Integrate A10 ADC
Abstract

This guide provides instructions to configure A10 ADC to send the event logs to EventTracker Enterprise. Once events are configured to send to EventTracker Manager, alerts, dashboards and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and A10 Application Delivery Controller AX/Thunder Series with ACOS 4.0 or later.

Audience

A10 ADC users, who wish to forward event logs to EventTracker Manager and monitor events using EventTracker SIEM.
# Table of Contents

Abstract .......................................................................................................................... 1  
Scope ................................................................................................................................. 1  
Audience ........................................................................................................................... 1  
Overview .......................................................................................................................... 4  
Prerequisites ...................................................................................................................... 4  
Enable Syslog forwarding on A10 ADC ........................................................................ 4  
  Configure Syslog Server ............................................................................................... 4  
  Configure ADC Logging .............................................................................................. 5  
  aFlex Script for ADC Logging .................................................................................... 5  
EventTracker Knowledge Pack (KP) ............................................................................... 8  
  Categories ...................................................................................................................... 8  
  Alerts .............................................................................................................................. 8  
  Reports .......................................................................................................................... 8  
  Knowledge Objects ....................................................................................................... 9  
Import Knowledge Pack into EventTracker .................................................................... 9  
  Import Categories ....................................................................................................... 10  
  Import Alerts ............................................................................................................... 11  
  Import Tokens .............................................................................................................. 12  
  Import Flex Reports .................................................................................................... 13  
  Import Token Templates ............................................................................................. 14  
  Import Knowledge Object .......................................................................................... 16  
Verify Knowledge Pack in EventTracker ...................................................................... 18  
  Verify Categories ....................................................................................................... 18  
  Verify Alerts ............................................................................................................... 18  
  Verify Tokens .............................................................................................................. 19  
  Verify Flex Reports .................................................................................................... 20  
  Verify Token Templates ............................................................................................. 21  
  Verify Knowledge Object .......................................................................................... 21
Create Dashboards in EventTracker ................................................................. 23
Schedule Reports ................................................................................................. 23
Create Dashlets ................................................................................................... 25
Sample Reports .................................................................................................... 29
Sample Dashboards ............................................................................................. 30
Overview

A10 Application Delivery Controller provides application availability and reliability by offering advanced server load balancing and flexible health monitoring capabilities. EventTracker examines imperative logs and leverages machine learning to identify application delivery traffic, configuration changes, user behavior and load balance events.

Prerequisites

- EventTracker v7.x and later should be installed.
- A10 Application Delivery Controller AX/Thunder Series running ACOS 4.0 or later should be installed.

Enable Syslog forwarding on A10 ADC

Configure Syslog Server

1. Log into the A10 ADC web UI.
2. Select Config > System > Settings.
3. In the menu bar, select Log.
4. In the Log Server field, enter the IP address of your EventTracker Manager.
5. Ensure that the Log Server Port is set to 514.
6. Leave all other settings at their default values.
7. Click OK.

Figure 1
NOTE: Please add port 514 to firewall exception, if applicable.

Configure ADC Logging

1. Log into the A10 ADC web UI.
2. Navigate to Config Mode > Service > aFleX.
3. Type in aFleX script given below and Save.

![Figure 2](image)

aFleX Script for ADC Logging

To configure application delivery logs use the aFleX Script given below:

```plaintext
when HTTP_REQUEST {
    # Set strings for the "client side"
    set time_client_request [clock seconds]
    set clicks_client_request [clock clicks -milliseconds]
    set date_time_request [clock format $time_client_request -format {%Y-%m-%d %H:%M:%S} ]
    set c_ip [IP::client_addr]
    set cs_uri_stem [HTTP::host][HTTP::uri]
    set cs_method [HTTP::method]
}```
set s_ip [IP::local_addr]
set s_port [TCP::local_port]
set host [HTTP::host]
set vip_ip [IP::local_addr]
set vip_port [TCP::local_port]
if {[HTTP::query] equals ""} {
    set cs_uri_query [HTTP::query]
} else { set cs_uri_query ".-" }
if {[HTTP::header exists Content-Length]} {
    set cs_bytes [HTTP::header Content-Length]
} else { set cs_bytes ".-" }
if {[HTTP::header exists Referer]} {
    set cs_Referer [HTTP::header "Referer"]
} else { set cs_Referer ".-" }
set cs_UserAgent [string map {" " "+"} [HTTP::header "User-Agent"]]
when HTTP_RESPONSE {
    # Set strings for the "server side"
    set clicks_server_response [clock clicks -milliseconds]
    set sc_status [HTTP::status]
    if {[HTTP::header exists Content-Length]} {
        set sc_bytes [HTTP::header Content-Length]
    } else { set sc_bytes ".-" }
}
# Correct TCL Bug with floating point values
set time_taken [expr $clicks_server_response - $clicks_client_request ]
if {$time_taken < 10} {
    set final_time_taken [string range "0.00$time_taken" 0 4]
} elseif { $time_taken < 100 } {
    set final_time_taken [string range "0.0$time_taken" 0 4]
} elseif { $time_taken < 1000} {
    set final_time_taken [string range "0.$time_taken" 0 4]
} else {
    set final_time_taken "[string index $time_taken 0].[string range $time_taken 1 3 ]"
}

# Format strings for logging
set log_str "$date_time_request $c_ip $s_ip $s_port $cs_method $cs_uri_stem $cs_uri_query $vip_ip $vip_port $sc_status $sc_bytes $cs_bytes $final_time_taken $cs_UserAgent $cs_Referer"

# write to syslog with Debug level
log local0.7 $log_str
# write to AX log (turn this for troubleshooting only, as you may have a lot of requests / second)
# log $log_str
}
EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; categories, alerts, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7 and later to support A10 ADC monitoring:

Categories

- **A10 ADC: Configuration Change** - This category based report provides information related to configuration changes using GUI or CLI.
- **A10 ADC: HA Events** - This category based report provides information related to high availability events.
- **A10 ADC: Management Service Status** - This category based report provides information related to change in management service status.
- **A10 ADC: Port Status Change** - This category based report provides information related to change in port or trunk status.
- **A10 ADC: Radius Server Error** - This category based report provides information related to radius server error.
- **A10 ADC: SLB Server Status** - This category based report provides information related to change in load balancing server status.

Alerts

- **A10 ADC: Configuration Change** - This alert is generated when configuration is added, deleted or modified.
- **A10 ADC: User Authentication Failed** - This alert is generated when user authentication fails.

Reports

- **A10 ADC - Application Delivery Traffic Details**: This report provides information related to application servers accessed by various clients with application usage details.
- **A10 ADC - Console Logon Success Details**: This report provides information related to users accessing the ADC console with admin privileges.
- **A10 ADC - User Authentication Failure Details**: This report provides information related to failed user authentication attempts.
Knowledge Objects

- **A10 ADC - Application Delivery Traffic Details:** This KO assists in evaluating application delivery controller traffic.
- **A10 ADC - Console Logon Success Details:** This KO assists in tracking console logon success events.
- **A10 ADC - User Authentication Failure Details:** This KO assists in identifying user authentication failure events.

### Import Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export/Import Utility**, and then click the **Import** tab.
3. Import **Category/Alert/Tokens/Templates/Flex Reports/Knowledge Object** as given below.
Import Categories

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

![Figure 4](image)

2. Locate **All A10 group categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.
   EventTracker displays success message.

![Figure 5](image)

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

1. Click **Alert** option, and then click the ‘**browse**’ button.

![Image of Export Import Utility window with 'browse' button highlighted]

Figure 6

2. Locate **All A10 group alerts.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.

EventTracker displays success message.

![Image of Export Import Utility window with success message]

Figure 7

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

1. Click **Token Value** option, and then click the ‘browse’ button.
2. Locate **All A10 group tokens.istoken** file, and then click the **Open** button.

![Figure 8](image1.png)

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

![Figure 9](image2.png)

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

1. Click **Scheduled Reports** option, and then click the ‘browse’ button.
2. Locate **All A10 group reports.issch** file, and then click the **Open** button.

![Figure 10](image)

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

![Figure 11](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.

![Figure 12](image)

3. Click on **Browse** button.

![Figure 13](image)

4. Locate **A10 token 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.
Import Knowledge Object

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

![Figure 16](image1)

3. In **IMPORT** pane click on **Browse** button.

![Figure 17](image2)

4. Locate **A10 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 Knowledge Pack in EventTracker

Verify Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. To view the imported categories, in the Category Tree, expand A10 group folder.

Verify Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search box, type ‘A10’, and then click the ‘search’ button.
   Alert Management page will display all the imported alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column and then click the **Activate Now** button.

   EventTracker displays message box.

   ![Successfully saved configuration](image)

   **Figure 22**

5. Click **OK**.

**Note:** Please specify appropriate **systems** in **alert configuration** for better performance.

### Verify Tokens

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 **A10** group folder.

   Token values are displayed in the token value 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 Scheduled Reports, scroll down and click A10 group folder.

Scheduled Reports are displayed in the Reports configuration pane.
NOTE: Please specify appropriate systems in report wizard for better performance.

Verify Token Templates

1. Click the Admin menu, and then click Parsing rule.
2. Select Template tab.
3. Scroll and find imported A10 token templates.

Verify Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects
2. Scroll down and select A10 in Objects pane.
   Imported A10 object details are shown.
Figure 26
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

![Configuration page]

2. Navigate to Reports>Configuration.
3. **Select A10** in report groups. Check **defined** dialog box.

4. Click on ‘**schedule**’ icon \( \square \) to plan a report for later execution.

![REPORT WIZARD](image)

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.

   ![Figure 32](image)

4. Click + to add a new dashboard.

   Flex Dashboard configuration pane is shown.

   ![Figure 33](image)

5. Fill fitting title and description and click **Save** button.

6. Click ![icon] to configure a new flex dashlet.

   Widget configuration pane is shown.
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.
16. If satisfied, click **Configure** button.

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

18. Click 📌 to add dashlet to earlier created dashboard.
## Sample Reports

1. **A10 - Application Delivery Traffic Details**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Address</th>
<th>Client Address</th>
<th>Client Server Bytes</th>
<th>Method Used</th>
<th>Server Address</th>
<th>Server Port</th>
<th>Status Code</th>
<th>Time Taken</th>
<th>URI</th>
<th>User Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/26/2015 02:21:34 PM</td>
<td>192.168.25.36</td>
<td>12</td>
<td>POST</td>
<td>10.41.30.4</td>
<td>443</td>
<td>55</td>
<td>200</td>
<td>0.125</td>
<td>Microsoft-Server-Phone5C2M</td>
<td>Apple-Phone5C2M</td>
</tr>
<tr>
<td>08/26/2015 05:41:29 PM</td>
<td>1.127.149.102</td>
<td>22</td>
<td>OPTIONS</td>
<td>10.41.30.45</td>
<td>443</td>
<td>10</td>
<td>200</td>
<td>0.094</td>
<td>Microsoft-Server-Phone5C2M</td>
<td>Microsoft-Server-Phone5C2M</td>
</tr>
<tr>
<td>08/26/2015 00:01:24 PM</td>
<td>122.168.26.36</td>
<td>38</td>
<td>GET</td>
<td>10.41.30.68</td>
<td>443</td>
<td>22</td>
<td>401</td>
<td>0.004</td>
<td>Mozilla/5.0+</td>
<td>Windows+H</td>
</tr>
<tr>
<td>08/27/2015 12:21:18 AM</td>
<td>192.168.25.36</td>
<td>57</td>
<td>POST</td>
<td>10.41.45.66</td>
<td>443</td>
<td>47</td>
<td>200</td>
<td>1.233</td>
<td>Microsoft-Server-Phone6C2M</td>
<td>Apple-Phone6C2M</td>
</tr>
<tr>
<td>08/27/2015 03:41:14 AM</td>
<td>192.168.25.52</td>
<td>42</td>
<td>POST</td>
<td>10.41.30.19</td>
<td>443</td>
<td>68</td>
<td>200</td>
<td>0.140</td>
<td>Microsoft-Server-Phone6C2M</td>
<td>Apple-Phone6C2M</td>
</tr>
<tr>
<td>08/27/2015 07:01:09 AM</td>
<td>200.12.25.36</td>
<td>0</td>
<td>OPTIONS</td>
<td>10.41.30.4</td>
<td>443</td>
<td>0</td>
<td>200</td>
<td>0.523</td>
<td>Microsoft-Server-Phone6C2M</td>
<td>Microsoft-Server-Phone6C2M</td>
</tr>
<tr>
<td>08/27/2015 11:21:04 AM</td>
<td>110.225.163.217</td>
<td>0</td>
<td>GET</td>
<td>10.41.30.68</td>
<td>443</td>
<td>0</td>
<td>401</td>
<td>0.052</td>
<td>Mozilla/5.0+</td>
<td>Windows+H</td>
</tr>
<tr>
<td>08/27/2015 01:40:59 PM</td>
<td>192.168.25.52</td>
<td>25</td>
<td>POST</td>
<td>10.41.45.76</td>
<td>443</td>
<td>47</td>
<td>200</td>
<td>1.233</td>
<td>Microsoft-Server-Phone6C2M</td>
<td>Apple-Phone6C2M</td>
</tr>
</tbody>
</table>

2. **A10 - User Authentication Failure Details**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Address</th>
<th>User Name</th>
<th>User Type</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/26/2015 02:21:34 PM</td>
<td>192.168.2.0</td>
<td>admin</td>
<td>remote</td>
<td>failed in the CLI authentication</td>
</tr>
<tr>
<td>08/26/2015 05:41:29 PM</td>
<td>192.168.2.4</td>
<td>slb-admin</td>
<td>remote</td>
<td>failed in the WEB authentication</td>
</tr>
<tr>
<td>08/26/2015 08:01:24 PM</td>
<td>192.168.1.26</td>
<td>admin</td>
<td>TACACS+</td>
<td>Contact with remote server failed</td>
</tr>
<tr>
<td>08/27/2015 12:21:19 AM</td>
<td>192.168.2.26</td>
<td>slb-admin</td>
<td>Local</td>
<td>Admin password error</td>
</tr>
<tr>
<td>08/27/2015 03:41:14 AM</td>
<td>192.168.1.26</td>
<td>admin</td>
<td>remote</td>
<td>failed in the CLI authentication</td>
</tr>
<tr>
<td>08/27/2015 07:01:09 AM</td>
<td>192.168.2.60</td>
<td>slb-admin</td>
<td>TACACS+</td>
<td>Contact with remote server failed</td>
</tr>
<tr>
<td>08/27/2015 11:21:04 AM</td>
<td>192.168.2.26</td>
<td>admin-3</td>
<td>Local</td>
<td>Admin password error</td>
</tr>
<tr>
<td>08/27/2015 01:40:59 PM</td>
<td>192.168.2.4</td>
<td>slb-admin</td>
<td>remote</td>
<td>failed in the WEB authentication</td>
</tr>
</tbody>
</table>
Sample Dashboards

1. **A10 - Server and Client Data Transfer Details**

   - **A10: Client Data Transferred in Bytes**
   - **A10: Server Data Transferred in Bytes**

2. **A10 - Client Agent Usage Details**

   - **A10: Client Agent Usage**