Integrate EZproxy
Abstract

This guide provides instructions to configure EZproxy to send the critical events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and EZproxy 6.x or later.

Audience

Administrators, who are responsible for monitoring EZproxy using EventTracker Manager.
# Table of Contents

Abstract .................................................................................................................................................. 1
Overview .................................................................................................................................................. 3
Prerequisites ............................................................................................................................................ 3
Configure EZproxy to send events to EventTracker ............................................................................. 3
   EZProxy syslog configuration ............................................................................................................. 3
   EZProxy audit log configuration ........................................................................................................ 4
   EventTracker DLA configuration ......................................................................................................... 5
EventTracker Knowledge Pack (KP) ......................................................................................................... 8
   Reports ................................................................................................................................................ 8
   Categories .......................................................................................................................................... 9
   Knowledge Objects ........................................................................................................................... 9
Import EZproxy Knowledge Pack into EventTracker ............................................................................ 9
   Import Parsing Rules ......................................................................................................................... 10
   Import Token Templates .................................................................................................................... 11
   Import Flex Reports .......................................................................................................................... 13
   Import Knowledge Object .................................................................................................................. 14
Verify EZproxy knowledge pack in EventTracker ................................................................................ 16
   Verify Parsing Rules .......................................................................................................................... 16
   Verify Token Templates ..................................................................................................................... 16
   Verify Flex Reports ............................................................................................................................ 17
   Verify Knowledge Object ................................................................................................................... 18
Create Dashboards in EventTracker ....................................................................................................... 19
   Schedule Reports ............................................................................................................................... 19
   Create Dashlets ................................................................................................................................. 21
Sample Dashboards .................................................................................................................................. 25
Sample Reports ........................................................................................................................................ 27
Overview

**EZproxy** is a web proxy server used by organizations to give access from outside the cooperation’s computer network to restricted-access websites that authenticate users by IP address.

EventTracker collects and analyzes critical events to provide an administrator insight on client traffic, user behavior and intrusion attempts.

Prerequisites

- **EventTracker v7.x or later** should be installed.
- **EZproxy v6.X or later** should be installed on Linux.

Configure EZproxy to send events to EventTracker

**EZProxy syslog configuration**

Following are the steps for forwarding usage logs from EZProxy to EventTracker machine using syslog.

1. First, check the location of EZproxy log file through `/usr/local/ezproxy/conf.txt`

Figure 1
2. Make an entry in the `/etc/rsyslog.conf` file as shown:

```
*.info /var/log/ezp.log
```

3. Make entry in the end of `/etc/rsyslog.conf` file as shown:

```
*.* @EventTracker Machine IP or hostname
```

**NOTE** - To generate and consume audit events, the additional directives are added to config.txt and the EventTracker DLA is configured.

### EZProxy audit log configuration

1. To enable **audit and intrusion logging** add following directives to `config.txt` file in EZproxy installation directory. As tabulated:

<table>
<thead>
<tr>
<th>Event</th>
<th>Directive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Events</td>
<td>Audit Login.Denied Login.Success Login.Success.Groups Login.Failure</td>
</tr>
<tr>
<td>Intrusion Events</td>
<td>IntruderIPAttempts -interval=5 -expires=15 20</td>
</tr>
<tr>
<td></td>
<td>IntruderUserAttempts -interval=5 -expires=15 10</td>
</tr>
</tbody>
</table>

**Table 1**

2. To transfer audit log files to EventTracker server, use the following script.

```bash
#!/bin/sh
USERNAME="your-ftp-user-name"
PASSWORD="your-ftp-password"
SERVER="your-ftp.server.com"

# EZproxy local directory to pickup *.txt file
FILE="/var/EZproxy"

# EventTracker remote server directory to upload file
LOGDIR="/EventTracker"

# login to remote server
ftp -n -i $SERVER <<EOF
user $USERNAME $PASSWORD
mkdir $LOGDIR
cd $LOGDIR
mput $FILE/*.*.txt
quit
EOF
```
3. Set a **cron** job for running above mentioned script at specific intervals.
   
   ```
   30 15 * * * /path/to/ftp.exproxy.script.sh
   ```

EventTracker DLA configuration

1. Open **EventTracker** in browser and logon.

   ![Figure 2](image)

   **Figure 2**

2. In EventTracker Enterprise, click the **Admin** drop-down, select **Manager**. Manager Configuration pane is shown:

   ![Figure 3](image)

   **Figure 3**

3. Select **Direct Log Archiver/Netflow Receiver** tab.
4. Select **Direct log file archiving from external sources** checkbox.
5. Click the **Add** button.

Direct Archiver Configuration pane is shown.
Integrate EZproxy

6. Select Others from Type dropdown.
7. Type txt as Logfile Extension.
8. Type an appropriate Configuration Name.
9. Click the Browse button and select path of EZproxy log folder created by above mentioned script.
10. Select Single Line dialog box.
11. Select TAB FROM field separator dropdown.
12. Select Extract fields from header checkbox.
13. Click the Configure button.

Direct archiver configuration pane is shown.

14. Type a fitting Log Source name.
15. Select desired Computer Name, Computer IP and System Type.
16. Scroll down and Click the Save & Close button.
Integrate EZproxy

Saved configuration is shown in DLA pane.

**Figure 7**

17. Click the **Save** button to consolidate changes.

**EventTracker Knowledge Pack (KP)**

Once logs are received in to EventTracker, Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support EZproxy monitoring.

**Reports**

1. **EZproxy - Allowed Traffic Details** – This report provides information related to web traffic allowed by EZproxy which includes device name, client address bytes transferred, request type, requested URI, requested URL, user agent type and user agent details fields.

2. **EZproxy - Denied Traffic Details** – This report provides information related to web traffic denied by EZproxy which includes device name, client address, error type and error details fields.

3. **EZproxy - User Logon Details** – This report provides information related to user logon/logoff events which includes user name, source address, logon status and logon details fields.

4. **EZproxy - Intrusion Details** – This report provides information related to intrusion attempts detected which includes user name, source address and attack type fields.
Categories

1. **EZproxy - Audit Log Purged** - This category briefs an administrator about purging of EZproxy audit logs.
2. **EZproxy - System Startup/Shutdown** - This category briefs an administrator about EZproxy startup and shutdown.

Knowledge Objects

1. **EZproxy - Allowed Traffic** - This KO assists in analysis of web traffic allowed through EZproxy.
2. **EZproxy - Denied Traffic** - This KO assists in analysis of web traffic denied through EZproxy.

**Import EZproxy Knowledge Pack into EventTracker**

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**, and then click the **Import** tab.

![EventTracker Control Panel](image_url)

Figure 8
Import Categories, Alerts, and Reports as given below.

**Import Parsing Rules**

1. Click **Token Value** option, and then click the browse button.
2. Locate **All EZproxy group of tokens.istoken** file, and then click the Open button.

![Figure 9](image)

3. To import token value, click the Import button. EventTracker displays success message.

![Figure 10](image)

4. Click OK, and then click the Close button.
Import Token Templates

1. Click the Admin menu, and then click Parsing rule.
2. Select Template tab, and then click on ‘Import’ option.

![Image of PARSING RULE](image)

**Figure 11**

3. Click on Browse button.

![Image of Browse button](image)

**Figure 12**
4. Locate **EZproxy token template.ettd** file, and then click the **Open** button.

![Image](image1.png)

**Figure 13**

5. Now select the check box and then click on **Import** option. EventTracker displays success message.

![Image](image2.png)

**Figure 14**

6. Click on **OK** button.
Import Flex Reports

1. Click Reports option, and then click the ‘browse’ button.
2. Locate All EZproxy group reports.issch file, and then click the Open button.

![Image of Export Import Utility window](image)

**Figure 15**

3. To import scheduled reports, click the Import button. EventTracker displays success message.

![Image of success message](image)

**Figure 16**

4. Click OK, and then click the Close button.
Import Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects.
2. Click on ‘Import’ option.

![Figure 17](image)

3. In IMPORT pane click on Browse button.

![Figure 18](image)

4. Locate EZproxy KO. etko file, and then click the UPLOAD button.
5. Now select the check box and then click on ‘MERGE’ option. EventTracker displays success message.

6. Click on OK button.
Verify EZproxy knowledge pack in EventTracker

Verify Parsing Rules

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.
3. In Token Value Group Tree to view imported token values, scroll down and click EZproxy group folder.

Token values are displayed in the token value pane.

Verify Token Templates

1. Click the Admin menu, and then click Parsing rule.
2. Select Template tab.
3. In Token Value Group Tree to view imported token values, scroll down and click EZproxy group folder.

Imported token template is displayed in the template pane.
Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported flex reports, scroll down and click EZproxy group folder. Imported reports are displayed in the Reports Configuration pane.

NOTE: Please specify appropriate systems in report wizard for better performance.
Verify Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Scroll down and select **EZproxy** in **Objects** pane.

Imported EZproxy object details are shown.

![Knowledge Objects](image)

Figure 24
Create Dashboards in EventTracker

Schedule Reports

1. Open **EventTracker** in browser and logon.

![Figure 25](image)

2. Navigate to **Reports>Configuration**.

![Figure 26](image)

3. Select **EZproxy** in report groups. Check **defined** dialog box.

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in Eventvault explorer** box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

**Create Dashlets**

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.
3. Navigate to Dashboard>Flex.

Flex Dashboard pane is shown.

4. Click + to add a new dashboard.

Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **Save** button.
6. Click ![+] to configure a new flex dashlet.

Widget configuration pane is shown.

![Widget Configuration](image)

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.
Evaluated chart is shown.

Figure 33

16. If satisfied, click **Configure** button.

Figure 34

17. Click ‘customize’ ☰ to locate and choose created dashlet.

18. Click ✚ to add dashlet to earlier created dashboard.
Sample Dashboards

- **EZproxy User Logons  Events Today**

![EZproxy - User Logons Events Today](image)

**Figure 35**

- **EZproxy Top Intrusion Attempts Today**

![EZproxy - Top Intrusion Attempts Today](image)

**Figure 36**
• **EZproxy Top Denied Clients Today**

![Graph showing the top denied clients today.](image)

Figure 37

• **EZproxy Top Allowed Clients Today**

![Graph showing the top allowed clients today.](image)

Figure 38
### EZproxy - Allowed Traffic Details

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device Name</th>
<th>Client Address</th>
<th>Bytes Transferred</th>
<th>Request Type</th>
<th>Requested URL</th>
<th>User Agent Type</th>
<th>User Agent Details</th>
<th>Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 Nov 2015:18:07:30</td>
<td>server8</td>
<td>172.31.181.205</td>
<td>503</td>
<td>GET</td>
<td>/</td>
<td>Mozilla/5.0</td>
<td>Macintosh; Intel Mac OS X 10.10_3</td>
<td>302</td>
</tr>
<tr>
<td>19 Nov 2015:18:11:59</td>
<td>server8</td>
<td>10.201.5.34</td>
<td>599</td>
<td>GET</td>
<td>images/footer.png</td>
<td>Mozilla/5.0</td>
<td>Windows NT 6.1; WOW64</td>
<td>404</td>
</tr>
<tr>
<td>18 Nov 2015:18:06:25</td>
<td>server8</td>
<td>172.31.181.205</td>
<td>503</td>
<td>HEAD</td>
<td>/</td>
<td>Mozilla/5.0</td>
<td>Macintosh; Intel Mac OS X 10.10_3</td>
<td>302</td>
</tr>
<tr>
<td>19 Nov 2015:18:12:47</td>
<td>server8</td>
<td>10.201.5.34</td>
<td>599</td>
<td>GET</td>
<td>images/footer.png</td>
<td>Mozilla/5.0</td>
<td>Windows NT 6.1; WOW64</td>
<td>404</td>
</tr>
<tr>
<td>18 Nov 2015:18:17:50</td>
<td>server8</td>
<td>172.31.181.205</td>
<td>503</td>
<td>GET</td>
<td>/</td>
<td>Mozilla/5.0</td>
<td>Macintosh; Intel Mac OS X 10.10_3</td>
<td>302</td>
</tr>
</tbody>
</table>

Figure 39

### EZproxy - Denied Traffic Details

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device Name</th>
<th>Client Address</th>
<th>Error Type</th>
<th>Error Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Nov 18 17:21:18 2016</td>
<td>server8</td>
<td>5.0.83.211</td>
<td>PHP Strict Standards</td>
<td>mktime(): int function mktime() not found; it is not safe to rely on the system's timezone settings; Please use the date.timezone setting, the TZ environment variable or the date_default_timezone_set() function. In case you used any of those methods and you are still getting this warning, you must likely misspelled the timezone identifier. We selected &quot;America/Chicago&quot; for &quot;CST-6/6:00 DST&quot; instead of /var/www/html/beck/includes/systemFunctions.inc on line 528</td>
</tr>
<tr>
<td>Wed Nov 18 18:01:09 2015</td>
<td>server8</td>
<td>10.0.60.231</td>
<td>PHP Warning</td>
<td>mysql_close(): supplied argument is not a valid MySQL-Link resource in /var/www/html/beck/includes/systemFunctions.inc on line 975</td>
</tr>
</tbody>
</table>

Figure 40
**EZproxy-User Logon Details**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Logon Status</th>
<th>User Name</th>
<th>Source Address</th>
<th>Logon Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-25-11 03:00:25</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>fried</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:36:55</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>hineo</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:22:55</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>jzhu3</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:21:55</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>antwiggins</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:20:55</td>
<td>HUEY-DLA</td>
<td>Login Failure</td>
<td>mepugh</td>
<td>14.21.25.03</td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:18:55</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>Ancruz</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:18:00</td>
<td>HUEY-DLA</td>
<td>Login Success</td>
<td>innogee</td>
<td>98.226.171.49</td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:14:25</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>klawson2</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:13:27</td>
<td>HUEY-DLA</td>
<td>Login Success</td>
<td>annat</td>
<td>99.71.120.05</td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:12:12</td>
<td>HUEY-DLA</td>
<td>Login Success</td>
<td>geikibishop</td>
<td>162.238.159.108</td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:11:25</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>swetty</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:10:55</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>jpark2</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:10:03</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>sillevell</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:09:30</td>
<td>HUEY-DLA</td>
<td>Login Success</td>
<td>entoobman</td>
<td>50.178.206.178</td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:09:25</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>kichappelow</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:09:25</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>godewitt</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:00:25</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>miller</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:00:25</td>
<td>HUEY-DLA</td>
<td>Logout</td>
<td>aojogar</td>
<td></td>
<td>Expired</td>
</tr>
<tr>
<td>2015-25-11 03:00:53</td>
<td>HUEY-DLA</td>
<td>Login Success</td>
<td>johnson</td>
<td>98.223.274.70</td>
<td>Expired</td>
</tr>
</tbody>
</table>

**EZproxy - User Logon Details**

**Figure 41**

**EZproxy-Intrusion Details**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Attack Type</th>
<th>User Name</th>
<th>Source Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-25-11 16:35:15</td>
<td>HUEY-DLA</td>
<td>Login Intruder User</td>
<td>antwiggins</td>
<td>162.238.159.108</td>
</tr>
</tbody>
</table>

**Figure 42**