Abstract

The purpose of this document is to guide the EventTracker users to understand, create correlation rules for v9.x and generate the relevant reports.

Audience

Administrator or technical staffs using EventTracker Correlator.
# Table of Contents

Abstract .................................................................................................................................................. 1

Audience.................................................................................................................................................. 1

Event Correlation..................................................................................................................................... 3
  Role of Event Correlation rules in EventTracker ................................................................................. 3

EventTracker Correlator ......................................................................................................................... 4
  Real time Correlator............................................................................................................................. 4
  On-Demand Correlator......................................................................................................................... 4

Prerequisites........................................................................................................................................... 4

Configure correlation rules in v9.x .......................................................................................................... 5
  To create new correlation rule.............................................................................................................. 5
  Action item to run a script.................................................................................................................... 14
  To edit correlation rule....................................................................................................................... 16
  To delete correlation rule.................................................................................................................... 19

Generate ‘EventTracker Correlation Events’ Report............................................................................. 20
  Configure Reports in v9.x.................................................................................................................... 20

Examples................................................................................................................................................. 22
  For Correlation of two events .............................................................................................................. 22
  To search for a particular substring ................................................................................................... 24
  Add ‘Event properties’ description in the ‘Action event’.................................................................... 25

Steps to enable Group level Event Correlation.................................................................................... 28
  How it works?....................................................................................................................................... 30
Event Correlation

EventTracker™ Correlator is feature add-on package, which runs along with EventTracker™. It compares and matches the pattern of predefined events to identify the correlation conditions. Correlation by definition is a class of statistical relationships between two or more variables or observed data values.

It is the process of analyzing events to identify patterns. This helps pinpoint problems such as abuse, intrusion, attacks, or failure. You can examine the pattern from multiple events from multiple systems.

Role of Event Correlation rules in EventTracker

EventTracker uses correlation rules to keep track of enterprise network behavior and its entities. This helps an organization to determine possible state, and generate appropriate action event. Here the correlation rules relates the incoming events and generates the alert based on the predefined rule details, if ‘EventTracker Real-time Correlator’ is installed.

The rules are governed by business logic and well-defined format which will be deciphered by ‘Correlation engine’. Each correlation rule will be a named rule and each rule must define at least one event and one action event against that event. Events and Action events are in N->N relation provided each rule set adheres to following constraints.

Constraints for Event:

- Each event must have label and must be unique to that correlation rule.
- No events can be repeated within that correlation rule.
- At least one event rule must be defined.
- Time span and occurrence both must be specified.
- Can have back reference to the preceding event as the place holder for data within same rule

Constraints for Event Actions (If EventTracker Real-time Correlator is installed):

- Each action event must have label and must be unique to that correlation rule.
- No action event can be repeated within that correlation rule.
- At least one ‘Action event rule’ must be defined.
- An action event can be constructed by referring to the any of the previous event generated.

NOTE

Correlation can work real-time (online) as well as on-demand (offline). However, action events will only work online, that is only if ‘EventTracker Real Time Correlator’ is installed.
EventTracker Correlator

EventTracker’s correlation engine is divided in two parts, Real time correlator and On-demand correlator.

Real time Correlator

It correlates the received events from the agent and performs the action based on the specified rule. Real time correlator engine processes the event as it comes and generate new event according to the specified behavior pattern. The correlation rule will take place only when the events show the defined pattern of occurrence. A set of predefined alerts are available by default and these alerts can be activated as per requirement.

On-Demand Correlator

The selected correlation rule will be applied while processing the on demand report. The report will be generated based on the properties given in the source event. The action event properties will not be considered while generating the report. If the generated events pass through the correlator rule parser, then the generated report will contain information of all the events occurred within the given life time.

Prerequisites

- EventTracker 9.0 (Build 18) should be installed and customer should have license for Real-time and On Demand feature respectively.
- EventTracker Correlator updates (given below) should be applied to the EventTracker Server or Console.

<table>
<thead>
<tr>
<th>Executable File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker v9.0</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE**

- During upgrade, the user has to reapply the respective feature add on for respective version of EventTracker installed. Later the user has to traverse to Admin Correl and select any existing rule and save it to make sure that custom alerts and reports are retained.
Configure correlation rules in v9.x

By default, EventTracker has activated some correlation rules in the default rule base. Default rule base contains the predefined correlation rules and an option to add new correlation rule.

To create new correlation rule

1. Log on to EventTracker.
2. Click Admin dropdown, and then select Correlation.

EventTracker opens Correlator Rules page.

![Correlator Rules Page](Figure 1)
Left pane displays list of correlation rules available, and right pane displays a page to add new correlation rule or edit selected rule details.

3 In **Correlator Rule Details** pane, enter the rule name in the **Name** field.

Example: `FileTransferF`

**NOTE:**

- This Rule name will be unique across the Correlator Rules.
- The input field should not contain space or special characters.

4 Enter the description for the rule in **Description** field.

Example: Failed to send Syslog DLA file to remote machine.

5 Click **Active** checkbox to activate the rule.

If you do not select the Active checkbox then Correlation rule will only get saved and will not be activated.

6 Click **Save**.

EventTracker displays Correlator event/Action Details pane.

7 Click **Add Event** hyperlink.
EventTracker displays properties pop-up window.

![Event Properties Pop-up Window](image)

**Figure 3**

<table>
<thead>
<tr>
<th>Executable File</th>
<th>Description</th>
</tr>
</thead>
</table>
| Label           | A name given to the Event/Event Action. It is unique across a correlation rule.  
*This is a mandatory field.* |
<table>
<thead>
<tr>
<th><strong>Life Time (Seconds)</strong></th>
<th>Specify the time limit (in seconds) of the event to hold for correlation. *This is a mandatory field.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Occurrence</strong></td>
<td>Enter the number of occurrences of the event to be monitored within specified duration. *This is a mandatory field.</td>
</tr>
<tr>
<td><strong>Log Type</strong></td>
<td>Log type of the event. (1=System, 2=Security, 3=Application)</td>
</tr>
<tr>
<td><strong>Event Type</strong></td>
<td>Event type. (1= Error, 2=Warning, 3=Info, 4=Audit Success, 5=Audit Failure)</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Enter the event category.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Enter the source of events.</td>
</tr>
<tr>
<td><strong>Event ID</strong></td>
<td>Enter the event ID if you wish to collect the event for particular event ID.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>Enter the user name if you wish to monitor the events for particular user.</td>
</tr>
<tr>
<td><strong>Computer</strong></td>
<td>Enter the system name if you wish to collect the events from particular system.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Enter the domain name.</td>
</tr>
</tbody>
</table>
8 Select/enter the appropriate event property details in the **Event Properties** field, and then click **Add**.

9 In **Correlator Event/Action Details** pane, move the pointer over newly created event name.

   EventTracker displays correlator event details in a pop-up window.
10 In Correlator Event/Action Details pane, click Add Action hyperlink. (If ‘EventTracker Real-time Correlator’ is installed)

EventTracker displays Action Properties pop-up window.
Enter appropriate label name in the **Label** field for the event action. This is a mandatory field.
NOTE
Label name in event properties and action properties cannot be same. If you enter the same name, EventTracker displays an error message.

12 Enter/select appropriate details in the ‘Action properties’ pane.

13 Click the ..Previous Reference dropdown to select the same values which you have entered in Event Properties field.

14 In the Description field, describe about the actions on the generated event.
NOTE
In this field, you add the substring from Event Properties description to look for more specific results in order to apply the correlation rule.

15 Click the **Add** button.

16 In **Correlator Event/Action Details** pane, move the pointer over newly created action name.
EventTracker displays correlator action details in a pop-up window.

**CORRELATOR RULE DETAILS**

<table>
<thead>
<tr>
<th>Name</th>
<th>FileTransferF</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Failed to send Syslog DLA file to remote machine</td>
<td></td>
</tr>
</tbody>
</table>

**CORRELATOR EVENT/ACTION DETAILS**

<table>
<thead>
<tr>
<th>Name</th>
<th>FileTransferA</th>
<th>Log Type</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>Warning</td>
<td>Category Id</td>
<td>0</td>
</tr>
<tr>
<td>Source</td>
<td>EventTracker</td>
<td>Event Id</td>
<td>3280</td>
</tr>
<tr>
<td>User</td>
<td>$FileTransferF</td>
<td>Computer</td>
<td>$FileTransferF</td>
</tr>
<tr>
<td>Domain</td>
<td>$FileTransferF</td>
<td>Description</td>
<td>Information event: Failed to send Syslog DLA file to remote machine.</td>
</tr>
</tbody>
</table>

Action item to run a script

1. Select or create a new correlator rule.
   
   Ex: UNIXRootLogin

2. Click **Add Action**.

   ![Figure 9](image)

   Action property window displays.

3. Select **Run Script** option.
Action Properties window displays.

4. Select/Enter the mandatory criteria in **Action Properties** window.

5. In **Parameters** pane, select **Column** or **Static** option.

6. If **Column** drop down is selected, then enter the relevant options and then click **Add Parameter**.

7. Click **Add**.
The existing script generates with relevant parameters.

To edit correlation rule

1. Select an existing rule.

2. Enter the required changes in **Correlation Rule Details**.

3. In **Correlator Event/Action Details** pane, click the existing event, update the required information and then click **Save**.

**NOTE:**

You can also insert an event after or before an existing event property. Move mouse over the event to insert another event.
4. Click existing **Generate Event** in **Action**, update the required information and then click **Save**.

5. To add another action, click **Add Action** hyperlink.
6. Enter the required information and then click **Add**.

You can add multiple numbers of events and actions. Refer Figure 15.
NOTE: If you want to delete an Action or an Event, click the Delete Icon.

To delete correlation rule

1. To delete any rule, select **Delete** icon.
EventTracker displays pop-up message.

2. Click the OK button.

**Generate ‘EventTracker Correlation Events’ Report**

**NOTE:**

For correlator rules to be visible under Reports -> Operations, select any existing rule and save it. EventTracker Correlation Events will be displayed under Reports -> Operations. This is applicable for On-demand correlator only.

**Configure Reports in v9.x**

1. Log on to EventTracker Enterprise. Select Reports, and then select Dashboard or Configuration.

2. Select New icon, and then select Operations tab.

3. In the ‘Reports Tree’, select EventTracker node and expand it.

4. Select EventTracker Correlation Events, select Report Type, and then click the Next button.

![Figure 17](image)
NOTE

You will find EventTracker Correlation Events Report only if you install On Demand Correlator.

(OR)

Right click EventTracker Correlation Events.

EventTracker displays the shortcut menu.

Select On Demand / Queued / Scheduled / Defined option.

EventTracker displays the ‘Reports Wizard’.

3 Click the Next >> button.

4 Select any rule for processing, and then click Next >> button.

Figure 18

You can now proceed further and configure the required correlation rule and the relevant reports will be generated.
Examples

For Correlation of two events

This example will help the user to search for a matched string extracted from two different events used for correlation. In the rule section Pattern field, a string comparison is required. Sample configuration is below.

```
 [[EVENT]
 Label=Event4625
 LifeTime=300
 LogType=2
 EventType=5
 CatId =
 Source =
 ComputerName =
 EventId=4625
 User =
 Domain =
 Description =&<Data Name='TargetUserName'>&&</Data>&
 [End]

 [[EVENT]
 Label=Event4624
 LifeTime=300
 LogType=2
 EventType=4
 CatId =
 Source =
 ComputerName =
 EventId=4624
 User =
 Domain =
```
Description=&lt;Data Name='TargetUserName'&gt;&amp;&lt;/Data&gt;&
[End]

[ACTION]
Label=ActionEvent555
DO=GenerateEvent
LogType=1
EventType=2
CatId=0
Source=EventTracker
ComputerName=
EventId=555
User=
Domain=
Description=This event indicates a successful login after 3 logon failure by an user$Event4625.Description$
Name='TargetUserName'&gt;&amp;&lt;/Data&gt;.
[End]

[RULE]
Label=sucessfulllogin
Description=sucessfulllogin after failure
Pattern=Event4625:3,Event4624:1,$Event4625.Description==$Event4624.Description
Action=ActionEvent555
[End]

**NOTE**

- At present rule condition is supported for EQUAL (==) and NOTEQUAL ( != )
- UI is not available to configure this in Rule section of INI.
To search for a particular substring

This example will help you to search for a specific description in the event properties of resultant events. For this, you need to enter the required description as substring in the ‘**Look for substring**’ option of Event Properties- Description.

```
[EVENT]
Label: Excessive4625
Life Time (Seconds): 300
Occurrences: 10
Log Type:
Event Type:
Category:
Source: System
Event ID: 4625
User:
Computer: MCLOON
Domain: TOONS
Description: Account Locked Out
[End]

[ACTIONS]
Label: Excessive4625A
Log Type: Security
Event Type: Audit Failure
Category:
Source: Intrusion
Event ID: 3258
User: System
Computer: $Excessive4625F
Domain: $Excessive4625F
```
The above rule set says that the events received from EventTracker™ to be monitored for an event that posses the event id 4625 and contains description as ‘Account Locked Out’. If that event occurred 10 (pattern) times in 300 (lifetime) seconds, then the action “Excessive4625A” will be fired which will generate a new event 3258.

The new event will be generated with the specified properties (Log type=security, Event Type=Audit Failure and so on). The Parameter fields ($) in the action properties will be replaced by appropriate values from the actual event.

Add ‘Event properties’ description in the ‘Action event’.

In the presence of event source description:

In some cases, you may need to reproduce some values from source event in the event generated by correlator. Following example will show you how to use the parameter to write ‘Action event’ description using details from Event Properties.
Source: Intrusion
Event ID: 3251
User: SYSTEM
Computer: $IntrEvt1
Domain: $IntrEvt1
Description: Critical alert - Intrusion detected.
An unauthorized and repeated logon request from $IntrEvt1.Description&Client Address: &15.
It may be due to sophisticated hacking attempt. Please investigate and if required block the IP address on the firewall.

The above rule set says that the events received from EventTracker™ to be monitored for an event that poses the event id 676 and contains as Client Address up to 15 characters in description. If that event occurred 5 (pattern) times in 300 (lifetime) seconds, then the action “Intract1” will be fired which will generate a new event 3251.

The new event will be generated with the specified properties (Log type=Security, Event Type=Audit Failure and so on). The Parameter fields ($) in the action properties will be replaced by appropriate values from the actual event.

In simple terms, while defining rule sets, you can make use of the existing event details by its name as the reference. The parameter references can use string substitutions also.

In the absence of event source description:
If the ‘Event properties’ description in Look for substring is left blank, then also the generated action event will display the source event description. Here, the action event will extract the description from an event which has occurred at the last in the given life time. Following example will show you the use of parameter to write an ‘Action Properties’ description.
The above rule set says that the events received from EventTracker™ to be monitored for an event that posses the event id 676. If that event occurred 5 (pattern) times in 300 (lifetime) seconds, then the action “Intract1” will be fired which will generate a new event 3251.

As the source event description is left blank, the description ‘$IntaEvt1.Description’ in action properties will fetch the description from the event which has occurred at the last in the given duration. In this example, the description of 5th event will be displayed in the action event.
Steps to enable Group level Event Correlation

Please apply the Update **ET90U18-038**, before proceeding with the steps.

**NOTE:** Please apply Update **ET90U18-002** on top of Update **ET90U18-038**.

To enable the correlation for group level,

1. Update the key “CorrelGroupBase” in tbl_Config to True or 1 (SQL Database).

2. Navigate to the ...install directory\EventTracker\ETCorrel

3. Next, in the “ETCorrel.ini” use the “@@” character for group consideration in “ComputerName =@@” column of [EVENT] section.

   This is shown below:

```
###########################################
# Prism Microsystems, Inc
# eMail : support@prismmicrosys.com
###########################################

[CORREL]
CacheSize = 50000
EventLifeSecs = 60
Debug = 0
ActionEventDestn = 127.0.0.1

[End]
```
#Rule: Excessive logon failures due to bad password in 2003 domain

[EVENT]
Label = excessive675
LifeTime = 300
LogType = 2
EventType = 5
CatId =
Source =
ComputerName = @@
EventId = 675
User =
Domain =
Severity =
Description =
Comments =
[End]

[ACTION]
Label = excessive675A
DO = GenerateEvent
Destination = 127.0.0.1:14505
LogType = 2
EventType = 5
CatId = 0
Source = Intrusion
ComputerName = $excessive675
EventId = 3253
User = $excessive675
Domain = $excessive675
Severity = 1
Description = Intrusion is detected - Excessive logon failures due to bad password. Number of log failures in your enterprise have crossed the limit. Please generate a report on event id 675 to verify that which system and user is trying responsible for intrusion.
Comments = [End]

[RULE]
Label = excessive675R
Description = Excessive logon failures due to bad password in 2003 domain
Pattern = excessive675:10
Action = excessive675A
[End]

4. After making the changes, restart the “Event Correlator” Service.

How it works?
After applying the update, for event rule where the Computer name is given as @@, it will consider the events based on group level.