Integrate Amazon Web Services

EventTracker v9.x and above

Publication Date: October 14, 2019
Abstract

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

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and Amazon CloudTrail.

Audience

Administrators who are assigned the task to monitor Amazon CloudTrail Logs using EventTracker.
# Table of Contents

1. Overview ........................................................................................................................................... 3

2. Prerequisites ..................................................................................................................................... 3

3. Configuring Amazon CloudTrail to forward logs to EventTracker .................................................. 3
   3.1 Collecting AWS Account ID ........................................................................................................... 3
   3.2 Creating a S3 Bucket ....................................................................................................................... 4
   3.3 Enabling read-only access for EventTracker ................................................................................. 6
   3.4 Creating a Trail for an Organization ............................................................................................. 13
      3.4.1 Creating a CloudTrail trail with the AWS Management Console ........................................... 13
   3.5 Forwarding the logs to EventTracker ........................................................................................... 17

4. EventTracker Knowledge Pack ............................................................................................................ 21
   4.1 Flex Reports ................................................................................................................................. 21
   4.2 Alerts ........................................................................................................................................... 23
   4.3 Dashboards ................................................................................................................................. 25

5. Importing Amazon AWS knowledge pack into EventTracker ............................................................ 31
   5.1 Categories .................................................................................................................................... 32
   5.2 Alerts ........................................................................................................................................... 33
   5.3 Token Value ................................................................................................................................. 34
   5.4 Knowledge Object ....................................................................................................................... 35
   5.5 Flex Reports ............................................................................................................................... 37
   5.6 Dashboard .................................................................................................................................... 38

6. Verifying Amazon AWS knowledge pack in EventTracker .............................................................. 40
   6.1 Categories .................................................................................................................................... 40
   6.2 Alerts ........................................................................................................................................... 41
   6.3 Token Value ................................................................................................................................. 42
   6.4 Knowledge Object ....................................................................................................................... 42
   6.5 Flex Reports ................................................................................................................................ 42
   6.6 Dashboard .................................................................................................................................... 43
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

- EventTracker agents should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on the host system/ server to run PowerShell.
- User must have root-level access to AWS console.
- You must also have enough permissions for the IAM user or role in the master account to successfully create a trail, bucket, and user.

3. Configuring Amazon CloudTrail to forward logs to EventTracker

The steps provided below will help to configure the EventTracker to receive events from AWS CloudTrail.

3.1 Collecting AWS Account ID

1. Login to your AWS Console.
2. Click on the username in the top right corner and select “My Account”: 
3. A new browser tab will open, check for “Account Settings” section:

Figure 2

3.2 Creating a S3 Bucket

1. Login to your “AWS Management Console for S3”
2. Once logged in, click on “Create bucket”:

Figure 3

3. A new pop-up box will open, “Create bucket”.

Figure 1
4. In the **Bucket name** field, type a unique DNS-compliant name for your new bucket. e.g. ETAdmin_Bucket.
5. In the “**Region**” field, select the desired region of your choice and then click on the “**Create**” button on the bottom left corner.
6. Once, the Bucket is created, navigate to “**AWS Management Console for S3**”. Click on the bucket you just created and **save the bucket ARN** (for future reference).
3.3 Enabling read-only access for EventTracker

To enable EventTracker to retrieve CloudTrail log data from your S3 bucket, create a new IAM user on your account. This user will only have read-only permission from the S3 bucket.

1. Login to your AWS Management Console for IAM User to create IAM users.
2. In the navigation pane, choose Users and then choose Add user.

3. In the “Set user details” section, specify the User Name for the new user.

4. In the “Select AWS access type” section, select the type of access this set of users will have. Choose “Programmatic access”:

---

Figure 6

Figure 7

Figure 8
5. Choose **Next: Permissions**.
6. On the **Set permissions** page, specify how you want to assign permissions to this set of new users.
7. Choose “**Attach existing policies to directly**” and click on “**Create Policy**”.

![Figure 9](image)

8. A new browser tab will open. Select the **Visual editor** tab. In the **Service** section type “**S3**”.
9. A Service hyperlink for “**S3**” will appear, click on it.

![Figure 10](image)

10. Once you click on “**S3**” hyperlink, fields will automatically populate in “**Action**” section:

![Figure 11](image)
11. In the “List” option, select as below image:

![Figure 12](image12.png)

12. In the “Read” option, select as below image:

![Figure 13](image13.png)

13. Next is the “Resources” section. Click on “Resources” to expand it. Now, select “Specific” option:

![Figure 14](image14.png)
14. You will be presented with two options:

![Figure 15](image1)

15. For the “bucket” option, click on “Add ARN” hyperlink and paste the bucket ARN which was saved during bucket creation and click “Add”.

![Figure 16](image2)

16. For the “object” option, put a tick on “Any”:

![Figure 17](image3)
17. Now, click on “Review Policy” button in the bottom right corner:

![Review Policy Button](image18)

Figure 18

18. In the review Policy page, mention the Policy Name and press the “Create policy” button.

![Create Policy](image19)

Figure 19

19. Your policy is now created. Revert to the “IAM Add user” tab in the browser. Refresh the policy list and select the recently created policy and press “Next: Tags” button –
20. Skip the “Add Tags” and click on “Next: Review”: 
21. In the next step, i.e. “Review”, verify all the values are correct and click the “Create user” button:

![Figure 22](image)

22. We are in the last step of creating a new IAM user. Your IAM user is now successfully created and you will be given an option to save the **Access Key ID** and **secret access key**. Click on the “Download .csv” button to download the ID and key and save it in your desired folder.

**Note** – This file will be imported while running the EventTracker Integrator.exe

![Figure 23](image)
3.4 Creating a Trail for an Organization

To maintain an ongoing record of events in an AWS account, users must first create a “trail”. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket.

**Note** - You must enable all features in your organization before you can create an organization trail.

3.4.1 Creating a CloudTrail trail with the AWS Management Console

1. Login to your “AWS Management console for CloudTrail”.
2. On the Left-hand panel, select “Trail” and click on “Create trail”:

![Figure 24](image)

3. On the “Create Trail” section, specify the “Trail name”. (CloudTrail Trail Naming Requirements)
4. The next step would be to select the region for which “trail” has to be enabled. For this, there are three options:
   - “All region” - Creates the same trail in all regions and delivers log files for all regions.

![Figure 25](image)
• “Current region” - Creates the trail in the current logged-in region and delivers log files for this region.

![Create Trail](image)

Figure 26

• “Manual assignment” – User must create a trail for each region they want the trail for, by logging into each region independently. For this, navigate to the top right corner and choose the region dropdown box:

![Region Dropdown](image)

Figure 27

5. Moving on to the “Management events” section, for Read/Write events, choose if you want your trail to log **All, Read-only, Write-only, or None**, and then choose **Save**.
6. On the “Data events” section, you can specify logging data events for **Amazon S3 buckets**, for **AWS Lambda functions**, or both.
   a. For Amazon S3 buckets: **(Choose the S3 tab)**
      I. To log data events for all S3 buckets in your AWS account, choose to **Select all S3 buckets in your account**. Then choose whether you want to log **Read** events, such as GetObject, **Write** events, such as PutObject, or both.
      II. To specify a bucket, choose the **Add S3 bucket**. Type the S3 bucket name and prefix (optional) for which you want to log data events. For each bucket, specify whether you want to log **Read** events, such as GetObject, **Write** events, such as PutObject, or both.

   ![Data events S3 tab](image)

   **Figure 28**

   b. For Lambda functions: **(Choose the Lambda tab)**
      I. To specify logging individual functions, select them from the list. **Note** - If you want to log data events for specific functions, you can manually add a function if you know its ARN.
      II. To log data events for all Lambda functions in your AWS account, select **Log all current and future functions**.
7. On the “Storage location” section, under “Create a new S3 bucket” choose “No” and then under “S3 bucket” select the Bucket Name you created in the earlier section.

8. To configure advanced settings, see Configuring Advanced Settings for Your Trail. Otherwise, choose to Create.
9. The new trail appears on the **Trails** page.

![Figure 33](image)

**3.5 Forwarding the logs to EventTracker**

1. Contact the [EventTracker support](#) team and get the “**AWS Integrator**” executable file.
2. Once the executable application is received, right click on the file and select “Run as Administrator”.
3. Run the Integrator, fill-in the given fields.
4. The First option is, “**Account ID**”. Refer to “**How to guide**” to get an account ID.

![Figure 34](image)

5. For “**Access Key ID**” and “**Secret Access Key**”, if you already have downloaded the “**credentials.csv**” file when creating an IAM user, click on the “**Select *.csv**” button and navigate to file path of “**credentials.csv**”. Doing so will populate the “**Access Key ID**” and “**Secret Access Key**” automatically.

![Figure 35](image)
Note – If you do not have the “credentials.csv” file, you can manually enter the keys

6. Next, is filling the “AWS Bucket Name”. Enter the S3 bucket name.

Note - Press “Ctrl” Key and select multiple regions, if any.
9. Click on the “Validate” button to verify the credentials:

10. Upon successful Validation, a message pops-up, click “OK”:
11. The “submit” button will now be enabled for finalize the process, click “Submit”:

![Figure 41](image1.png)

12. A message pops-up for successful integration, click “OK”:

![Figure 42](image2.png)
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.

![Figure 43](image)

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

![Figure 44](image)
• **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.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Type</th>
<th>Requested Action</th>
<th>Source IP Address</th>
<th>Interface Description</th>
<th>Subnet ID</th>
<th>Network Interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/29/2019 11:33:02 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>CreateNetworkInterface</td>
<td>12.6.70.33</td>
<td>testinterface</td>
<td>subnet-1/108b675</td>
<td>983cc0302e1be3f0</td>
</tr>
<tr>
<td>05/29/2019 11:33:05 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>DeleteNetworkInterface</td>
<td>12.6.70.33</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/29/2019 12:05:22 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>CreateNetworkInterface</td>
<td>12.6.70.33</td>
<td>testinterface</td>
<td>subnet-1/108b675</td>
<td>983cc0302e1be3f0</td>
</tr>
<tr>
<td>05/29/2019 12:06:18 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>DeleteNetworkInterface</td>
<td>12.6.70.33</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/29/2019 12:06:22 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>CreateNetworkInterface</td>
<td>12.6.70.33</td>
<td>testinterface</td>
<td>subnet-1/108b675</td>
<td>983cc0302e1be3f0</td>
</tr>
<tr>
<td>05/01/2019 02:02:16 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>CreateNetworkInterface</td>
<td>12.6.70.33</td>
<td>AWS Internal</td>
<td>subnet-1/108b675</td>
<td>983cc0302e1be3f0</td>
</tr>
</tbody>
</table>

Figure 45

• **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.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Type</th>
<th>Account ID</th>
<th>Region</th>
<th>Source IP Address</th>
<th>Requested Action</th>
<th>User Name</th>
<th>Group Name</th>
<th>User ARN</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/27/2019 05:38:07 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>247855xxxxx</td>
<td>us-east-1</td>
<td>12.6.70.233</td>
<td>RemoveUserFromGroup</td>
<td>Karen</td>
<td>mypp</td>
<td></td>
</tr>
<tr>
<td>05/27/2019 05:39:07 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>247855xxxxx</td>
<td>us-east-1</td>
<td>12.6.70.233</td>
<td>AddUserToGroup</td>
<td>Karen</td>
<td>mypp</td>
<td></td>
</tr>
<tr>
<td>05/28/2019 11:32:35 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>247855xxxxx</td>
<td>us-east-1</td>
<td>12.6.70.234</td>
<td>AddUserToGroup</td>
<td>John</td>
<td>CloudWatch</td>
<td></td>
</tr>
<tr>
<td>05/28/2019 11:32:36 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>247855xxxxx</td>
<td>us-east-1</td>
<td>12.6.70.235</td>
<td>AddUserToGroup</td>
<td>Mike</td>
<td>Read_only</td>
<td></td>
</tr>
<tr>
<td>05/28/2019 11:32:36 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>247855xxxxx</td>
<td>us-east-1</td>
<td>12.6.70.236</td>
<td>DeleteUser</td>
<td>Mike</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/28/2019 11:32:36 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>247855xxxxx</td>
<td>us-east-1</td>
<td>12.6.70.237</td>
<td>CreateUser</td>
<td>Mike</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/28/2019 11:32:36 AM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>247855xxxxx</td>
<td>us-east-1</td>
<td>12.6.70.238</td>
<td>CreateUser</td>
<td>John</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 46

• **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.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Type</th>
<th>Account ID</th>
<th>Region</th>
<th>Source IP Address</th>
<th>Requested Action</th>
<th>Bucket Name</th>
<th>Error Code</th>
<th>Bucket Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/27/2019 05:27:02 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>2000361xxxxx</td>
<td>us-east-2</td>
<td>12.6.70.233</td>
<td>GetBucketEncryption</td>
<td>envelope192</td>
<td>ServerSideEncryption</td>
<td>ConfigurationNotRun</td>
</tr>
<tr>
<td>05/27/2019 05:27:02 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>2000361xxxxx</td>
<td>us-east-2</td>
<td>12.6.70.234</td>
<td>GetBucketPublicAccess</td>
<td>envelope192</td>
<td>NoS3PublicAccess</td>
<td>BlockConfiguration</td>
</tr>
<tr>
<td>05/29/2019 12:03:12 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>2000361xxxxx</td>
<td>us-east-2</td>
<td>172.18.144.11</td>
<td>CreateBucket</td>
<td>envelope192</td>
<td>AccessDenied</td>
<td></td>
</tr>
<tr>
<td>05/28/2019 02:30:54 PM</td>
<td>AWS_COMPUTERS</td>
<td>Root</td>
<td>2000361xxxxx</td>
<td>us-east-2</td>
<td>172.18.144.11</td>
<td>PutBucketPolicy</td>
<td>envelope192</td>
<td>S3 = AWSCloudFront</td>
<td></td>
</tr>
</tbody>
</table>

Figure 47
- **Amazon AWS Policy Activity** – This report will generate a detailed view of the activities related to policy, i.e. AttachUserPolicy, GetPolicy, DetachRolePolicy, CreatePolicy, etc.

<table>
<thead>
<tr>
<th>Event DateTime</th>
<th>Computer</th>
<th>User Type</th>
<th>Account ID</th>
<th>Source IP Address</th>
<th>Service Name</th>
<th>Region</th>
<th>Requested Action</th>
<th>Policy ARN</th>
<th>User Name</th>
</tr>
</thead>
</table>

Figure 48

- **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.

<table>
<thead>
<tr>
<th>Event DateTime</th>
<th>Computer</th>
<th>User Type</th>
<th>Account ID</th>
<th>Source IP Address</th>
<th>Region</th>
<th>Requested Action</th>
<th>Group Name</th>
<th>Group ID</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-05-27T06:30:58Z</td>
<td>AWS COMPUTERS</td>
<td>Root</td>
<td>2000361xxxx</td>
<td>12.6.70.233</td>
<td>us-east-2</td>
<td>CreateSecurityGroup</td>
<td>test_securitygroup</td>
<td>sg-0de86943e4f26752a</td>
<td></td>
</tr>
<tr>
<td>2019-05-27T06:30:11Z</td>
<td>AWS COMPUTERS</td>
<td>Root</td>
<td>2000361xxxx</td>
<td>12.6.70.234</td>
<td>us-east-2</td>
<td>DeleteSecurityGroup</td>
<td>sg-0de86943e4f26752a</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 49

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.

• **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.**

![Amazon AWS Login Success Activity By User Type](image)

*Figure 50*

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

![Amazon AWS Login Failed Activity By Failed Reason](image)

*Figure 51*
• **Amazon AWS Policy Activity By Source IP.**

![Amazon AWS Policy Activity By Source IP](image1)

*Figure 52*

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

![Amazon AWS Policy Activity By User Type](image2)

*Figure 53*
• Amazon AWS Login Failed Activity By User Agent.

![Amazon AWS Login Failed Activity By User Agent](image)

Figure 54

• Amazon AWS All Operations Activity By Event Name.

![Amazon AWS All Operations Activity By Event Name](image)

Figure 55
• Amazon AWS Login Failed Activity By City.

![Amazon AWS Login Failed Activity By City](image)

Figure 56

• Amazon AWS User Management Activity By User Added.

![Amazon AWS User Management Activity By User Added](image)

Figure 57
- Amazon AWS User Management Activity By User Deleted.

![Amazon AWS User Management Activity By User Deleted](image)

*Figure 58*

- Amazon AWS Policy Activity By Service Name.

![Amazon AWS Policy Activity By Service Name](image)

*Figure 59*
• **Amazon AWS Bucket and Object Activity By Error Codes.**

![Amazon AWS Bucket and Object Activity By Error Codes](Image)

*Figure 60*

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

![Amazon AWS Critical Security Activity By Source IP Address](Image)

*Figure 61*
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.

### 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 on the “**Import**” button:
3. EventTracker displays a success message:

![Success Message](image)

**Figure 65**

### 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 on the “**Import**” button:
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 on the “Import” button:
5.4 Knowledge Object

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

Figure 69
2. Next, click on the “import object” icon:

   ![Figure 70](image)

3. A pop-up box will appear, click “Browse” in that and navigate to the file path with extension “.etko” button

   ![Figure 71](image)

4. A list of available knowledge objects will appear. Select the relevant files and click on “Import” button:

   ![Figure 72](image)
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)”:

![Figure 73](image)

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:

![Success message](image)

**Figure 75**

### 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 on “**Import**” Button.
6. Click “Customize dashlet” button as shown below:

![Customize dashlet](image)

Figure 79

7. Now, put a text on the **Search bar**: “Amazon” and then select the Amazon AWS Dash-lets and then click the “Add” button.

![Customize dashlets](image)

Figure 80

### 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”:

![Figure 82](image-url)
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.

![Parsing Rules](image1)

Figure 83

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.

![Knowledge Objects](image2)

Figure 84

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**”
2. In “Amazon AWS” dashboard you should be now able to see something like this: