Integrate F5 BIG-IP

EventTracker v9.x and later

Publication Date: May 14, 2019
Abstract

This guide provides instructions to configure F5 BIG-IP to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and F5 BIG-IP (Firmware version 9.x to 14.x).

Audience

F5 BIG-IP users, who wish to forward syslog events to EventTracker manager.
# Table of Contents

Abstract ........................................................................................................................................... 1
Scope .................................................................................................................................................. 1
Audience ............................................................................................................................................... 1
Overview ........................................................................................................................................... 3
Pre-requisite ....................................................................................................................................... 3
Configure F5 BIG-IP to forward logs to EventTracker ................................................................. 3
  For Version 9.4.5-9.4.8 ..................................................................................................................... 3
  For Version 10.0.0-10.2.4 ................................................................................................................... 3
  For Version 11.x to V14.x .................................................................................................................. 4
EventTracker Knowledge Pack ......................................................................................................... 4
  Reports ............................................................................................................................................. 4
  Alerts ............................................................................................................................................... 8
  Dashboards ..................................................................................................................................... 9
Import F5 BIG-IP knowledge pack into EventTracker ................................................................. 12
  Categories ...................................................................................................................................... 13
  Alerts .............................................................................................................................................. 13
  Token Template ............................................................................................................................... 14
  Knowledge Object .......................................................................................................................... 16
  Flex Reports .................................................................................................................................. 17
  Dashboard ...................................................................................................................................... 18
Verify F5 BIG-IP knowledge pack in EventTracker ................................................................. 20
  Categories ...................................................................................................................................... 20
  Alerts .............................................................................................................................................. 21
  Token Template ............................................................................................................................... 22
  Knowledge Objects .......................................................................................................................... 22
  Flex Reports .................................................................................................................................. 23
  Dashboard ...................................................................................................................................... 24
Overview

F5 BIG-IP turns your network into an agile infrastructure for application delivery. It’s a full proxy between users and application servers, creating a layer of abstraction to secure, optimize, and load balance application traffic. This gives you the control to add servers easily, eliminate downtime, improve application performance, and meet your security requirements.

EventTracker supports F5 BIG-IP 1600 series and above, it forwards the syslog-ng messages to EventTracker manager. EventTracker generates the alert and report for critical events.

Pre-requisite

- EventTracker v9.x or above should be installed.
- You must have a console with root access to the F5 BIG-IP system.

Configure F5 BIG-IP to forward logs to EventTracker

The mechanism that the F5 BIG-IP uses to log events remotely is the Linux utility syslog-ng which is enabled by default.

For Version 9.4.5-9.4.8

1. Use an SSH client to access the F5 Big-IP device.
2. Type root and press enter.
3. Enter the F5 Big-IP password.
4. Type bpsh, and press enter.
5. To configure the remote syslog server, type the following command:
   `bigpipe syslog remote server <IP_address>`
   For example: `bigpipe syslog remote server 10.1.1.1`
6. To save the configuration, type the following command:
   `bigpipe save`
7. Type exit and press enter.

For Version 10.0.0-10.2.4

1. Use an SSH client to access the F5 Big-IP device.
2. Type root and press enter.
3. Enter the F5 Big-IP password.
4. Type bpsh, and press enter.
5. To add a single remote syslog server, use the following command syntax:

6. `bigpipe syslog remote server {<name> {host <IP_address>}}`

7. For example, `bigpipe syslog remote server {server1.net {host 10.1.1.1}}`

8. To save the configuration, type the following command:

9. In versions **10.0.0** through **10.2.1**: `bigpipe save`

10. In versions **10.2.2** and later: `bigpipe save all`

11. Type `exit` and press enter.

For Version 11.x to V14.x

1. Use an SSH client to access the F5 Big-IP device.
2. Type `root` and press enter.
3. Enter the F5 Big-IP password.
4. Log in to the Traffic Management Shell (tmsh) by typing the following command:
   `tmsh`
5. To add a single remote syslog server, use the following command syntax:
   `modify /sys syslog remote-servers add { <name> { host <IP address> remote-port <port> } }`
   For example, to add EventTracker server 172.28.31.40 with port 514 and name ETLog, type the following command:
   `modify /sys syslog remote-servers add { ETLog { host 172.28.31.40 remote-port 514 } }

6. To save the configuration, type the following command:
   `save /sys config`

7. Type `quit`, and press enter.

EventTracker Knowledge Pack

Once F5 BIG-IP events are enabled and F5 BIG-IP events are received in EventTracker, Alerts, and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support F5 BIG-IP monitoring.

Reports

- **F5 BIG-IP Login and Logout Activity**: This report provides information related to user logon and logout which includes User Name, Host Address, Logon Attempts, Session Start Time and Session End Time fields.
Sample Logs:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>EventSource</th>
<th>Userip</th>
<th>Login attempts</th>
<th>Username</th>
<th>Login Time</th>
<th>Logout Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2019 03:48:51 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>SYSLOG auth</td>
<td>10.140.50.15</td>
<td>1</td>
<td>admin(admin)</td>
<td>Thu Apr 25 15:53:54 2019</td>
<td></td>
</tr>
<tr>
<td>05/02/2019 03:48:51 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>SYSLOG auth</td>
<td>10.140.50.15</td>
<td>1</td>
<td>admin(admin)</td>
<td>Thu Apr 25 15:53:50 2019</td>
<td></td>
</tr>
<tr>
<td>05/02/2019 03:48:52 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>SYSLOG auth</td>
<td>10.140.50.15</td>
<td>1</td>
<td>admin(admin)</td>
<td>Thu Apr 25 15:53:41 2019</td>
<td></td>
</tr>
<tr>
<td>05/02/2019 11:29:32 AM</td>
<td>WIN-F5-BIG-IP</td>
<td>SYSLOG authpriv</td>
<td>10.140.50.15</td>
<td>1</td>
<td>admin(admin)</td>
<td>Thu Apr 25 15:53:16 2019</td>
<td></td>
</tr>
<tr>
<td>05/02/2019 11:29:32 AM</td>
<td>WIN-F5-BIG-IP</td>
<td>SYSLOG authpriv</td>
<td>10.140.50.15</td>
<td>1</td>
<td>admin(admin)</td>
<td>Thu Apr 25 15:52:44 2019</td>
<td></td>
</tr>
<tr>
<td>05/02/2019 11:29:32 AM</td>
<td>WIN-F5-BIG-IP</td>
<td>SYSLOG authpriv</td>
<td>10.140.50.15</td>
<td>1</td>
<td>admin(admin)</td>
<td>Thu Apr 25 15:53:13 2019</td>
<td></td>
</tr>
</tbody>
</table>

**F5 BIG-IP Login Failed Activity:** This report provides information related to user logon failure which includes User Name, Host Address, Logon Attempts, Session Start Time and Session End Time fields.
Sample Logs:

- **F5 BIG-IP Global Traffic Management Activity**: This report provides information related to global traffic management.
Sample Logs:

**F5 BIG-IP Local Traffic Management Activity:** This report will generate a detailed view of local traffic management logs.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Process</th>
<th>Process ID</th>
<th>Source User</th>
<th>File Path</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/03/2019 03:16:43 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>tmsh[10142]:01420002:5</td>
<td>10142</td>
<td>root</td>
<td>/Common</td>
<td>Command OK</td>
</tr>
<tr>
<td>05/03/2019 03:16:45 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>tmsh[9444]:01420002:5</td>
<td>9444</td>
<td>root</td>
<td>/Common</td>
<td>Command OK</td>
</tr>
<tr>
<td>05/03/2019 03:16:51 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>tmsh[8811]:01420002:5</td>
<td>8811</td>
<td>root</td>
<td>/Common</td>
<td>Command OK</td>
</tr>
<tr>
<td>05/03/2019 03:16:59 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>tmsh[8117]:01420002:5</td>
<td>8117</td>
<td>root</td>
<td>/Common</td>
<td>Command OK</td>
</tr>
<tr>
<td>05/03/2019 03:17:05 PM</td>
<td>WIN-F5-BIG-IP</td>
<td>tmsh[7477]:01420002:5</td>
<td>7477</td>
<td>root</td>
<td>/Common</td>
<td>Command OK</td>
</tr>
</tbody>
</table>

Sample Logs:
- **F5 BIG-IP SSL Activity**: This report will generate a detailed view on all the SSL related activities as seen on F5 BIG-IP.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Log Info</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/04/2019 04:24:06 PM</td>
<td>VN-F5-BIG-IP</td>
<td>Connection error</td>
<td>10.151.100.100</td>
<td>993</td>
<td>208.100.26.235</td>
<td>42868</td>
</tr>
<tr>
<td>05/04/2019 04:24:06 PM</td>
<td>VN-F5-BIG-IP</td>
<td>No shared ciphers between SSL peers</td>
<td>10.151.100.100</td>
<td>993</td>
<td>208.100.26.235</td>
<td>42750</td>
</tr>
<tr>
<td>05/04/2019 04:24:06 PM</td>
<td>VN-F5-BIG-IP</td>
<td>SSL Handshake failed for TCP</td>
<td>10.151.100.100</td>
<td>993</td>
<td>208.100.26.235</td>
<td>42868</td>
</tr>
<tr>
<td>05/04/2019 04:24:06 PM</td>
<td>VN-F5-BIG-IP</td>
<td>Connection error</td>
<td>10.151.100.100</td>
<td>993</td>
<td>208.100.26.235</td>
<td>42868</td>
</tr>
</tbody>
</table>

**Figure 9**

**Sample Logs:**

```plaintext
event_computer       ● WIN-F5-BIG-IP
event_datetime       ● 5/4/2019 4:40:22 PM
event_datetime_use   ● 1556668222
event_id             ● 3230
event_log_type       ● Application
event_source         ● syslog local0
```

**Figure 10**

**Alerts**

- **F5 BIG-IP: ARP entry deleted** - This alert is generated when an ARP entry is deleted.
- **F5 BIG-IP: Authentication failed** - This alert is generated when authentication fails.
- **F5 BIG-IP: Authentication success** - This alert is generated when authentication succeeds.
- **F5 BIG-IP: Connection error** - This alert is generated when a connection has an error.
- **F5 BIG-IP: Monitor removed** - This alert is generated when a monitor is removed from local traffic management.
- **F5 BIG-IP: Packet filtering disabled** - This alert is generated when packet filtering is disabled.
- **F5 BIG-IP: Packet filtering rule modified** - This alert is generated when the packet filtering rule is modified.
- **F5 BIG-IP: Pool member status down** - BIG-IP: Pool member status down.
- **F5 BIG-IP: Root login failure** - This alert is generated when the root has authentication failure.
- **F5 BIG-IP: User account deleted** - This alert is generated when the user account is deleted.
Dashboards

- **F5 BIG-IP: Login failed - By city**

![Figure 11](image1.png)

- **F5 BIG-IP: Login and Logout - By source IP**

![Figure 12](image2.png)
• F5 BIG-IP: Global Traffic Management

![F5 BIG-IP: Global Traffic Management](image1.png)

**Figure 13**

• F5 BIG-IP: Login failed - By source IP

![F5 BIG-IP: Login Failed - By Source IP](image2.png)

**Figure 14**
• F5 BIG-IP: Login failed - By user name

Figure 15

• F5 BIG-IP: Login and Logout - By user name

Figure 16
Import F5 BIG-IP knowledge pack into EventTracker

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

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

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

![Figure 17](image17.png)

![Figure 18](image18.png)
3. Click the **Import** tab.

**Categories**

1. Click the **Category** option, and then click the browse button.

![Figure 19](image)

2. Navigate to the location having a file with the extension “.iscat” and then click “Import” button.
3. EventTracker displays a success message:

![Figure 20](image)

**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” button.

Token Template

1. Click Parsing Rules under the Admin option in the EventTracker manager page.

2. Next, click the “Template” tab and then click the “Import Configuration” button.
3. Now, click “Browse” button and navigate to the folder where “.ettd” file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click “Import” button:
Knowledge Object

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

![Figure 26](image)

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

![Figure 27](image)

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

![Figure 28](image)

4. A list of available Knowledge objects will appear. Select the relevant files and click the “**Import**” button.
Flex Reports

1. In EventTracker control panel, select “Export/ Import utility” and select the “Import tab”. Then, click Reports option, and choose “New (*.etcrx)”:
2. Once you have selected “New (*.etcrx)”, a new pop-up window will appear. Click “Select File” button and navigate to the file path with a file having extension “.etcrx”.

3. Select all the relevant files and then click Import button.

![Figure 31](image)

![Figure 32](image)

EventTracker displays a success message:

![Figure 33](image)

**Dashboard**

1. Logon to **EventTracker Enterprise**.
2. Navigate to **Dashboard ➔ My Dashboard**.
3. In “My Dashboard”, click **Import Button**:

4. Select the **Browse** button and navigate to file path where dashboard file is saved.

5. Once completed, click “**Upload**” button.

6. Next, select all the relevant dashboards for F5 BIG-IP and click “**Import**” button.
Verify F5 BIG-IP knowledge pack in EventTracker

Categories

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand F5 BIG-IP LTM group folder to view the imported categories:
Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In search box enter F5 BIG-IP and then click the Search button. EventTracker displays alert of F5 BIG-IP.
Token Template

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Template.
2. On the Template tab, click on the F5 BIG-IP LTM group folder to view the imported Token Templates.

Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand F5 BIG-IP LTM group folder to view the imported Knowledge objects.
Flex Reports

1. In the EventTracker Enterprise 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 F5 BIG-IP LTM group folder to view the imported F5 BIG-IP LTM reports.
Dashboard

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

2. In “F5 BIG-IP” dashboard you should be now able to see something like this:
Figure 45