Netsurion | EventTracker®

Integrate Barracuda Web Application

EventTracker v9.x and above

Publication Date: October 28, 2019

Abstract

This guide provides instructions to retrieve Barracuda Web Application event logs and integrate it with EventTracker. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Barracuda Web Application.

Audience

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and Barracuda Web Application.

Table of Contents

1.Overview

Barracuda offers a Web Application Firewall (WAF) that provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

2.Integrating Barracuda WAF with EventTracker

1. Log into the Barracuda Web Application Firewall web interface.
2. Go to ADVANCED > Export Logs.
3. In the syslog section, click Add syslog server and specify the following:
    - **Name** - Enter a name for the syslog server.
    - **IP Address** – Enter the IP address of the EventTracker manager.
    - **Port** – Enter the port number on which the syslog VCP configuration (e.g. 514).
    - **Connection Type** – Set the connection type to transmit the logs from the Barracuda Web Application Firewall to the syslog server.
4. Verify that the logs in EventTracker manager are received or not.

3.EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.
The following Knowledge Packs are available in EventTracker to support Barracuda Web Application.

3.1 Flex Reports

- **Barracuda Web Application – Traffic Activity :** This report gives you information about the access log along with the username, source IP address, destination IP and session ID.

3.2 Saved Searches

- **Barracuda Web Application – Traffic Activity :** This saved search gives you information about the access log along with the username, source IP address, destination IP and session ID.

4. Importing Barracuda Web Application knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Knowledge Objects
- Token Template.
- Flex Reports.
- Categories.
- Dashboard.

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

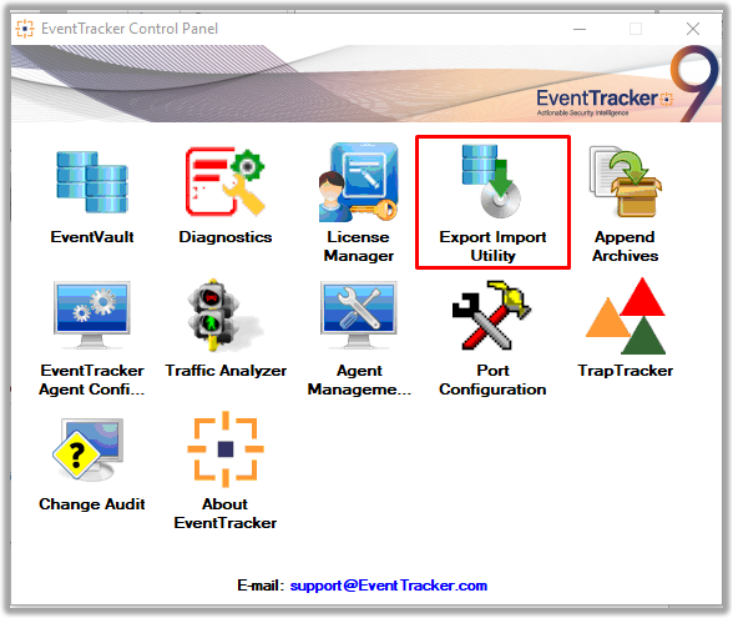

Figure 1

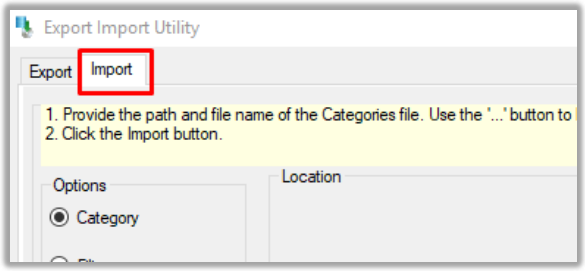

Figure 2

3. Click the **Import** tab.

4.1 Knowledge Object

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

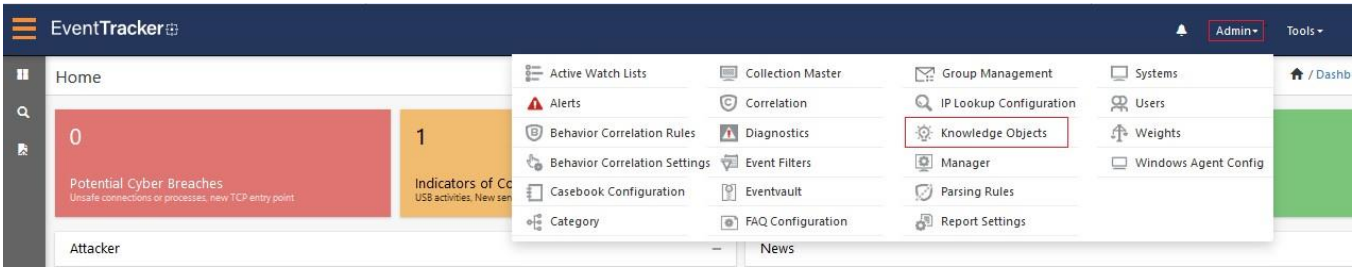

Figure 3

2. Click on the **Import** button.
3. Click on **Browse**.

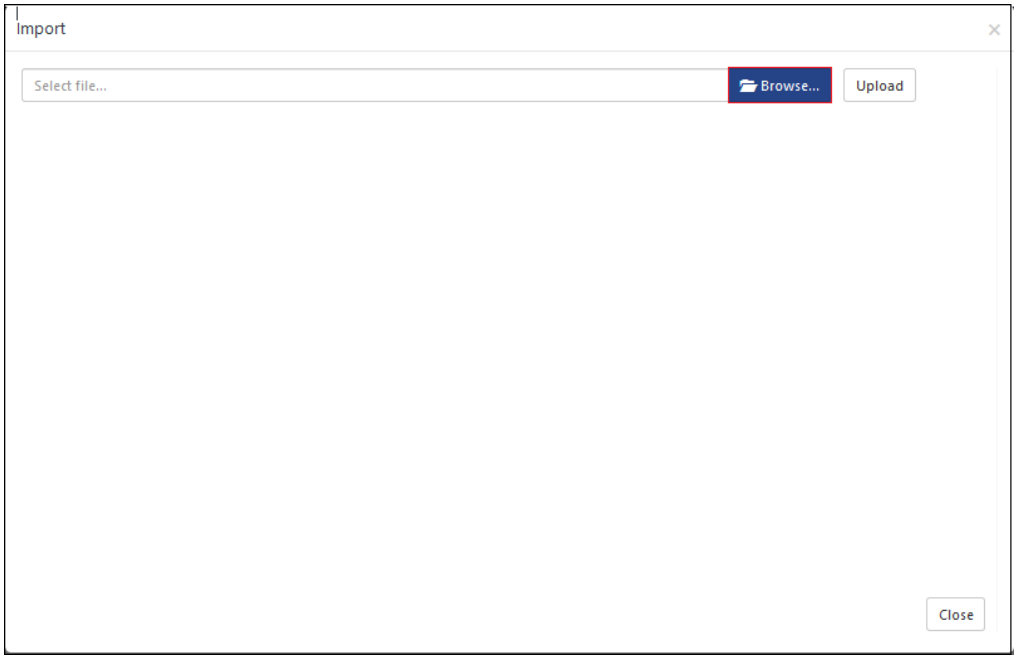

Figure 4

4. Locate the file named **KO_JIRA.etko**.
5. Now select all the checkbox and then click on '**Import**' option.
6. Knowledge objects are now imported successfully.

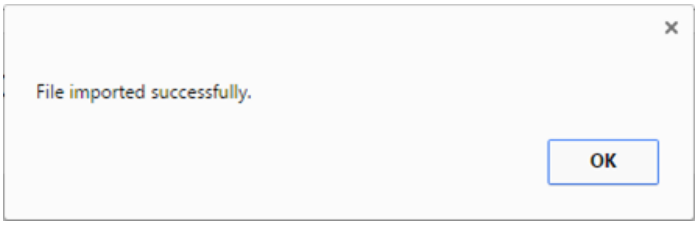

Figure 5

4.2 Token template

1. Click on the **Parsing rule** under the **Admin** option in the EventTracker manager page.

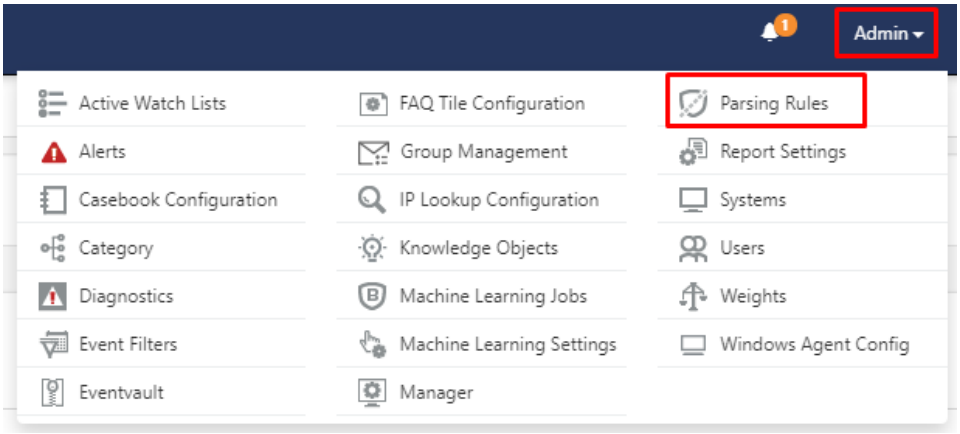

Figure 6

2. Select **Template** and click on **import** icon in the top right corner.

Figure 7

3. Select the file of type ***.ettd**(EventTracker template dashlets.)
4. Select all the Barracuda Web Application template name.
5. And click on the **import** icon.

6. Template(s) imported successfully.

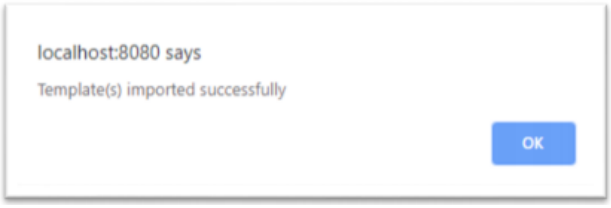

Figure 8

4.3 Flex Reports

1. In the EventTracker control panel, select "**Export/ Import utility**" and select the "**Import tab**". Then, click **Reports** option, and choose "**New (*.etcrx)**":

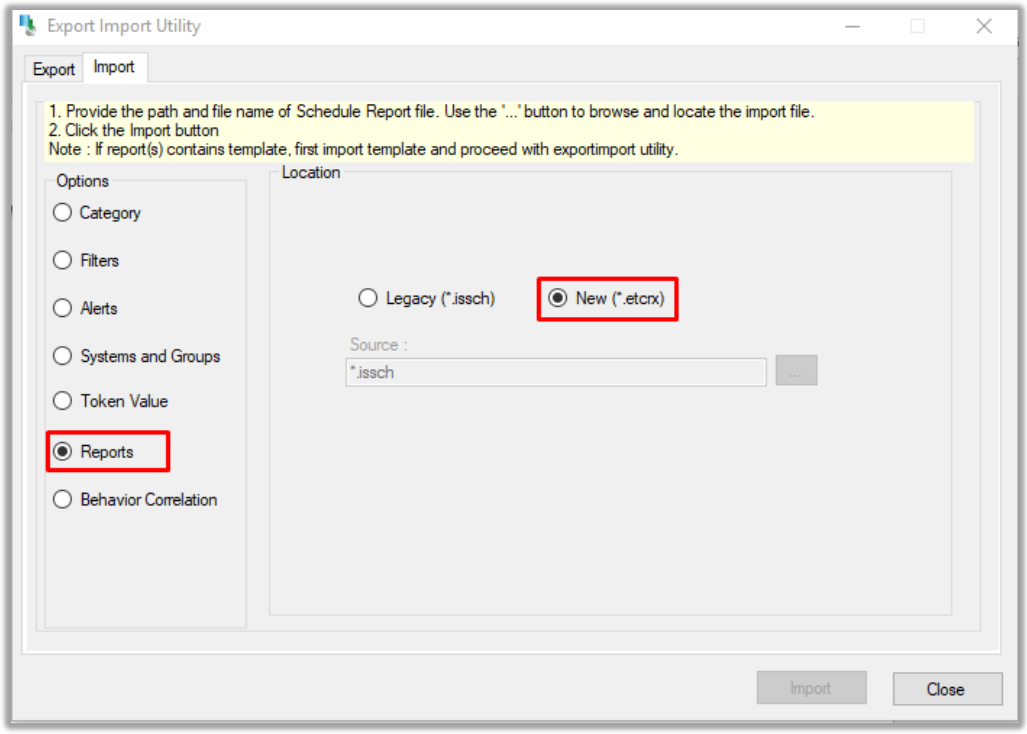

Figure 9

2. Once you have selected "**New (*.etcrx)**", a new pop-up window appears. 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 **Import** button.
4. EventTracker displays a success message:

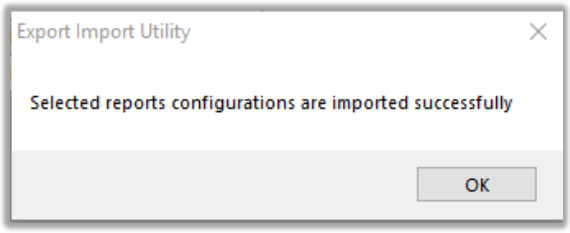

Figure 10

4.4 Category

1. Click the **Category** option, and then click the ... browse button.
2. Locate the **Category_Barracuda Web Application.iscat** file, and then click the open button.
3. To import category, click the Import button.
4. EventTracker displays a success message.

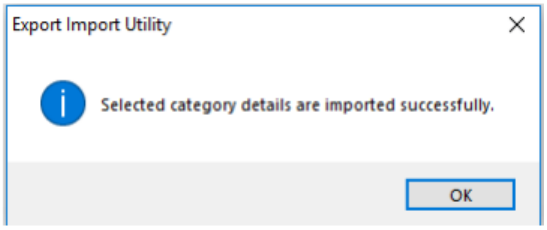

Figure 11

5. Click the OK button, and then click the Close button.

5. Verifying Barracuda Web Application knowledge pack in EventTracker

5.1 Knowledge Object

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

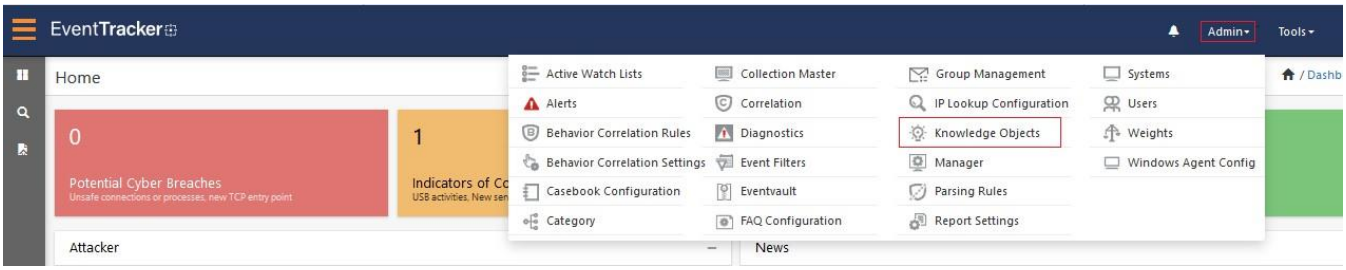

Figure 12

2. In the Knowledge Object tree, expand the **Barracuda Web Application** group folder to view the imported Knowledge objects.

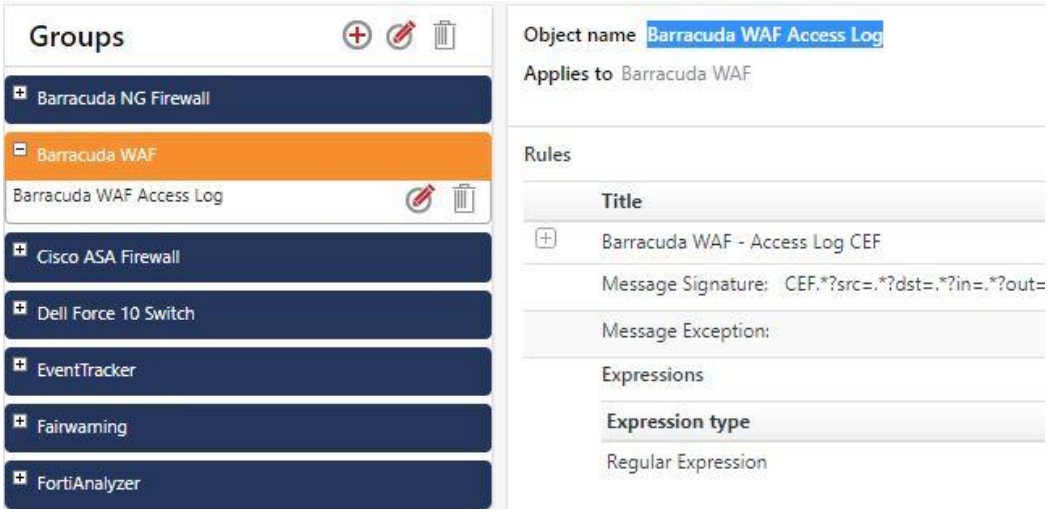

Figure 13

5.2 Token template

1. Click on **Parsing rules** under **Admin**.

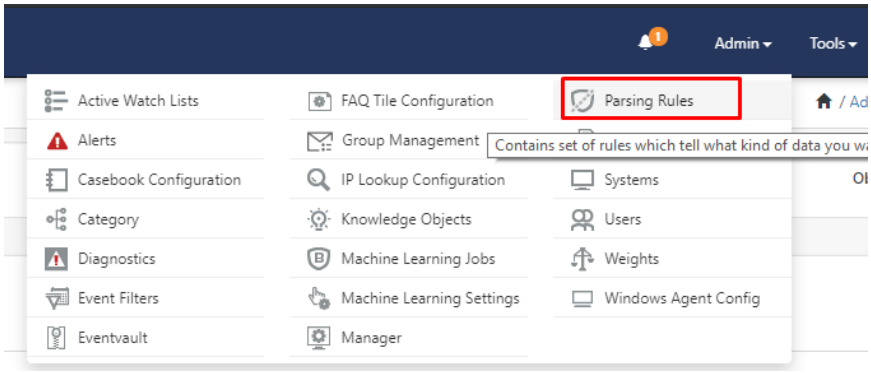

Figure 14

2. Select **template** under parsing rules and select the **Barracuda Web Application** group.
3. All the templates are present under **Barracuda Web Application**.

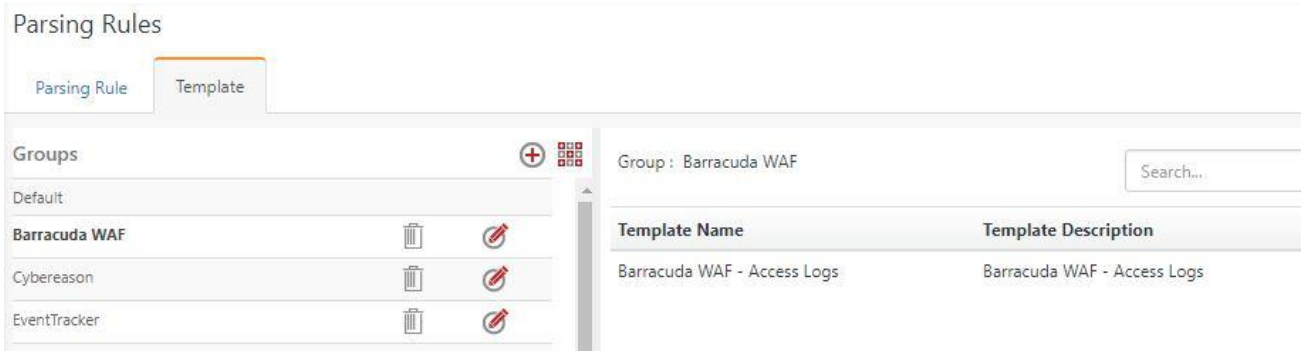

Figure 15

5.3 Flex Reports

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

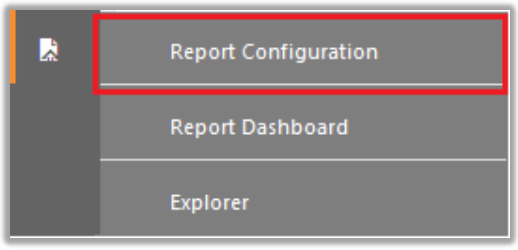

Figure 16

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

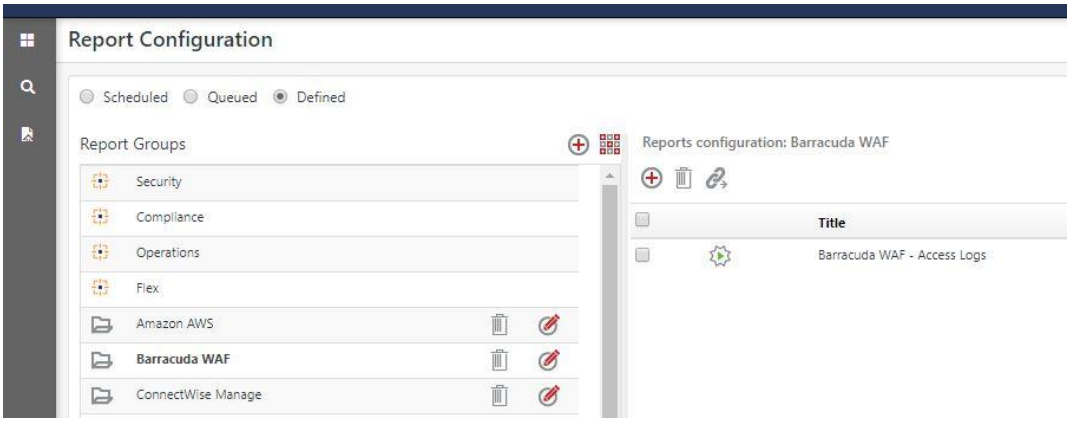

Figure 17

5.4 Category

1. Login to EventTracker.
2. Click the **Admin** menu, and then click **Category**.

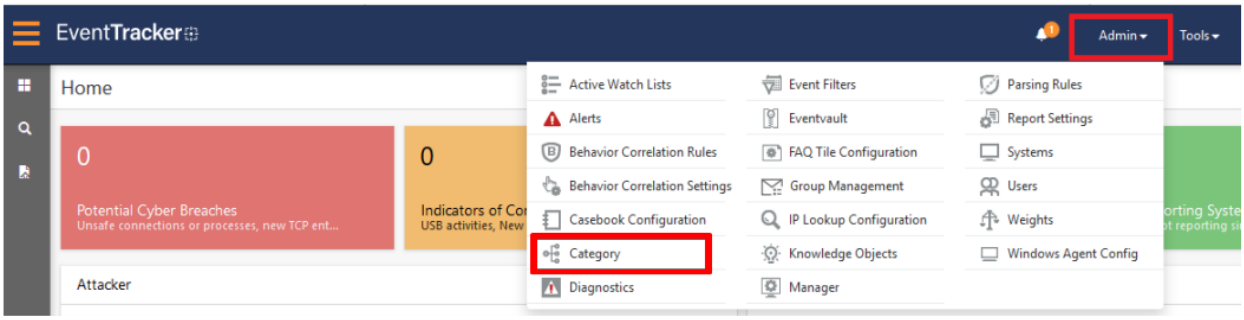

Figure 18

3. Click the search, and then search with Barracuda Web Application.

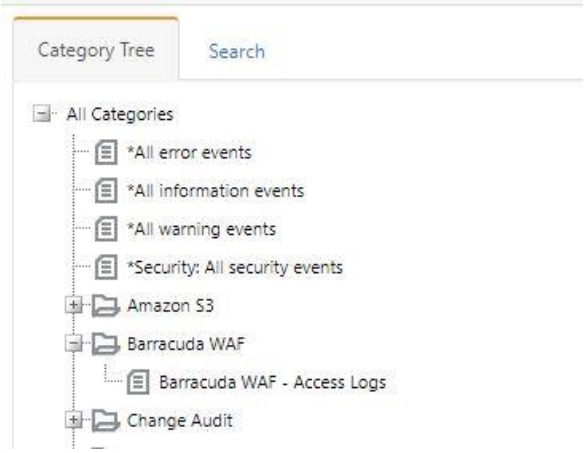

Figure 19