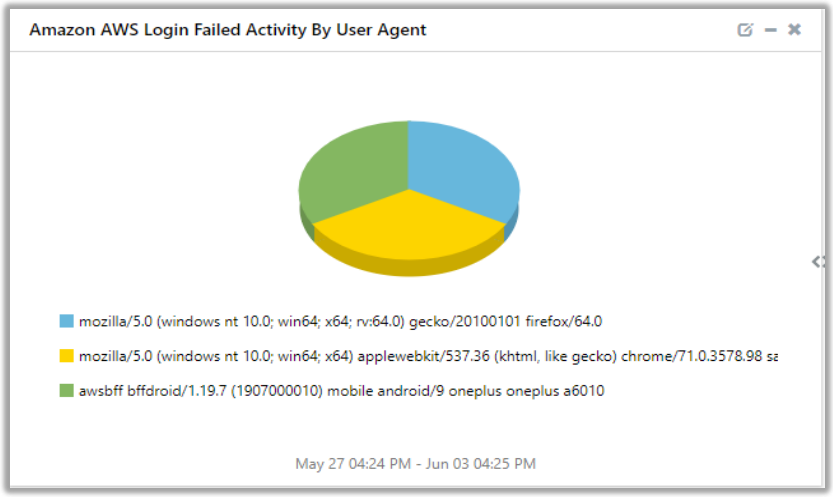


- **Amazon AWS Policy Activity By User Type**.

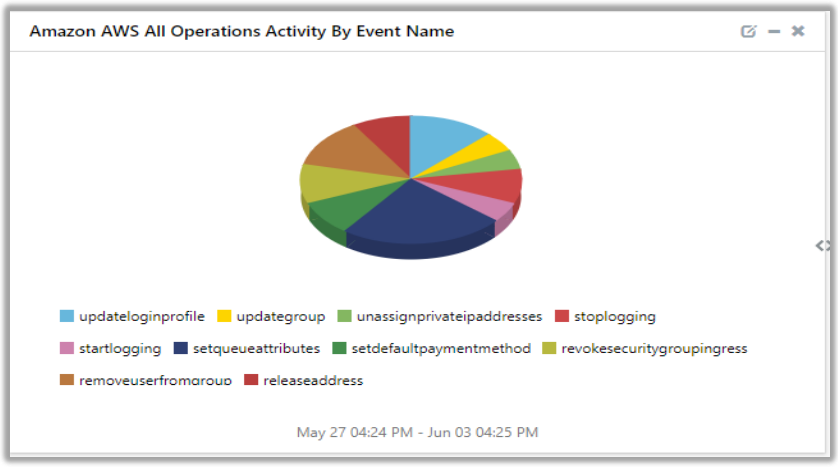


© Copyright Netsurion. All Rights Reserved.

- **Amazon AWS Login Failed Activity By User Agent**.



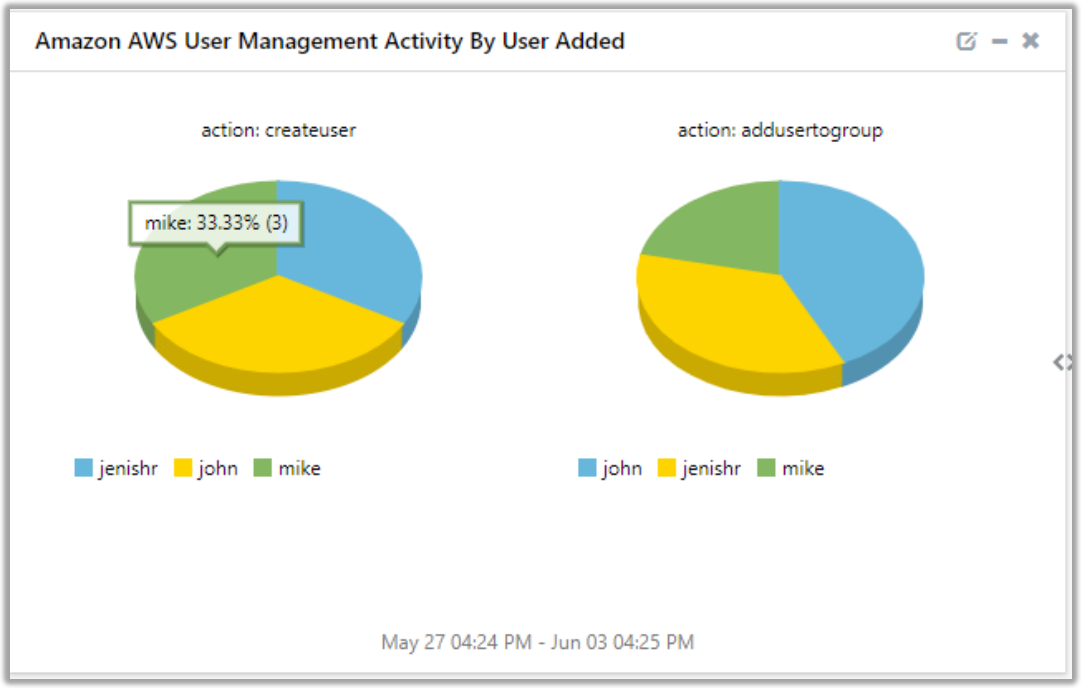
- **Amazon AWS All Operations Activity By Event Name**.



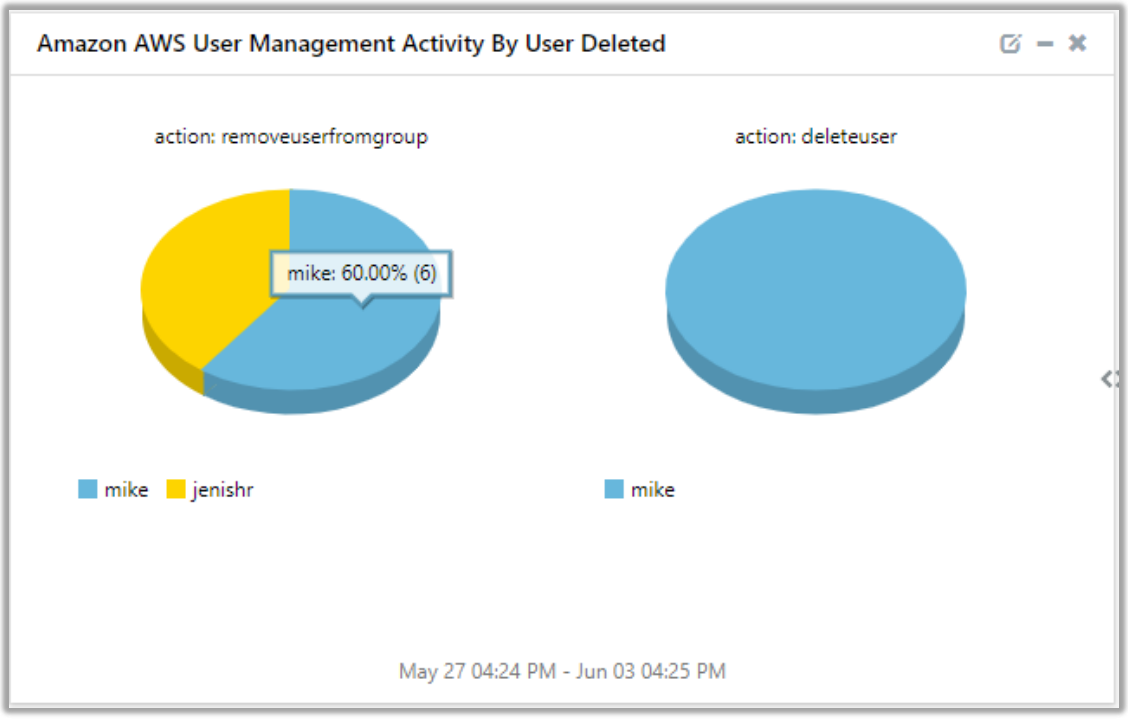
- **Amazon AWS Login Failed Activity By City**.

© Copyright Netsurion. All Rights Reserved.

- **Amazon AWS User Management Activity By User Added**.

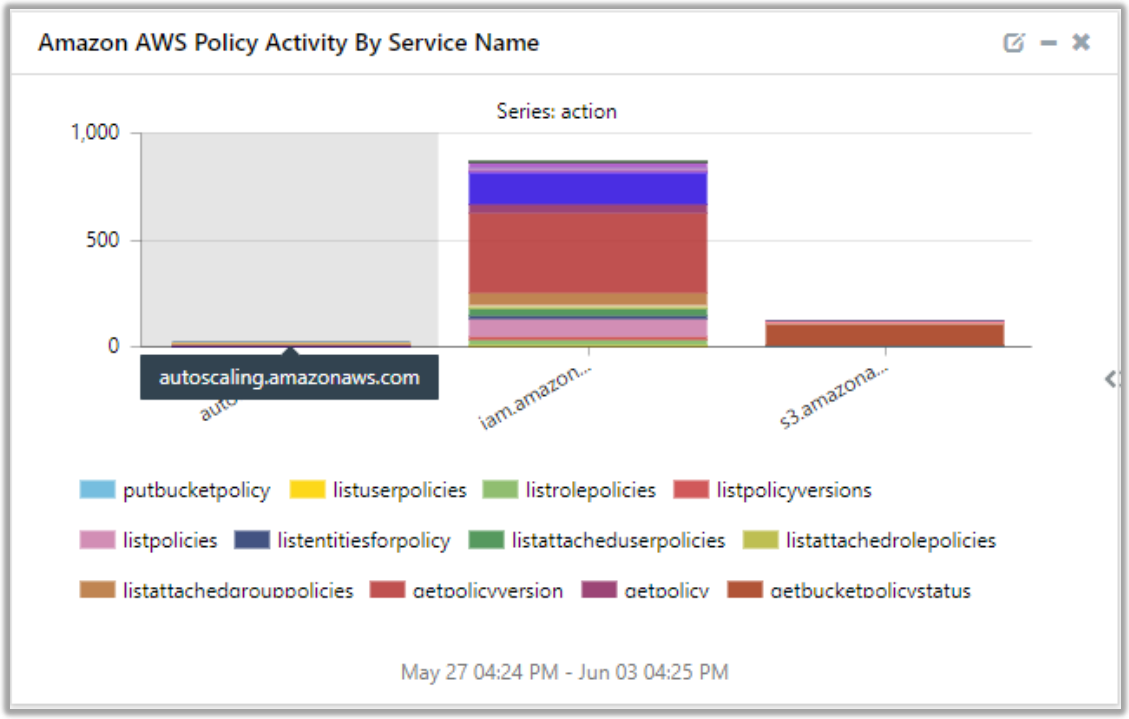


- **Amazon AWS User Management Activity By User Deleted**.

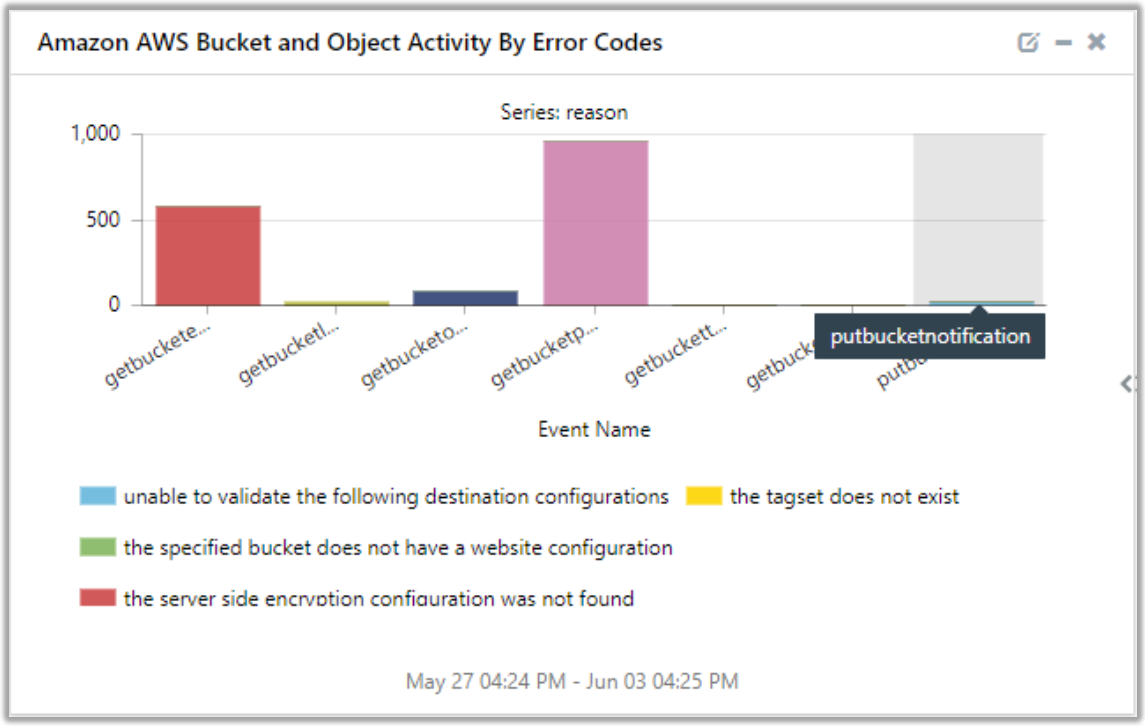


© Copyright Netsurion. All Rights Reserved.

- **Amazon AWS Policy Activity By Service Name**.

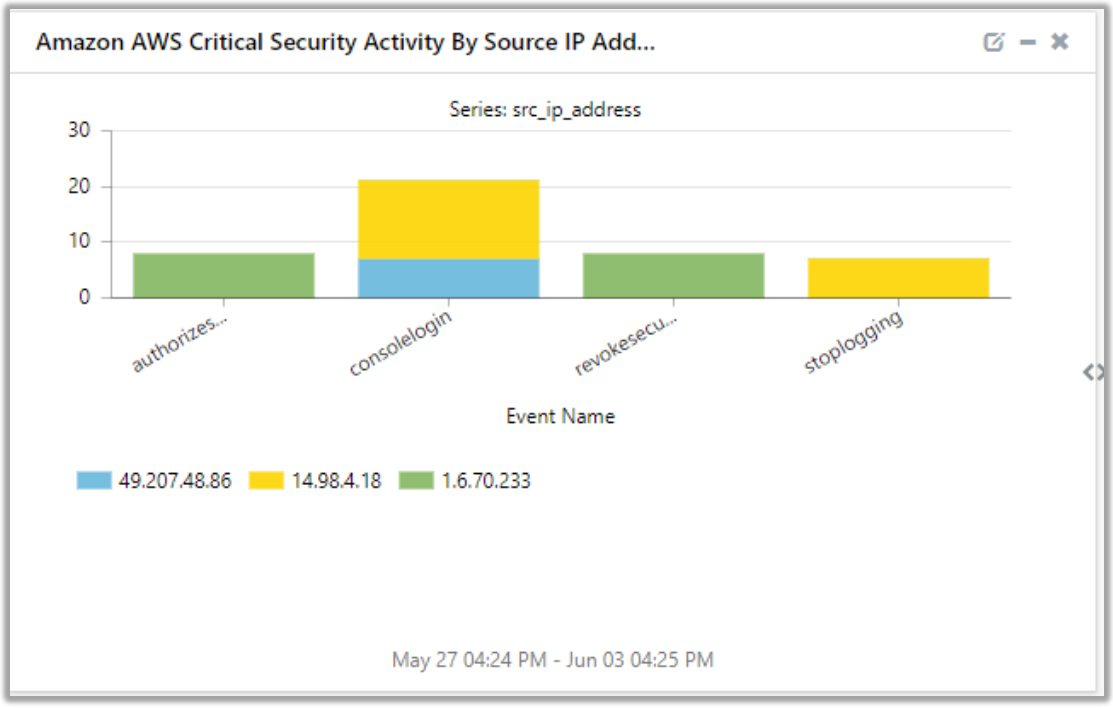


- **Amazon AWS Bucket and Object Activity By Error Codes**.

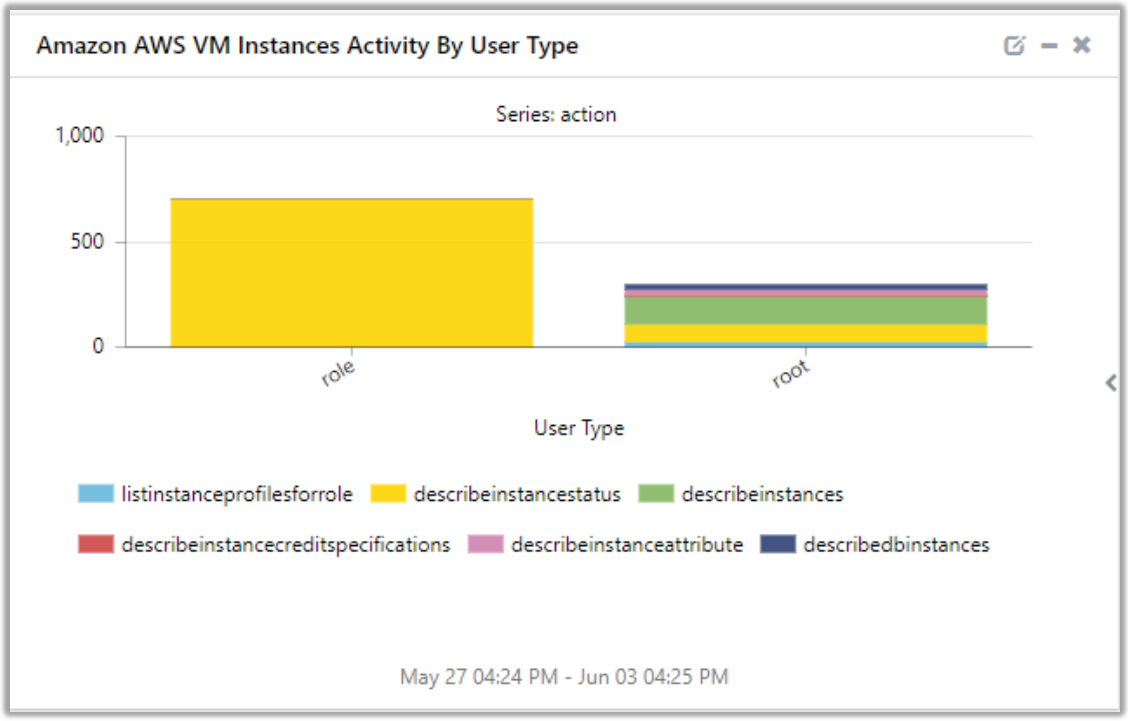


© Copyright Netsurion. All Rights Reserved.

- **Amazon AWS Critical Security Activity By Source IP Address**.



- **Amazon AWS VM Instances Activity By User Type**.



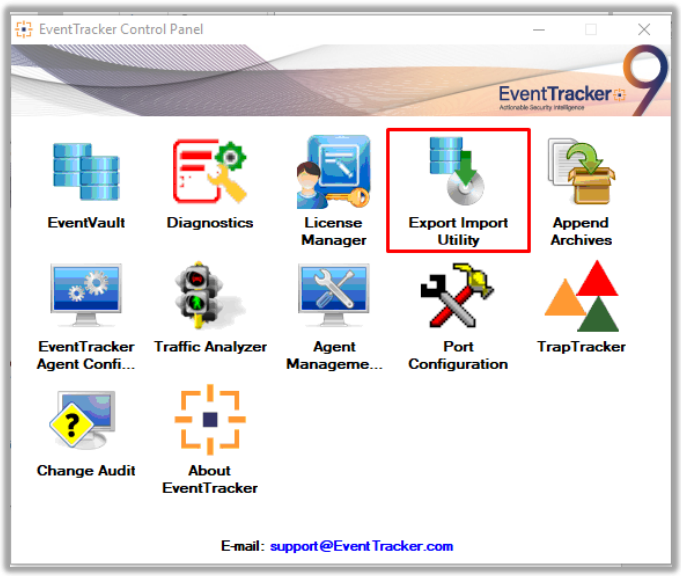
© Copyright Netsurion. All Rights Reserved.

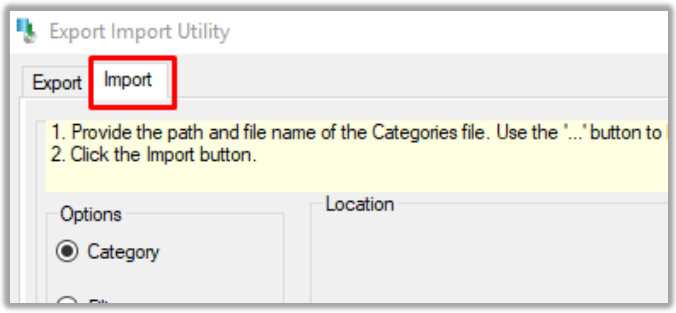
5. Importing Amazon AWS Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Value
- Knowledge Objects
- Flex Reports
- Dashboard

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



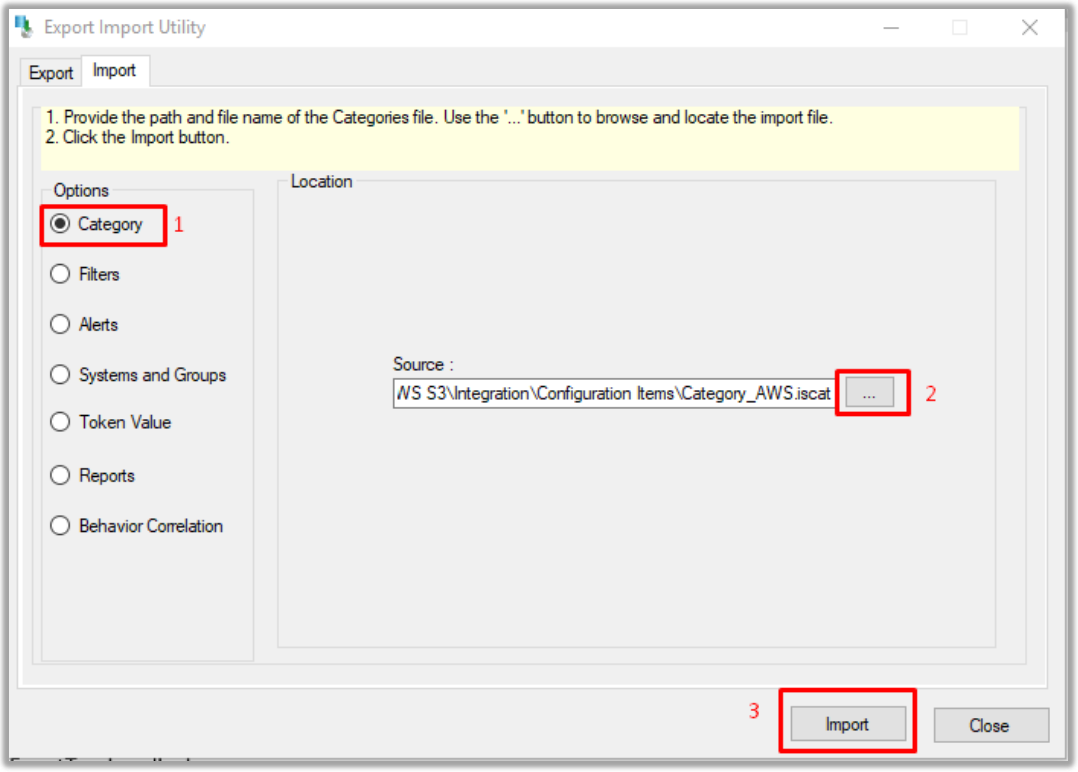


3. Click the **Import** tab.

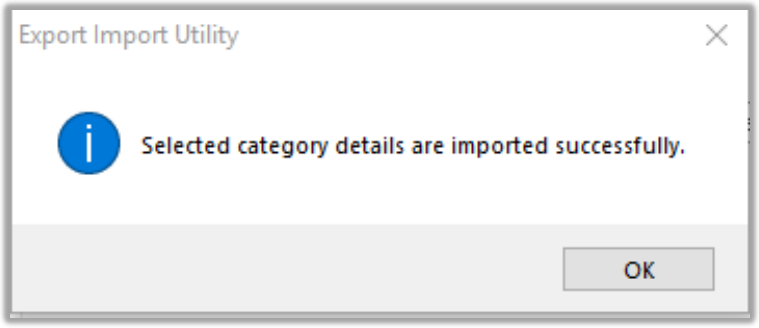
© Copyright Netsurion. All Rights Reserved.

5.1 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.**



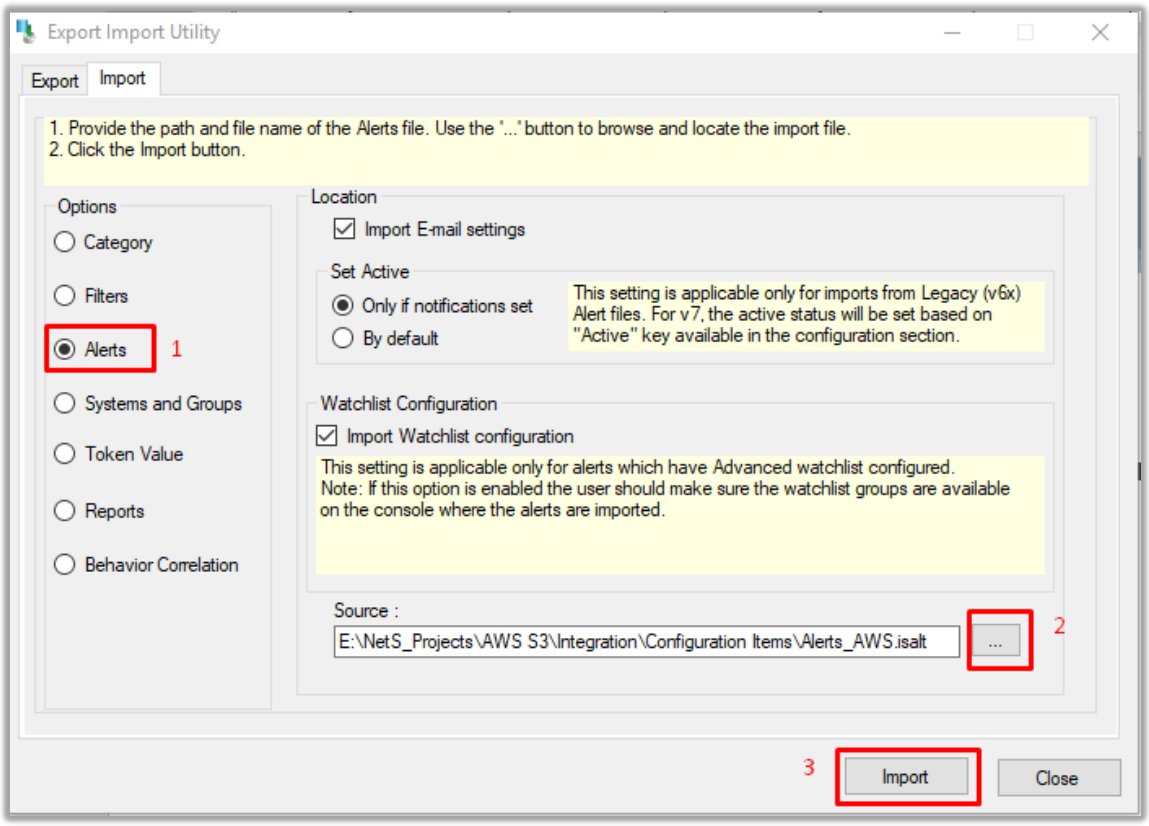
3. EventTracker displays a success message:



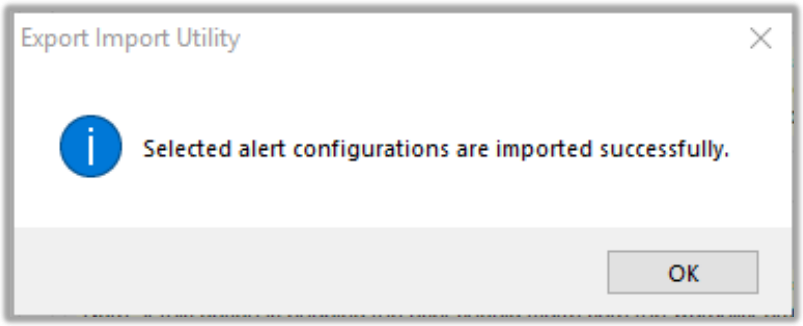
5.2 Alerts

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

© Copyright Netsurion. All Rights Reserved.



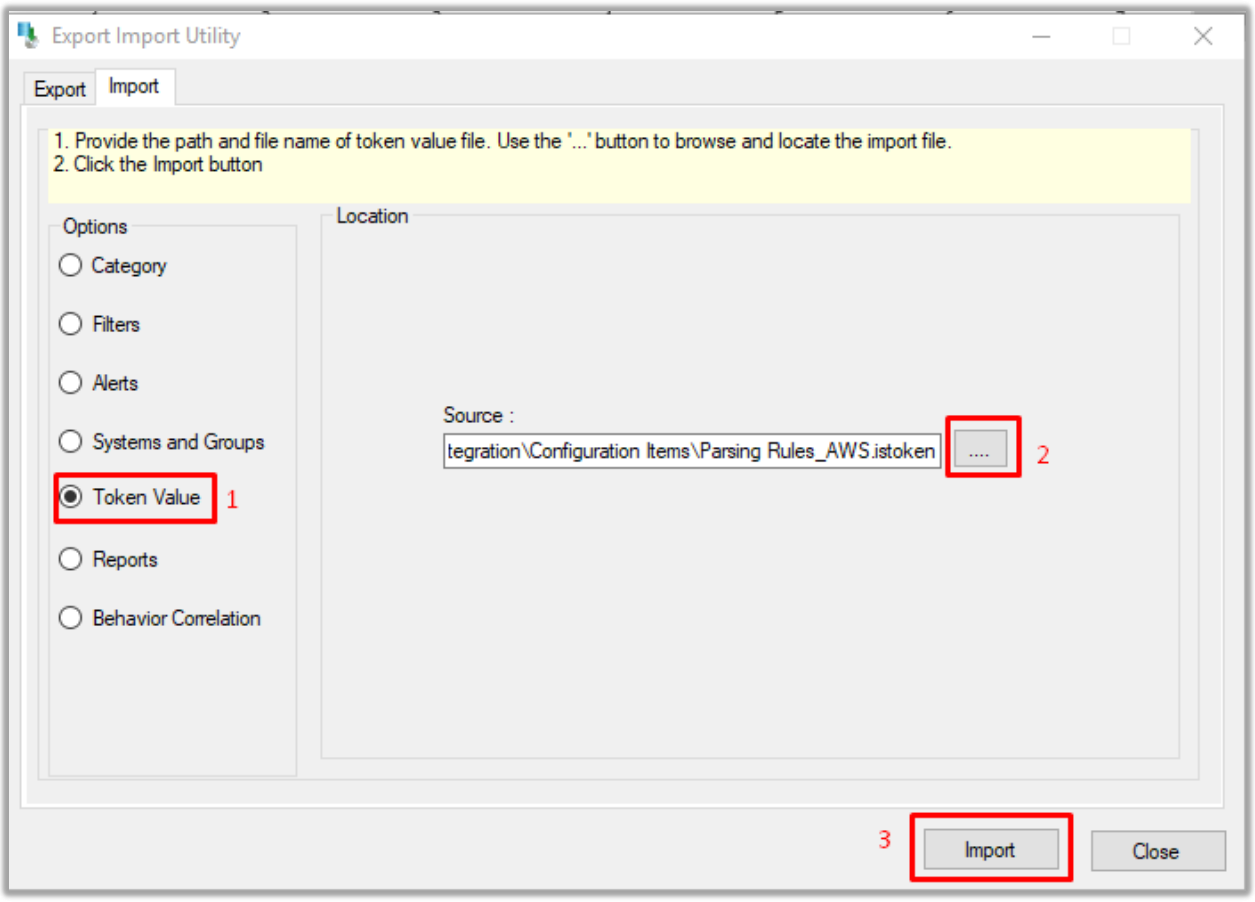
3. EventTracker displays a success message:



5.3 Token Value

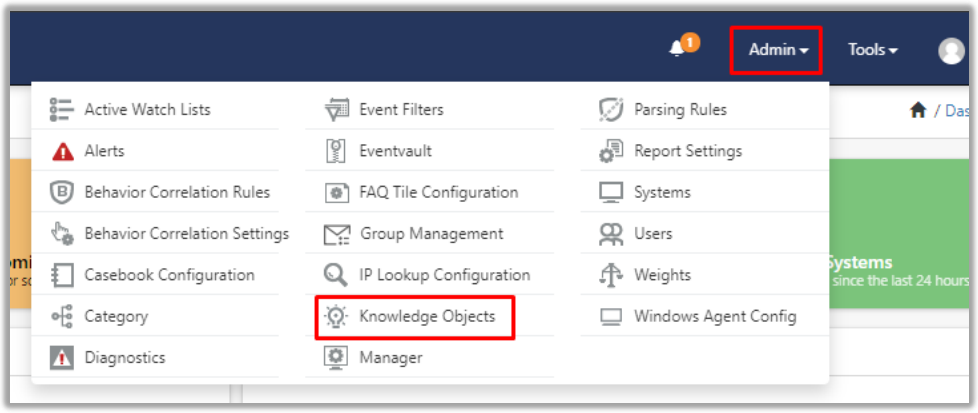
1. In EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Click **Reports** option and choose **New (*.istoken).**
2. Navigate to the location having a file with the extension **".istoken**" and then click **Import**.

© Copyright Netsurion. All Rights Reserved.



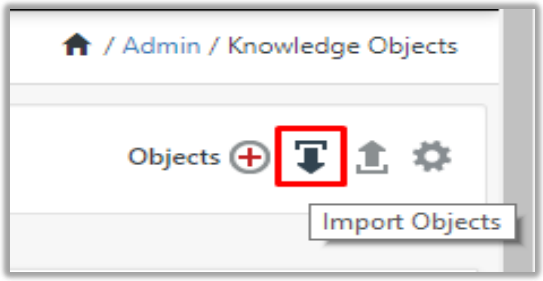
5.4 Knowledge Object

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



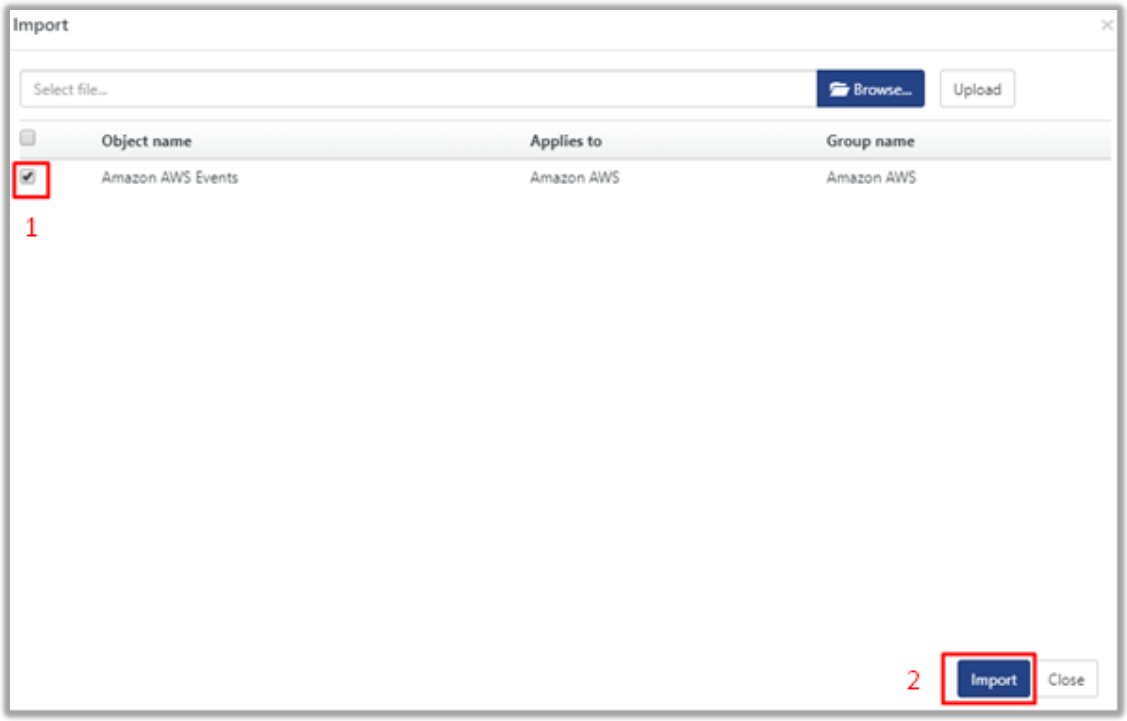
2. Click on the **Import Object** icon.

© Copyright Netsurion. All Rights Reserved.



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

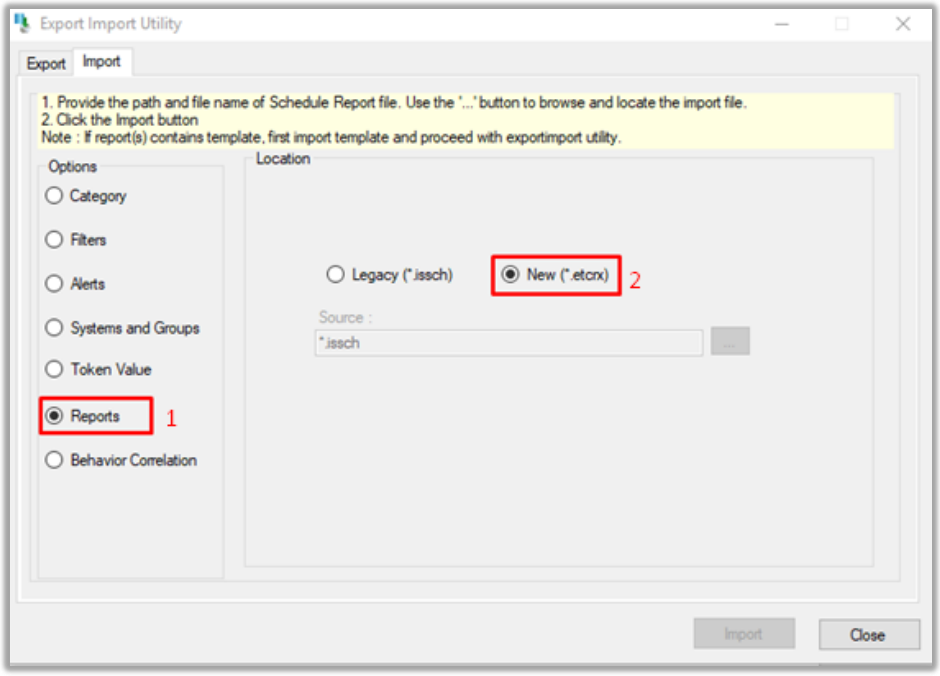
4. A list of available knowledge objects will appear. Select the relevant files and click **Import.**



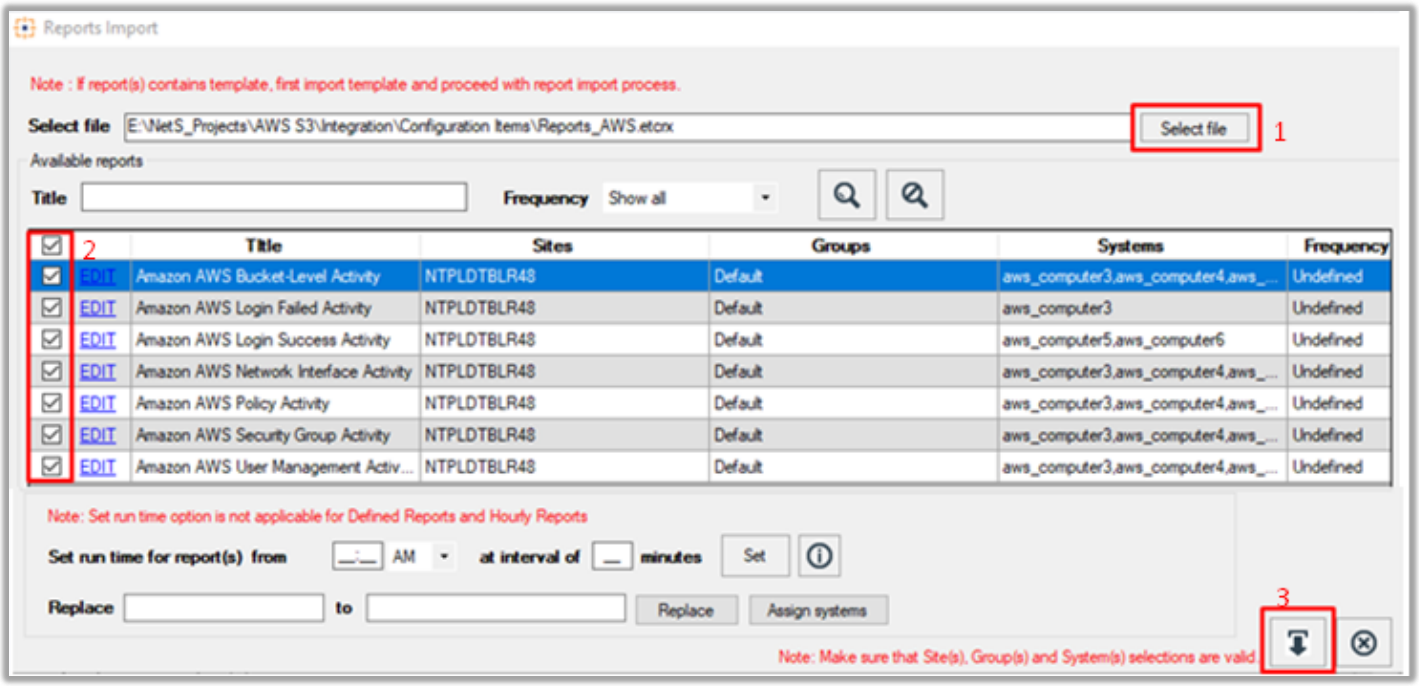
5.5 Flex Reports

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

© Copyright Netsurion. All Rights Reserved.

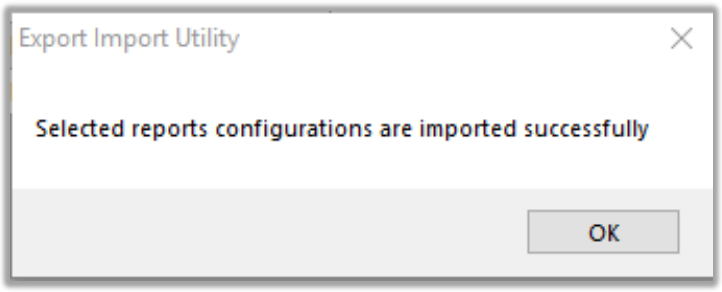


2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click on the **Select File** button and navigate to the file path with a file having the extension **".etcrx**".
3. Select all the relevant files and then click on the **Import** button  .



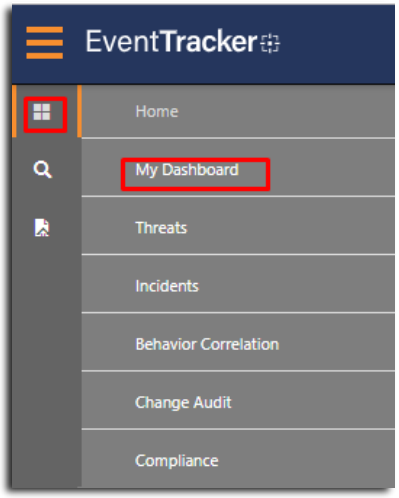
4. EventTracker displays a success message:

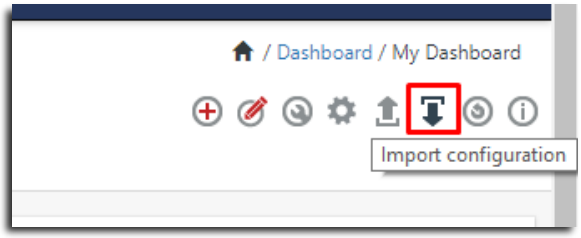
© Copyright Netsurion. All Rights Reserved.



5.6 Dashboard

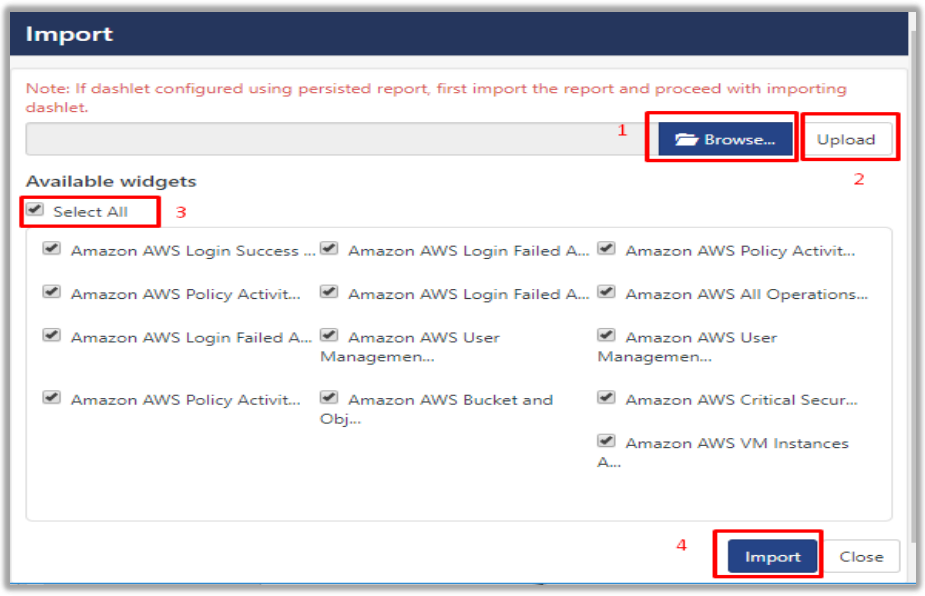
1. Login to **EventTracker**.
2. Navigate to **Dashboard → My Dashboard**.
3. In My Dashboard, click **Import Button**:



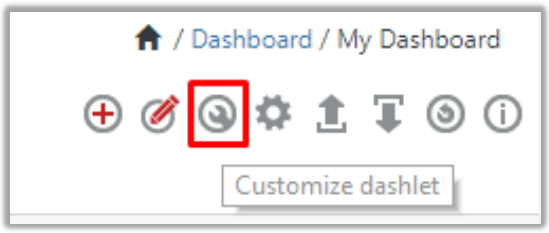


4. Select the **Browse** button and navigate to the file path where the dashboard file is saved and click on the **Upload** button.
5. Once completed, choose **Select All** and click **Import**.

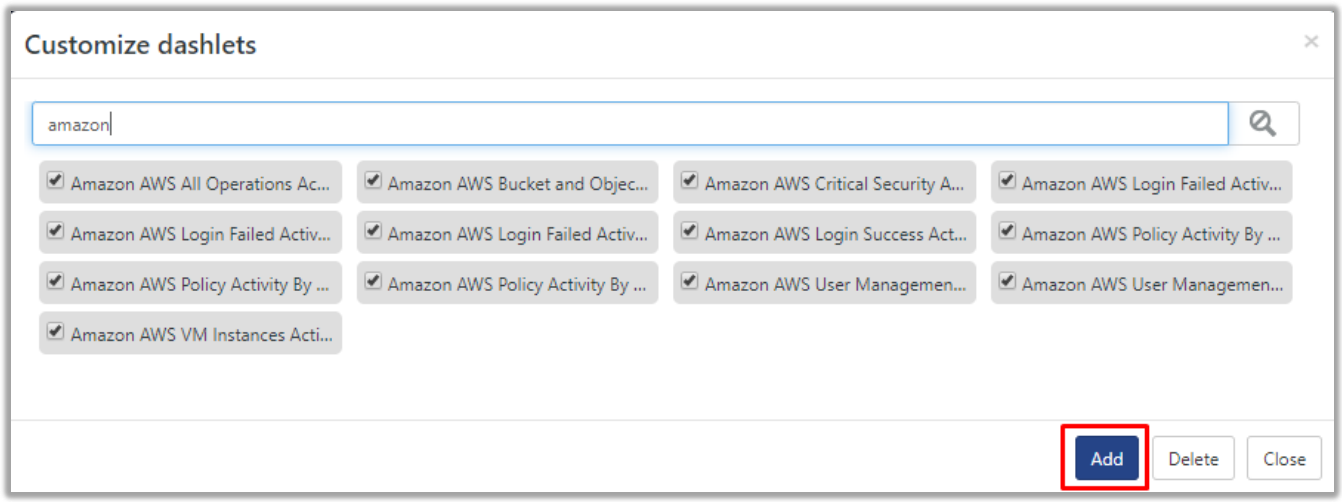
© Copyright Netsurion. All Rights Reserved.



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



7. Put a text on the **Search bar: "Amazon"** and then select the Amazon AWS dashlets and then click the **Add** button.

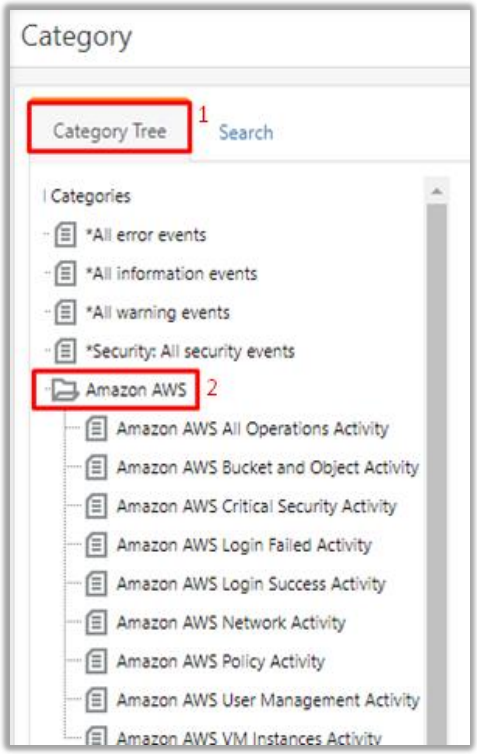


© Copyright Netsurion. All Rights Reserved.

6. Verifying Amazon AWS Knowledge Pack in EventTracker

6.1 Categories

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



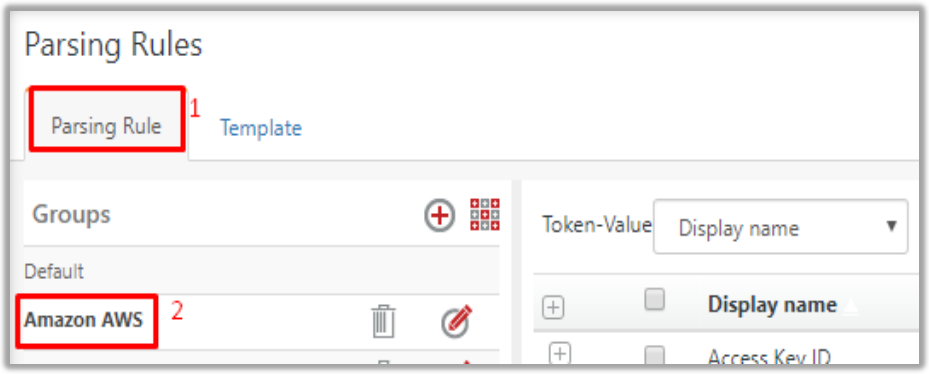
6.2 Alerts

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

© Copyright Netsurion. All Rights Reserved.

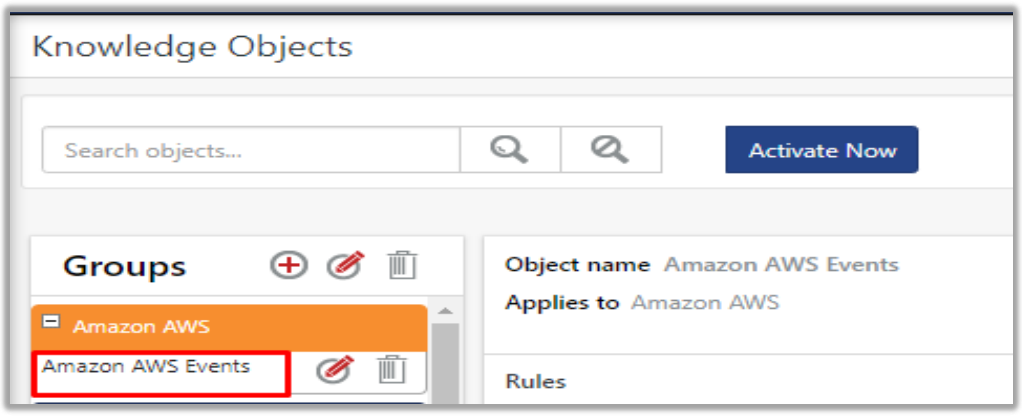
6.3 Token Value

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



6.4 Knowledge Object

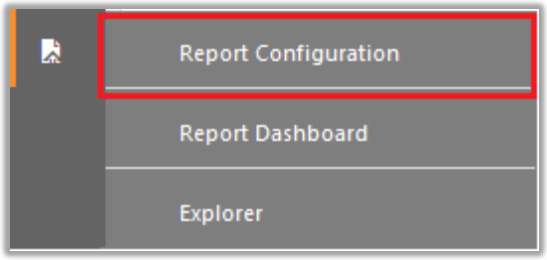
1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **Amazon AWS Events** group folder to view the imported Knowledge objects.



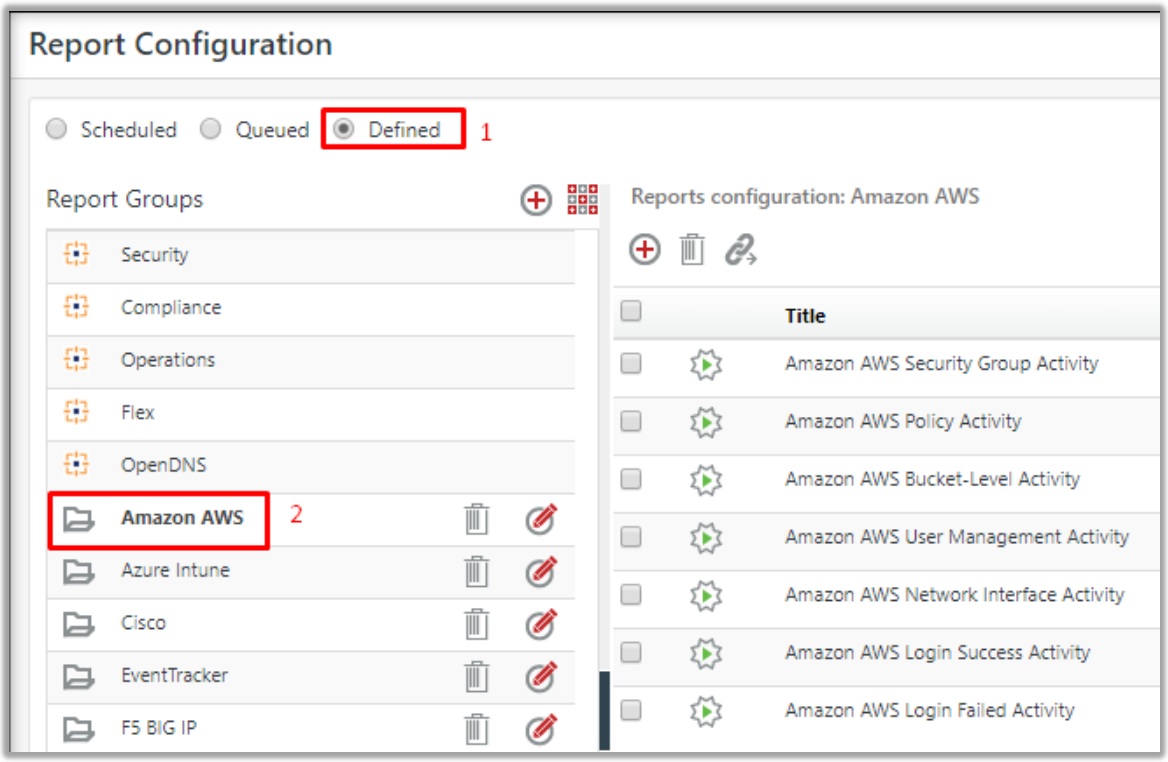
© Copyright Netsurion. All Rights Reserved.

6.5 Flex Reports

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



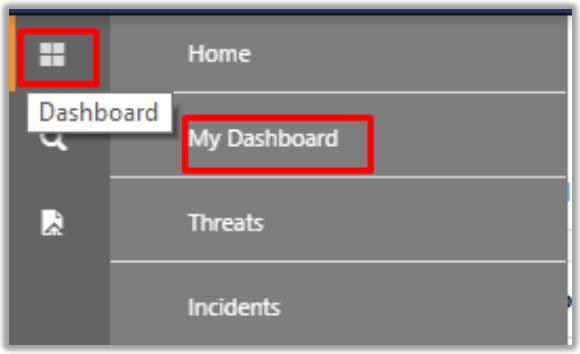
2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Amazon AWS** group folder to view the imported reports.



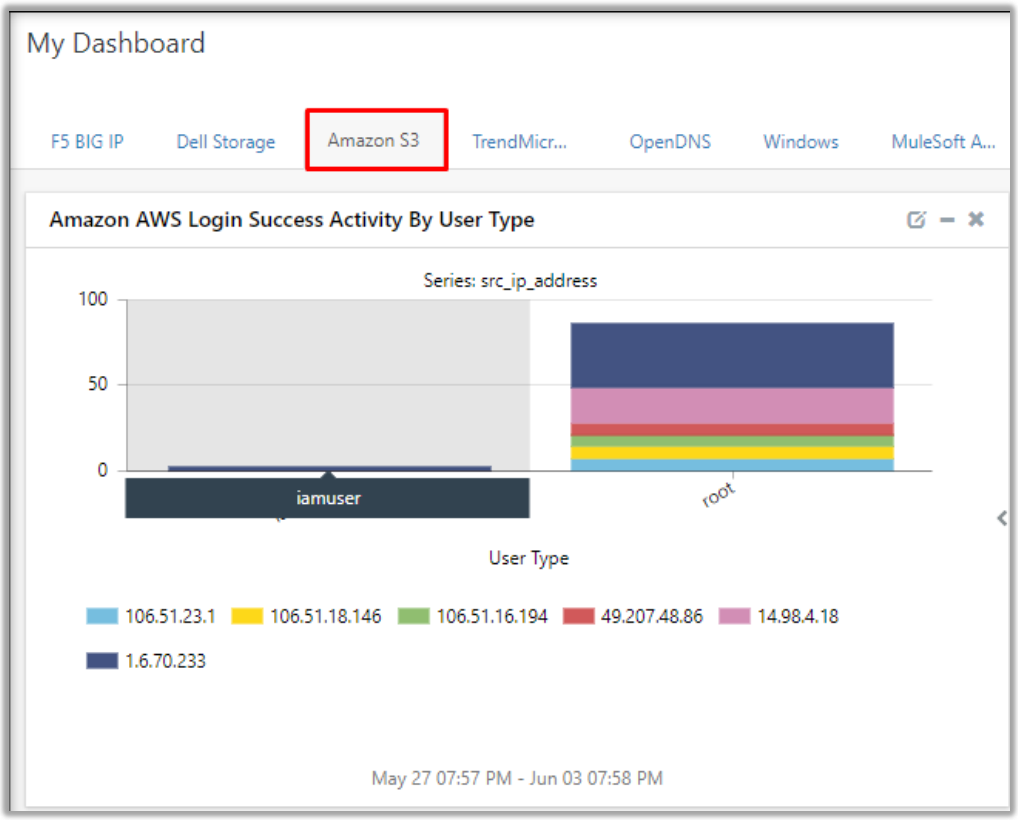
6.6 Dashboard

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

© Copyright Netsurion. All Rights Reserved.



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



© Copyright Netsurion. All Rights Reserved.

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 #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

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

https://www.netsurion.com/company/contact-us

© Copyright Netsurion. All Rights Reserved.