Integrate Apache Web Server
Abstract

This guide helps you in configuring Apache Web Server and EventTracker to receive Apache Web server events. The detailed procedures required for monitoring Apache Web server is explained in the guide.

Scope

The configurations detailed in this guide are consistent with EventTracker version 8.x and Apache Web Server 2.4.43 or later.

Audience

Administrators who are assigned the task to monitor and manage Apache Web Server events using EventTracker.

The information contained in this document represents the current view of EventTracker on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker makes no warranties, express or implied, as to the information in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract ................................................................................................................................................. 1
Overview.................................................................................................................................................. 3
Apache Integration with Cent OS ........................................................................................................... 3
Prerequisites ........................................................................................................................................... 3
Configure rsyslog to send Syslog events to EventTracker server ....................................................... 3
Apache Integration with Windows .......................................................................................................... 5
Prerequisites ........................................................................................................................................... 5
Configure XAMPP to send events to EventTracker server .................................................................. 5
Configure log file monitor (LFM) for monitoring Apache Web Server ............................................. 7
Filter Configuration for LFM ................................................................................................................. 11
EventTracker Knowledge Pack ............................................................................................................. 13
  Categories ............................................................................................................................................ 13
  Alerts ................................................................................................................................................... 14
  Flex Reports ....................................................................................................................................... 15
Import Apache Web Server knowledge pack into EventTracker ...................................................... 21
  Category ............................................................................................................................................ 22
  Alerts .................................................................................................................................................. 23
  Templates ........................................................................................................................................... 24
  Flex Reports ....................................................................................................................................... 26
Verify Apache Web Server knowledge pack in EventTracker .......................................................... 27
  Category ............................................................................................................................................ 27
  Alerts .................................................................................................................................................. 28
  Template .......................................................................................................................................... 29
  Flex Reports ....................................................................................................................................... 29
Create Flex Dashboards in EventTracker ............................................................................................. 30
  Schedule Reports ............................................................................................................................... 30
  Create Dashlets ................................................................................................................................ 33
  Sample Flex Dashboards .................................................................................................................. 36
Overview

The Apache HTTP server is a software (or program) that runs in the background under an appropriate operating system, which supports multi-tasking, and provides services to other applications that connect to it, such as client web browsers. Its power rather comes from added functionality introduced through many modules that are written by programmers and can be installed to extend the server’s capabilities.

Apache Integration with Cent OS

Prerequisites

- EventTracker v8.x should be installed.
- Apache Web Server 2.4.43 or later should be installed.
- To check Apache Server Version:
  Run ‘httpd –v’ command in terminal window. You will get an output similar to the below:

  [root@demo ~]# httpd -v
  “Server version: Apache/2.4.43 (UNIX)”

Configure rsyslog to send Syslog events to EventTracker server

1. Login to the Linux Redhat/CentOS machine as root.
2. Open Terminal window.
3. Access Apache Configuration files to obtain and change the log format.
4. Open /etc/httpd/conf.d/httpd.conf

   [root@localhost ~]# vi /etc/httpd/conf.d/httpd.conf cls_

5. The default log format will be as shown in the below image.
Integrate Apache Web Server

6. But in order to generate the desired logs we need to customize the Log format and replace the existing logs as shown below:

```xml
<IfModule log_config_module>

# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#

<IfModule logio_module>

# You need to enable mod_logio.c to use %I and %O
LogFormat "%h %I %u %t "%r" %>s "%{Referer}i" "%{User-Agent}i"

CustomLog logs/httpd/access.log combined
CustomLog "!/usr/bin/logger -t httpd -i -p local4.info" combined
</IfModule>
</IfModule>
```

7. Once the log format is changed and saved, you will get the logs generated as shown below in the sample log.

```
Dec 15 05:40:21 PNPL-6-KP Dec 15 05:40:21 localhost httpd[8161]: 192.168.137.236
172.30.1.54 - - [15/Dec/2016:14:10:02 -0500] "GET /wp-content/plugins/simple-html-slider/css/shs-front.css?ver=3.7.1 HTTP/1.1" 404 4144 "http://172.30.5.64/knowledge-center/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.28 Safari/537.36"
```

8. Open `rsyslog.conf` in VI Editor.
   ```
   vi /etc/rsyslog.conf
   ```

9. For enabling syslog for apache put the below configuration in `rsyslog.conf`
   ```
   local4.* /var/log/httpd/access.log
   local3.* /var/log/httpd/error.log
   ```
10. Add `local3` and `local4` in below mentioned section of `rsyslog.conf`

```
/var/log/messages
```

11. Add the below mentioned line in file `rsyslog.conf` at last.

```
**@IP address of EventTracker Enterprise machine:514
Example:** @10.10.10.167:514
```

**NOTE:** Use ‘@@’ for TCP and ‘@’ for UDP to forward log to Remote host. It would forward the syslog messages to EventTracker Enterprise machine.

12. Restart the syslog service.

```
Service rsyslog restart
```

### Apache Integration with Windows

#### Prerequisites

- EventTracker v8.x should be installed.
- Apache Web Server 2.4.43 or later should be installed.
- Windows Version 7 or later should be installed.
- Xampp version 3.2.2 or higher
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

#### Configure XAMPP to send events to EventTracker server.

1. Access the XAMPP control panel.
2. Click on “Config” and select Apache (httpd.conf) file to get the Apache configuration details.

![Image of XAMPP Control Panel](image)

**Figure 2**

3. The .conf file contains the basic Log format which is as shown below:

```plaintext
<IfModule log_config_module>
    # The following directives define some format nicknames for use with 
    # a CustomLog directive (see below).
    
    LogFormat "%h %l %u %t "%r" %>s %b "%{Referer}i" "%{User-Agent}i" "combined"
    LogFormat "%h %l %u %t "%r" %>s %b "%{Referer}i" "%{User-Agent}i" "common"
</IfModule>
```

**Figure 3**

4. But in order to generate the desired logs we need to customize the Log format and replace the existing logs as below:
5. Save the `.conf` file.
6. Once the log format is changed and saved, you will get the logs generated as shown below in the sample log. Logs can be found in the location “`\xampp\apache\logs`”

```
::1 - - [06/Jan/2017:10:22:56 +0530] "GET /dashboard/jobid=-5%20union%20select%2012345678987654321,2,3,4,5,6,concat(admin,0x23,email,0x5D,loginname,0x7E,pass),8,9,0,1,2,3,4,5,6,7,8,9,0%20from%20users-- HTTP/1.1" "C:/xampp/apache/error/HTTP_NOT_FOUND.html.var" 404 1054 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36"
```

Configure log file monitor (LFM) for monitoring Apache Web Server

To perform LFM configuration, deploy the EventTracker agent on Apache Web Server machine. For this, please refer [EventTracker Agent installation guide](#). After installation of the ET agent, check the steps to configure LFM.

1. Go to the `\Program Files (x86)\Prism Microsystems\EventTracker\Agent` and double click on “Etaconfig” file as shown below:
2. Click the button **Logfile Monitor** and then click the button **Add File Name** and select the **Filename** from where the logs need to be parsed. Also select the checkbox **Logfile Monitor** as shown above in the figure.

3. Select **Get All Existing Log Files** option as shown above.
4. In **Select Log File Type** drop down, select the **Textline** option.
5. Select the folder “:\xampp\apache\logs”
6. Choose the log files that need to be parsed and click on **OK**.

![Select Folder/File Name](image)

**Figure 8**

7. Click on **Add String**.

![Search String](image)

**Figure 9**

8. In the field **Enter Search String**, enter Asterisk(*) symbol. Select the checkbox **Current DateTime**. Click on **OK**.
9. Click On “Save”.

Figure 10

Figure 11
10. Logs will now be sent to the EventTracker Enterprise.
11. You can also add multiple file names such as `error.log`, `audit.log` from which the log needs to be parsed by following the above steps.

**Filter Configuration for LFM**

1. Filter is Set in order to generate Online events.
2. Set the Filters by clicking on “**Event Filters**” to obtain only the desired event id logs that are needed.

![EventTracker Agent Configuration](image-url)
3. Click on the **Filter Exception** to add a New exception for a particular Event ID.

![Filter Exception window](image13)

**Figure 13**

4. Fill in the fields as shown below to set a Filter exception.

![Event Details window](image14)

**Figure 14**

5. Click on **OK** and **Save**.
EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories, reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Linux as well as Windows.

Categories

- **Bad Client Request**: This category provides information regarding the HTTP ‘Error 400: Bad Request’ which typically occurs when a web server receives a request that is unable to understand.
- **Bad Gateway**: This category provides information regarding the Gateway error which means that one server on the internet received an invalid response from another server.
- **Client Request Method Not Allowed**: This category provides information regarding the method specified in the Request-Line which is not allowed for the resource identified by the request-uri.
- **Client Request timed Out**: This category provides information regarding the client unable to produce a request within the time that the server was prepared to wait.
- **Gateway Timeout**: This category provides information regarding one server that did not receive a timely response from another server.
- **Http Request Forbidden**: This category provides information if server understood the request, but is refusing to fulfill it.
- **Http version Not Supported**: This category provides information regarding server that does not support, or refuses to support, the HTTP protocol version that is being used.
- **Internal Server Error**: This category provides information regarding the server that encountered an unexpected condition which prevented it from fulfilling the request.
- **Page Request Success**: This category provides information regarding the server which returned with the valid data that was requested for.
- **Pre-condition failed**: This category provides information regarding the precondition that fails when it is tested on the server.
- **Proxy Authentication required**: This category provides information that the client must first authenticate itself with the proxy.
- **Request Entity too Large**: This category provides information regarding the server that is refusing to process a request because the entity is too large.
- **Request Expectation Failed**: This category provides information regarding the expectation given that could not be met by the server.
- **Request URI too long**: This category provides information regarding the server that is refusing to service the request because the uri is longer than the server that is willing to interpret.
• **Resources Created**: This category provides information regarding the request that has been fulfilled and resulted in a new resource being created.

• **Resources Down Permanently**: This category provides information regarding the resources or data that cannot be fetched as the server no longer contains the requested resource.

• **Resources not found**: This category provides information regarding the server that has not found anything matching the request uri.

• **Unauthorized Client Request**: This category provides information regarding the request that requires user authentication.

• **Unspecified Content length**: This category provides information regarding the resource which has content characteristics, which are not acceptable.

• **Unsupported Media type**: This category provides information regarding the server that is refusing to service the request because the entity of the request is in a not supported format.

**Alerts**

• **Apache-Access Denied** - This alert is generated when user logon is failed (e.g. http 401,403)

• **Apache-Request Forbidden** - This alert is generated when access is not allowed to the server due to several authentication criteria.

• **Apache-Resource Moved Permanently** - This alert is generated when resources or data stored is moved or removed from the database.
Flex Reports

- **Apache-Auth Finder**: This report provides the information about an attacker trying to search for the Authentication pages.

![Figure 15](image1)

**Logs Considered:**

![Figure 16](image2)

- **Apache-Directory Traversal**: This report provides information of ways in which an HTTP exploit takes place which allows attackers to access restricted directories and execute commands outside of the web server’s root directory.
**Logs Considered:**

- **Apache-Sql Injection:** This report provides information about the attackers who are trying to do sql injection on apache web server. It also provides information about the uri on which attacker is trying to execute suspicious sql queries which we can correlate with sql syntax error to confirm whether it is a possible sql injection or not.
Log Considered:

- **Apache-URI error**: This report provides information related to users using incorrect URI to access the server which is not recognized or rejected by Apache.

![Figure 20](image)

![Figure 21](image)

Log Considered:

![Figure 22](image)
- **Apache-Page Views**: This report provides us the information about the browser pages accessed by the user.

![Figure 23](image1)

**Logs Considered:**

![Figure 24](image2)

- **Apache Traffic Details**: This report provides the Web traffic details of the user traversal when accessing an Apache web page

![Figure 25](image3)
Integrate Apache Web Server

Logs Considered:

Figure 26

- **Apache-Backup Finder:** This report shows the attempts to identify backup copies of discovered files. It does so by requesting a number of different combinations of the filename (e.g., index.bak, index.html~, copy of index.html).

Figure 27

Logs Considered:

Figure 28
- **Apache-Client access errors**: This report provides information regarding the various errors on the server when any request is given by the client.

  ![Figure 29](image-url)

  **Logs Considered:**

  ![Figure 30](image-url)

- **Apache-Server Errors**: This report provides the different Server side and database errors when trying to access the Apache Server.

  ![Figure 31](image-url)
Integrate Apache Web Server

Logs Considered:

![Log Table](image)

Figure 32

Import Apache Web Server knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Templates
- Knowledge Objects
- Flex Reports

**NOTE:** Export knowledge pack items in the following sequence:

- Categories
- Alerts
- Templates
- Knowledge Objects
- Flex Reports

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility.
3. Click the **Import** tab.

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate the **All Apache Web Server group of categories.iscat** file, and then click **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

![Figure 35](image)

4. Click the **OK**, and then click the **Close** button.

**Alerts**

1. Click **Alerts** option, and then click the browse button.
2. Locate the **All Apache Web Server group of alerts.isalt** file, and then click the **Open** button.

![Figure 36](image)

2. To import alerts, click the **Import** button. EventTracker displays success message.
3. Click **OK**, and then click the **Close** button.

**Templates**

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

3. Click on **Browse** button.
Integrate Apache Web Server

4. Locate All Apache Web Server group of Template.ettd file, and then click the Open button.

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

6. Click on OK button.
Flex Reports

1. Click **Reports** option, and then click the browse button.
2. Locate the **All Apache Web Server group of flex reports.issch** file, and then click the **Open** button.

Figure 42

3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

Figure 43
Verify Apache Web Server knowledge pack in EventTracker Category

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Categories.

   In the Category Tree, expand Apache Web Server group folder to see the imported categories.

![Category Management](image)

Figure 44
Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In the Search field, type 'Apache Web Server', and then click Go button.
3. Alert Management page will display the imported Apache Web Server alert.

![Alert Management Page](image)

Figure 45

4. To activate the imported alerts, select the respective checkbox in the Active column. EventTracker displays message box.

![Message Box](image)

Figure 46

5. Click the OK button, and then click the Activate now button.

**NOTE:**
You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the Activate Now button.
Template

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.

Figure 47

Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.
2. In Reports Configuration pane, select Defined option.
3. In search box enter ‘Apache Web Server’, and then click the Search button.
   EventTracker displays Flex reports of ‘Apache Web Server’.
Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open EventTracker in browser and logon.
2. Navigate to Reports>Configuration.


![Figure 50](image)

4. Click on ‘schedule’ to plan a report for later execution.
5. Click Next button to proceed.
6. In review page, check Persist data in EventVault Explorer option.
7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.
Create Dashlets

1. Open EventTracker Enterprise in browser and logon.

2. Navigate to Dashboard>Flex.
   Flex Dashboard pane is shown.

3. Fill suitable title and description and click Save button.
4. Click to configure a new flex dashlet. Widget configuration pane is shown.
5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.

15. Click ‘customize’ to locate and choose created dashlet.
16. Click + to add dashlet to earlier created dashboard.
Sample Flex Dashboards

For below dashboard DATA SOURCE: Apache- Apache-Client access errors

1. Apache Web Server - Apache Client access error
   WIDGET TITLE: Apache Web Server - Apache Client side error
   CHART TYPE: Donut
   AXIS LABELS [X-AXIS]: Client IP and Port of Request

   ![Figure 58](image)

   For below dashboard DATA SOURCE: Apache- Apache-Backup Finder

2. Apache Web Server – Apache Backup Finder
   WIDGET TITLE: Apache Web Server – Apache BackupFinder
   CHART TYPE: Donut
   AXIS LABELS [X-AXIS]: Client IP Address

   ![Figure 59](image)
For below dashboard **DATA SOURCE: Apache- Apache-Auth Finder**

3. **Apache Web Server - Apache Auth Finder**
   **WIDGET TITLE:** Apache Web Server – Apache Auth Finder
   **CHART TYPE:** Stacked Column
   **AXIS LABELS [X-AXIS]:** Client IP Address

![Figure 60](image)

For below dashboard **DATA SOURCE: Apache- Apache-Directory Traversal**

4. **Apache Web Server – Apache-Directory Traversal**
   **WIDGET TITLE:** Apache Web Server – Apache Directory Traversal
   **CHART TYPE:** Donut
   **AXIS LABELS [X-AXIS]:** URI Stem

![Figure 61](image)
For below dashboard **DATA SOURCE: Apache- Apache-Page Views**

5. **Apache Web Server - Apache Page Views**  
**WIDGET TITLE:** Apache Web Server – Apache Page Views  
**CHART TYPE:** Stacked Column  
**AXIS LABELS [X-AXIS]:** Client IP Address

![Figure 62](image)

For below dashboard **DATA SOURCE: Apache- Apache-Sql Injections**

6. **Apache Web Server - Apache Sql Injection**  
**WIDGET TITLE:** Apache Web Server – Apache Sql Injection  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Client IP Address

![Figure 63](image)
For below dashboard **DATA SOURCE:** Apache- Apache-Traffic Details

7. **Apache Web Server - Apache Traffic Details**  
**WIDGET TITLE:** Apache Web Server – Traffic Details  
**CHART TYPE:** Line  
**AXIS LABELS [X-AXIS]:** Client IP Address

![Figure 64](image)

For below dashboard **DATA SOURCE:** Apache- Apache-Uri Error

8. **Apache Web Server - Apache URI Error**  
**WIDGET TITLE:** Apache Web Server – URI error  
**CHART TYPE:** Line  
**AXIS LABELS [X-AXIS]:** URI Stem

![Figure 65](image)
For below dashboard **DATA SOURCE: Apache- Apache-Server Error**

9. **Apache Web Server – Apache Server Error**

**WIDGET TITLE:** Apache Web Server – Apache Server Error

**CHART TYPE:** Donut

**AXIS LABELS [X-AXIS]:** Error String

![Apache Server Error Chart](image-url)