Direct Log Archiver Configuration Guide – Version 8.x
Abstract

The purpose of this document is to help users archive log files collected from external sources.

Audience

Users who have enormous number of backlog log files collected from external sources or do not wish to risk the security of critical system resources.
Table of Contents

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

Direct Log Archiver ........................................................................................................ 4
  Move files to a specific folder ....................................................................................... 4
  Direct Log Archiver functionality ............................................................................... 4

Usage of Direct Log Archiver ....................................................................................... 5
  On the remote system where the log files are dumped .............................................. 5

On the EventTracker Manager System ........................................................................ 10
  Create VCP Port for DLA ......................................................................................... 10
  Associate VCP Port with DLA .................................................................................. 12

Configure DLA ............................................................................................................. 13

Verify ......................................................................................................................... 17

Verify in System Manager ......................................................................................... 17

Verify Task Manager .................................................................................................. 18

Verify Cache Folder .................................................................................................... 19

Verify Archives folder ............................................................................................... 19

Create Custom Configuration (INI) file ........................................................................ 20

Import Entire Row as Description ............................................................................... 24

System Manager .......................................................................................................... 27

Search DLA System Instance Logs ............................................................................. 27

EventTracker generated DLA related events ............................................................... 29

Vulnerability Scanners & Parsers ................................................................................ 31

Qualys Parser .............................................................................................................. 31
  Qualys Severity to EventTracker Weightage Mapping .............................................. 32

Nessus Parser ............................................................................................................... 32
  Nessus Severity to EventTracker Weightage Mapping ............................................ 33

SAINT Parser ............................................................................................................... 33
  SAINT Severity to EventTracker Weightage Mapping ............................................. 34

eEye Retina Parser ....................................................................................................... 34
  Retina Severity to EventTracker Vulnerability mapping .......................................... 35
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid7 NeXpose Parser</td>
<td>35</td>
</tr>
<tr>
<td>Rapid7 NeXpose Severity to EventTracker Weightage Mapping</td>
<td>36</td>
</tr>
<tr>
<td>Parse Vulnerability Scan Reports</td>
<td>36</td>
</tr>
<tr>
<td>Verify Vulnerability Parser Result – Windows Event Viewer</td>
<td>37</td>
</tr>
<tr>
<td>OpenVAS Parser</td>
<td>40</td>
</tr>
<tr>
<td>OpenVAS Threat to EventTracker Vulnerability mapping</td>
<td>40</td>
</tr>
<tr>
<td>Verify Vulnerability Parser Result – Windows Event Viewer</td>
<td>43</td>
</tr>
<tr>
<td>Appendix</td>
<td>45</td>
</tr>
<tr>
<td>Install and Configure FTP service in Win 2003</td>
<td>45</td>
</tr>
<tr>
<td>Install FTP service in Win 2003</td>
<td>45</td>
</tr>
<tr>
<td>Configure FTP Service in Win 2003</td>
<td>49</td>
</tr>
<tr>
<td>Grant user permission to access FTP site in Win 2003</td>
<td>54</td>
</tr>
<tr>
<td>Install and Configure FTP service in Win 2008</td>
<td>57</td>
</tr>
<tr>
<td>Install FTP service in Win 2008</td>
<td>57</td>
</tr>
<tr>
<td>Create FTP site in Win 2008</td>
<td>65</td>
</tr>
<tr>
<td>Configure FTP service in Win 2008</td>
<td>70</td>
</tr>
<tr>
<td>Grant User Permission to access FTP site in Win 2008</td>
<td>75</td>
</tr>
<tr>
<td>Install and Configure FTP service in Win 2012</td>
<td>79</td>
</tr>
<tr>
<td>Install FTP service in Win 2012</td>
<td>79</td>
</tr>
<tr>
<td>Example - Enable Automatic Logging (IIS)</td>
<td>86</td>
</tr>
<tr>
<td>To enable logging</td>
<td>86</td>
</tr>
<tr>
<td>DLA for BEA WebLogic logs</td>
<td>91</td>
</tr>
<tr>
<td>Configure Direct Log Archiver for BEA WebLogic logs</td>
<td>91</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>93</td>
</tr>
</tbody>
</table>
Direct Log Archiver

Direct Log Archiver helps to create CAB files by reading log files collected from external sources. Direct Log Archiver gets the required information like path of the source folder where log files are dumped, etc., from two ini files namely parser.ini and a user-defined ini file. These files are editable templates where you are required to provide valid information in appropriate sections for the Direct Log Archiver to use. Successful creation of CAB files depends on that vital information so exercise caution while providing configuration details.

Move files to a specific folder

Few of the optimal methods to move log files to the target location are as follows:

1. Manually move log files to the target location.
2. Create a script and configure the task scheduler in case of WINDOWS systems or run as CRON jobs in case of LINUX or UNIX or SOLARIS systems to automatically move log files to the target location.
3. Upload log files through FTP.

   It is highly recommended to consult application/OS specific documents to move log files to a specific folder.

Direct Log Archiver functionality

Once in 15 minutes EventTracker Scheduler service checks if “LogFileParser.exe” is running. If it is running, EventTracker Scheduler does not spawn a new instance. Otherwise, EventTracker Scheduler will launch LogFileParser.exe. LogFileParser in turn

1. Collects necessary information by reading the parser.ini that exists on the system where EventTracker is installed typically...\Program Files\Prism Microsystems\EventTracker
2. Reads the user-defined ini file in the source folder where logs are dumped on the remote system.
3. Reads the log files, creates a temp db in the ...\Program Files\Prism Microsystems\EventTracker\Cache folder, and inserts all records into the db.
4. Creates a sub-folder “Completed’ in the respective directories where logs are stored and moves the log files that have been read successfully to the “Completed’ folder. This helps the LogFileParser to identify the new log files and the ones that have been already processed.

EventTracker EventVault service compresses and securely stores the raw log data in the respective folders under...\Program Files\Prism Microsystems\EventTracker\Archives folder. Folders are created based on the value provided in the [Rxer_Port] section in the parser.ini file. If nothing is mentioned CAB files are stored in the ...\Program Files\Prism Microsystems\EventTracker\Archives\14505 folder.

This cycle repeats until there is no log file left for processing.
Usage of Direct Log Archiver

On the remote system where the log files are dumped

Note that if the EventTracker Manager and the log files source folder exist on the same system, you need not share the folder.

1. Create a folder “LOGFILES’

   For every application/log type, you need to create a different folder under “LOGFILES” directory.

   For example, create “W3SVC1’ and “SOLARIS-WEBLOG’ under “LOGFILES’ directory to dump IIS server logs and Solaris web logs.

   ...\LOGFILES\W3SVC1
   ...\LOGFILES\SOLARIS-WEBLOG

   If different types of logs are created by the same application like “FIREWALL LOGS’ and “WEB PROXY LOGS’ as in case of ISA Server, then create appropriate number of sub folders.

   ...\LOGFILES\ISASERVERLOGS\FWS
   ...\LOGFILES\ISASERVERLOGS\WEB

   For every application/log type you need to create a different configuration file and store it in the same folder where the respective log files are dumped. You can name the configuration files as you please.

   For example, create “FWS.ini’ and “WEB.ini’ files for ISA server logs. Update and save the configuration files with appropriate information in their respective folders.

   ...\LOGFILES\ISASERVERLOGS\FWS\FWS.ini
   ...\LOGFILES\ISASERVERLOGS\WEB\WEB.ini

2. Share the “LOGFILES’ folder and grant “Full Control’ Sharing permissions & “Full Control’ Security permissions to a domain user who has admin privileges over the system where log files are dumped and the EventTracker server system.

   For example, “JERRY’ is the computer where log files are dumped and “WEBDOC1’ is the computer where EventTracker is installed.
In this case, share the folder “LOGFILES’ on “JERRY’ and grant “Full Control’ access Sharing permission and “Full Control’ Security permission to “ETADMIN’.

“ETAdmin’ is a domain user and has admin privileges over both the systems (“WEBDOC1’ & “JERRY’)

a. Right-click the LOGFILES folder.
b. Click the Sharing tab.
c. Select the Share this folder option.
d. Click Permissions.
e. Click Add to add user (ETAdmin).
f. Click Locations to search the location of the User object.
g. Click OK after selecting the location of the user.
h. Type the name of the user in the Enter the object name to select field.
i. Click Check Names.
j. Select an appropriate user, if multiple user objects exist and then click OK.
k. Click OK.
l. Select the Full Control check box.
m. Click Apply and then click OK.
n. Click Apply.
o. Click the **Security** tab.

![Security tab](image_url)

Figure 2

p. Click **Add** to add “ETAdmin” user object.
q. Select the **Full Control** check box.
Figure 4


c. Click **Apply**, and then click **OK**.

LogFileParser creates a sub-folder “Completed” in the respective directories where logs are stored and moves the log files that have been read successfully to the new folder. This helps the LogFileParser to identify the new log files and the ones that are already processed.

For example, after processing “FIREWALL LOGS’ and ‘WEB PROXY LOGS’, LogFileParser moves the log files that are read successfully to the “Completed’ folder.

```
...\LOGFILES\ISASERVERLOGS\FWS\Completed\n
...\LOGFILES\ISASERVERLOGS\WEB\Completed
```
On the EventTracker Manager System

- Create VCP Port for DLA
- Associate the VCP Port with DLA

Create VCP Port for DLA

1. Log on to EventTracker.
2. Click the Admin hyperlink at the upper-right corner.
3. Click Manager from the dropdown list.
4. Click the Syslog / Virtual Collection Point tab.
5. Click Add under Virtual Collection Points.
   EventTracker displays the Receiver Port window.
6. Type the port number and a brief description in the Port Number and Description fields.

```
<table>
<thead>
<tr>
<th>Port Number</th>
<th>14515</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>DLA</td>
</tr>
<tr>
<td>Cache Path</td>
<td>C:\Program Files\Prism Microsystems\EventTracker\Cache</td>
</tr>
</tbody>
</table>

Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.
```

7. Click Save.
   EventTracker adds the port to the Virtual Collection Points pool.
8. Click **Save** on the Manager Configuration page.
Associate VCP Port with DLA

1. Click the **Direct Log Archiver** tab.

![Manager Configuration Screen](image)

2. Select the **Direct log file archiving from external sources** check box. EventTracker enables the Associated virtual collection point drop-down list.

3. Select the port (14515) from the **Associated virtual collection point** drop-down list.

4. Type the number of days in the **Purge files after** field to automatically delete the files transferred after specified number of days.

5. Click **Save** on the **Manager Configuration** page.
Configure DLA

1. In Direct Log Archiver tab, click the Add button. EventTracker displays the Direct Archiver Configuration pop-up window.
2. Select the log file extension from the Type drop-down list.

NOTE: EventTracker v8.0 now supports JSON, XML and Log4XML file types also.

3. Type the name of the configuration file with extension in the Configuration Name field, if you already have one.
   - You can also create an ini file with custom settings.
   - For more information, refer Create Custom Configuration (ini) file.
4. Type the path of the directory where log files are stored in the Log File Folder field.
   (OR)
   Click the Browse button to select the folder.

Figure 8
5. Click **Configure**.

EventTracker displays Direct Archiver Configuration window with more configuration options.

![Direct Archiver Configuration Window](image)
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Name of the log file configuration</td>
</tr>
<tr>
<td>Log Source</td>
<td>Source of the logs.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>Name of the computer from where the logs originated.</td>
</tr>
<tr>
<td>Computer IP</td>
<td>IP address of the computer from where the logs originated. If the computer could be resolved, then the IP address is displayed automatically in this field. Click the Get IP button if the IP address is not displayed automatically.</td>
</tr>
<tr>
<td>System Type</td>
<td>Select the operating system of the computer.</td>
</tr>
<tr>
<td>System Description</td>
<td>Type the system description. The description should be informative for future reference.</td>
</tr>
<tr>
<td>Comment Line Token</td>
<td>Type the character that is used to comment a line. Direct Log Archiver will ignore these comments.</td>
</tr>
<tr>
<td>Formatted Description</td>
<td>This option is selected by default. Parsed fields are mapped to the fields defined in the Message Fields.</td>
</tr>
<tr>
<td>Entire Row as Description</td>
<td>No field specification is required because the whole line will be considered as the description of the event.</td>
</tr>
<tr>
<td>Log File Format</td>
<td>If the log file is standard, then select an appropriate log file format from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>For example, if you select Microsoft IIS Log File Format, EventTracker populates the columns related to the file format in the Message Fields list.</td>
</tr>
<tr>
<td></td>
<td>Select the column name and click Remove to remove the column. You can also add new columns. Type the name of the column in the Message Fields field and then click Add.</td>
</tr>
<tr>
<td>Message Fields</td>
<td>Type the fields that you want to extract from the logs and then click Add.</td>
</tr>
<tr>
<td></td>
<td>To remove, select the field name and then click Remove.</td>
</tr>
<tr>
<td>Select Event Date &amp; Time fields</td>
<td></td>
</tr>
<tr>
<td>No. of fields</td>
<td>The log may contain date and time as a single filed in that case select No. of fields as 1.</td>
</tr>
<tr>
<td></td>
<td>If Date and Time are two different fields, then select the No. of Fields as 2.</td>
</tr>
<tr>
<td>Date Field</td>
<td>Select the Date field from the drop-down list box.</td>
</tr>
<tr>
<td>Time Field</td>
<td>Select the Time field from this drop-down list box.</td>
</tr>
</tbody>
</table>
6. Enter/select appropriate data in the relevant fields.

7. Click **Save & Close**.
EventTracker adds the DLA settings to the configuration pool.

![Manager Configuration](image)

Figure 6

Note that for every application/log you need to provide information and update the Direct Archiver.

**Verify**

- Verify in the System Manager
- Verify in the Task Manager
- Verify in the Cache Folder
- Verify in the Archives Folder

**Verify in System Manager**

To crosscheck EventTracker Receiver receives logs through the VCP port associated with the Direct Log Archiver.

1. Click the **Admin** hyperlink.
2. Click **Systems**.
Verify Task Manager

To verifyLogFileParser is initiated by the EventTracker Scheduler process and EventTracker Receiver spawned a new process EtReceiver-W-14515.exe.

- Open the Task Manager
Verify Cache Folder

Verify mdb Files are being created in the Cache Folder.

- Open the “Cache’ folder in the EventTracker installation folder.

![Figure 9](image)

Verify Archives folder

Verify archive folder is created with the folder name as VCP port number assigned to DLA.

1. Open the “Archives“ folder in the EventTracker installation folder.

![Figure 10](image)

2. Open the folder 14515 to view the DLA related CAB files moved by EventTracker EventVault service.
Create Custom Configuration (INI) file

If the ini file does not exist in the root directory of log files, type the name of the configuration file in the Configuration Name field. EventTracker creates a configuration file with the settings you provide in the Log File Configuration window.

1. Open the Manager Configuration page.
2. Click the Direct Log Archiver tab.
3. Click Add under Direct Log Archiver. Type appropriately in the relevant fields.
4. Click **Configure**.
5. Enter/select appropriately in the relevant fields.
6. Select the **Log File Format** as **Custom Log File Format**.
Direct Archiver Configuration

Log file configuration

Configuration Name: C:\LOGFILES\ISALOGIWeb\isaserverlog
Log Source: ISAWEB
Computer Name: ISA
Computer IP: 192.168.1.1

System Type: 2000 Server
System Description: ISA WEB
Comment Line Token: #

Entire Row as Description
Formatted Description
Log File Format: Custom Log File Format
Message Fields

Select Event Date and Time Fields
No of Fields: 2
Date Field
Time Field

Select Column Mapping
Computer

<< BACK  SAVE & CLOSE  CANCEL

Figure 18
7. Type the field name **Message Fields** field.
8. Click **Add**.

Direct Log Archiver adds the message fields.

![Direct Archiver Configuration](image)

9. Click **Save & Close**.
10. Click **Save** on the **Manager Configuration** page.

Direct Log Archiver creates the ini file and starts parsing the log files in the source folder. Open the log files source folder to verify if Direct Log Archiver has created the ini file.
Import Entire Row as Description

When you select this option, no field specification is required since the entire row is considered as the description of the event.

1. Open the Manager Configuration page.
2. Click the Direct Log Archiver tab.
3. Click Add under Direct Log Archiver.
4. Type appropriately in the relevant fields.
5. Click **Configure**. Enter/select appropriately in the relevant fields.
6. Select **Entire Row as Description** option.
7. Click **Save & Close**.
8. Click **Save** on the **Manager Configuration** page.
System Manager

EventTracker creates a DLA system instance with the name of the Agent appended by “-DLA’ and transfers filtered events and other log files through the DLA channel.

Also, adds the DLA system instances under Default system group.

Search DLA System Instance Logs

1. Log on to EventTracker.
2. Click the Search hyperlink at the upper-right corner. EventTracker opens the Log Search browser.
3. Expand the Computer node and click a DLA system. For example, MCLOON-DLA (OR)
4. Type a DLA system instance name in the search field and then click GO. Example: MCLOON-DLA Log Search Utility displays the Match Counts graph.

![Match Counts (Last 7 days) - Internet Explorer](http://192.168.1.159:8080/EventTracker/LogSearch/KeywordIndexerGraph.aspx?Param=sys:mcloon-dla&ts=1438566407211)

Figure 16
5. Click the **Click here** hyperlink to search unindexed events.
6. Click any disc on a cylinder to search logs in a particular time frame.
Log Search Timeline window displays the search result.

![Log Search Timeline](image)

**Figure 17**
## EventTracker generated DLA related events

<table>
<thead>
<tr>
<th>Event Id</th>
<th>Description</th>
<th>Event Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>3244</td>
<td>Direct log archiver started processing.</td>
<td>This event is generated when Direct Log Archiver is started file processing.</td>
</tr>
<tr>
<td>3245</td>
<td>Direct log archiver successfully processed the following files: C:\LogFiles\W3SVC1\ex070709.log C:\LogFiles\W3SVC1\ex070710.log C:\LogFiles\W3SVC1\ex070712.log</td>
<td>This event is generated when Direct Log Archiver successfully completes processing of log files.</td>
</tr>
<tr>
<td>3246</td>
<td>Direct log archiver stopped processing: Total number of files processed: No files are available for processing. Direct log archiver stopped processing. Total number of files processed: 3</td>
<td>This event is logged when Direct Log Archiver stops processing. This event contains total number of files processed.</td>
</tr>
<tr>
<td>3247</td>
<td>Direct log archiver failed to process the following files: C:\LogFiles\W3SVC1\ex070622.log C:\LogFiles\W3SVC1\ex070626.log C:\LogFiles\W3SVC1\ex070628.log</td>
<td>This event is logged when Direct Log Archiver fails to process log files. This event contains the list of files processing failed.</td>
</tr>
</tbody>
</table>
**Event Id:** 3254

**Source:** EventTracker

**Description:** Direct Log Archiver did not find any file to process in last 24 hours for following configured path:

```<Log file full path> Event```

**Information:**

**Cause:**

This event is logged when Direct Log Archiver did not process any file in last 24 hours for configured path. Description contains Log file path for which it did not find any files in last 24 hours.

**Resolution:**

a. Verify the Logfile path is correct and file is available in this path

b. Verify log file type configured is correct

**Source:** [http://kb.eventtracker.com](http://kb.eventtracker.com)
Vulnerability Scanners & Parsers

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses. There are several types of vulnerability scanners available today, distinguished from one another by a focus on targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. Vulnerability scanners are a core technology component of Vulnerability management.


Qualys Parser

The EventTracker v8 parser reads the Qualys XML report and extracts vulnerability information from it to adjust the vulnerability weightage of systems managed by EventTracker. When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see below) and updates the vulnerability weightage of the managed system.

The root element of a Qualys XML report is named "SCAN". It contains a child element named "IP" for each IP address that was scanned by the vulnerability scanner. The child objects of "IP" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Qualys XML are:

1. Minimal
2. Medium
3. Serious
4. Critical
5. Urgent
Qualys Severity to EventTracker Weightage Mapping

<table>
<thead>
<tr>
<th>Qualys Severity</th>
<th>EventTracker Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Minimal)</td>
<td>1 (Low)</td>
</tr>
<tr>
<td>2 (Medium)</td>
<td>2 (Medium)</td>
</tr>
<tr>
<td>3 (Serious)</td>
<td>3 (High)</td>
</tr>
<tr>
<td>4 (Critical)</td>
<td>4 (Serious)</td>
</tr>
<tr>
<td>5 (Urgent)</td>
<td>5 (Critical)</td>
</tr>
</tbody>
</table>

Nessus Parser

The EventTracker v8 reads the Nessus XML (V1 and V2) report and extracts vulnerability information from it to adjust the vulnerability weightage of systems managed by EventTracker. When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see below) and updates the vulnerability weightage of the managed system.

Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Nessus XML are:

0 - Open Port
1 – Low
2 – Medium
3 – High
Nessus Severity to EventTracker Weightage Mapping

<table>
<thead>
<tr>
<th>Nessus Severity</th>
<th>EventTracker Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (Open Port)</td>
<td>0 (Undefined)</td>
</tr>
<tr>
<td>1 (Low)</td>
<td>1 (Low)</td>
</tr>
<tr>
<td>2 (Medium)</td>
<td>3 (High)</td>
</tr>
<tr>
<td>3 (High)</td>
<td>5 (Critical)</td>
</tr>
</tbody>
</table>

SAINT Parser

The EventTracker v8 parser reads the SAINT XML report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

The integration is tested with report generated by version 7.4.1 of SAINT.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see below) and updates the value of "V" for the managed system.

The root element of a SAINT XML report is named "report". It contains a child element called "details" from which EventTracker extract the vulnerability information. This element contains a child element named "host_info" for each system that was scanned by the vulnerability scanner.

The child objects of "host_info" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the SAINT XML are:

1. critical - Critical Problem (Red) – Vulnerabilities which could allow an attacker to gain direct and unassisted read, write, or command execution access, or to create a denial of service.
2. concern - Area of Concern (Yellow) – Vulnerabilities which could allow privilege elevation, remote access upon some user action, bypass of security measures, use of the target as an intermediary in an attack, or disclosure of passwords or other information that could be used in an attack, but do not themselves result in direct, unassisted remote access.
3. potential - Potential Problem (Brown) – Services or applications which may or may not be vulnerabilities, depending on the version, patch level, or configuration. Further investigation on the part of the administrator may be necessary.
4. service - Service (Green) – Any service which is running, regardless of whether or not it is vulnerable.
SAINT Severity to EventTracker Weightage Mapping

<table>
<thead>
<tr>
<th>SAINT Severity</th>
<th>EventTracker Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>service (Green)</td>
<td>0 (Undefined)</td>
</tr>
<tr>
<td>potential (Brown)</td>
<td>1 (Low)</td>
</tr>
<tr>
<td>concern (Yellow)</td>
<td>3 (High)</td>
</tr>
<tr>
<td>critical (Red)</td>
<td>5 (Critical)</td>
</tr>
</tbody>
</table>

eEye Retina Parser

The EventTracker v8 parser reads the Retina XML report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see below) and updates the value of "V" for the managed system.

The root element of a Retina XML report is named "scanJob". It contains a child element called "hosts" from which EventTracker extract the vulnerability information. This element contains a child element named "host" for each system that was scanned by the vulnerability scanner.

The child objects of "host" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Retina XML are:

Information - A security vulnerability that gives the attacker more information, which then helps him to target his attacks more successfully. These can be directory structures, account names, network addresses, or the internal descriptions and information of other machines.

Low - Low-risk vulnerability usually include vulnerabilities that can be exploited to read files containing public information, or a vulnerability that gives an attacker very minimal access to a remote system.

Medium - Medium Level usually includes vulnerabilities that can be exploited to gain general access to a system. Vulnerabilities that allow attackers to remotely view sensitive files can be categorized here also.
High - Full remote access. A vulnerability that can be exploited to gain total access of a machine remotely falls under this category. These vulnerabilities are extremely severe, and tools to exploit them are usually publicly available.

Retina Severity to EventTracker Vulnerability mapping

<table>
<thead>
<tr>
<th>Retina Severity</th>
<th>EventTracker Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>0 (Undefined)</td>
</tr>
<tr>
<td>Low</td>
<td>1 (Low)</td>
</tr>
<tr>
<td>Medium</td>
<td>3 (High)</td>
</tr>
<tr>
<td>High</td>
<td>5 (Critical)</td>
</tr>
</tbody>
</table>

Rapid7 NeXpose Parser

The EventTracker v8 parser reads the Rapid7 NeXpose XML report and extracts vulnerability information from it to adjust the vulnerability weightage of systems managed by EventTracker. When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see below) and updates the vulnerability weightage of the managed system.

The root element of a Rapid7 NeXpose XML report is named "SCAN". It contains a child element named "IP" for each IP address that was scanned by the vulnerability scanner. The child objects of "IP" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Rapid7 NeXpose XML are:

1 – Minimal
2 – Medium
3 – Serious
4 – Critical
5 – Urgent
Rapid7 NeXpose Severity to EventTracker Weightage Mapping

<table>
<thead>
<tr>
<th>Rapid7 NeXpose Severity</th>
<th>EventTracker Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Minimal)</td>
<td>1 (Low)</td>
</tr>
<tr>
<td>2 (Medium)</td>
<td>2 (Medium)</td>
</tr>
<tr>
<td>3 (Serious)</td>
<td>3 (High)</td>
</tr>
<tr>
<td>4 (Critical)</td>
<td>4 (Serious)</td>
</tr>
</tbody>
</table>

Parse Vulnerability Scan Reports

1. Log on to EventTracker.
2. Click the Admin hyperlink at the upper-right corner.
3. Click Manager on the Control Panel.
4. Click the Syslog / Virtual Collection Point tab.
5. Add a port under Virtual Collection Points.
6. Click the Direct Log Archiver tab.
7. Click Add under Direct Log Archiver.
   Direct Log Archiver displays the configuration pop-up window.
8. Select the Type as Vulnerability.
9. Select a parser from the Parser drop-down list.
10. Type the path of the source folder.

(OR)

Click the Browse button to select the folder.
11. Click **Save**.
12. Click **Save** on the **Manager Configuration** page.

Similarly add Nessus Parser. EventTracker adds the DLA settings to the configuration pool.

**Verify Vulnerability Parser Result – Windows Event Viewer**

1. Open the Windows Event Viewer.
2. Expand **Windows Logs**, and then select **Application** on the left pane.
3. Set the event filter to display event id 2045
4. Double-click an event to view details.
Figure 20

Figure 28
OpenVAS Parser

The EventTracker v8 parser reads the OpenVAS XML report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest threat value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see below) and updates the value of "V" for the managed system.

The root element of a OpenVAS XML report is named "report". (The "report" element might optionally be enclosed in an outer "get_reports_response" element). The "report" element contains a child element with the same name i.e. "report". This child "report" element contains a child element called "results" (XPath:"
/report/report/results") from which EventTracker extract the vulnerability information. This element contains a child element named "result" for each vulnerability detected on all systems that were scanned by the vulnerability scanner.

The child objects of "result" element contain host name and vulnerability information. Each vulnerability detected on target has threat value associated with it. The possible threat values defined in the OpenVAS XML are:

- 1- Debug
- 2- Log
- 3- Low
- 4- Medium
- 5- High

OpenVAS Threat to EventTracker Vulnerability mapping

<table>
<thead>
<tr>
<th>OpenVAS Severity</th>
<th>EventTracker Weightage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug</td>
<td>1 (Low)</td>
</tr>
<tr>
<td>Log</td>
<td>2 (Medium)</td>
</tr>
<tr>
<td>Low</td>
<td>3 (High)</td>
</tr>
<tr>
<td>Medium</td>
<td>4 (Serious)</td>
</tr>
<tr>
<td>High</td>
<td>5 (Critical)</td>
</tr>
</tbody>
</table>
To configure OpenVAS parser

1. Log on to EventTracker.
2. Click the **Admin menu** at the upper-right corner and then click **Manager**.
3. Click the **Direct Log Archiver** tab.
4. Click **Add** under **Direct Log Archiver**.
   - Direct Log Archiver displays the configuration pop-up window.
5. Select the **Type** as **Vulnerability**.
6. Select a parser from the **Parser** drop-down list.
   - In this case, OpenVAS parser.
7. Type the path of the source folder.
   - (OR)
     - Click the **Browse** button to select the folder.

![Direct Archiver Configuration](image)

**Figure 29**

8. Click the **Configure** button.
9. Click **Save** on the **Manager Configuration** page.

EventTracker adds the DLA settings to the configuration pool.
Verify Vulnerability Parser Result – Windows Event Viewer

1. Open the Windows Event Viewer.
2. Expand Windows Logs, and then select Application on the left pane.
3. Set/search the event viewer for Event Id 2161.

![Windows Event Viewer](image)

Figure 22

4. Double-click an event (i.e. Event ID: 2161) to view details.
Figure 23
Appendix

Install and Configure FTP service in Win 2003

Install FTP service in Win 2003

1. Click the **Start** button, select **Settings**, and then select **Control Panel**.
2. Double-click **Add or Remove Programs**, and then select **Add/Remove Windows Components**. Windows Component Wizard displays.
3. Click **Application Server**.
   Do not select the check box.

![Windows Components Wizard](image)

4. Click **Details**. Click **Internet Information Services (IIS)**.
   Do not select the check box.
5. Click **Internet Information Services (IIS)**.
   Do not select the check box.
6. Click **Details**.
7. Select the **File Transfer Protocol (FTP) Services** check box and then click **OK**.
Common Files and Internet Information Services Manager check boxes are selected by default once you select the File Transfer Protocol (FTP) Services check box.

8. Click OK on the Application Server window.

![Windows Components Wizard](image)

**Figure 36**

Windows Components Wizard starts configuring the requested changes.

![Insert Disk](image)

**Figure 37**

9. Insert the Disk when asked for and then click OK to continue.
10. Click the **Finish** button.
Configure FTP Service in Win 2003

1. Click the Start button, select Programs, and then select Administrative Tools.
2. Click Internet Information Services (IIS) Manager.
3. Expand the local computer node.
4. Right-click Default FTP Site and then select Properties from the shortcut menu.

Default FTP Site Properties window is displays.

5. Click the Security Accounts tab.
6. Clear the **Allow anonymous connections** check box. This prevents unauthorized users accessing the FTP site.

7. Click **Yes** on the confirmation message box.

8. Click the **Home Directory** tab.
9. Type the path of the folder where you want to dump log files in the **Local path** field. You can also **Browse** and select the folder path.

10. Click the **Directory Security** tab.
The **Granted access** option is selected by default. This option facilitates only the selected computers to communicate with the FTP server.

11. Click the **Add** button.
**Single computer** option is selected by default. Type the IP address of the computer in the **IP address** field and then click **OK**. You can also use **DNS Lookup** to resolve hostnames.

12. Select the **Group of computers** option to add a set of computers.

![Deny Access](image)

**Figure 32**

13. Type the **Network ID** and **Subnet mask** in the relevant fields and then click **OK**.

14. Click **OK** on the Default FTP Site Properties window.
Grant user permission to access FTP site in Win 2003

1. Right-click Default FTP Site and select **Permissions** from the shortcut menu.

![Figure 46](image)

**Security tab displays.**

![Figure 47](image)
2. Click the Add button.

3. Type the name of the user in the Enter the object names to select field, for example, ETAdmin

4. Click Check Names when it is enabled.

5. Click OK.

Grant full control security permissions to the administrator.
6. Click **OK** and then close the Internet Information Services (IIS) Manager console.
Install and Configure FTP service in Win 2008

Install FTP service in Win 2008

1. Click the **Start button**, select **Programs**, and then select **Administrative Tools**.
2. Select **Server Manager**.

![Server Manager](image)

Figure 34
3. Click **Roles** on the left pane.
4. Click **Add Roles**.
   Add Roles Wizard displays.

5. Click **Next >**.
   Add Roles Wizard displays Select Server Roles window.

6. Click the **Web Server (IIS)** check box.
7. Click **Next >**
8. Click **Next >**

9. Scroll down to select **FTP Server**.
10. The sub options **FTP Service and FTP Extensibility** will be selected automatically.

11. Click **Next >**.

   Confirm Installation selections pane displays.
12. Cross the options and then click the **Install** button. Installation Results displays a successful message.
13. Click the **Close** button.
Create FTP site in Win 2008

1. Click the **Start button**, select **Programs**, and then select **Administrative Tools**.
2. Select **Internet Information Services (IIS) Manager**.
3. Expand the local computer node, expand **Roles** node, and then expand **Web Server (IIS)** node.
4. Select **Internet Information Services** and then select **Sites** folder.

![Figure 38](image)

5. Select **Add FTP Site** in **Actions** pane.

Add FTP site window displays.
6. Enter **FTP site name**:  
   Ex: Default FTP Site  
7. Select the browse button and select the physical path.
8. Click the **Next** button.

   Binding and SSL Setting window displays.
9. Click **Next** and then click the **Finish** button.
The default FTP site window displays.

Figure 43
Configure FTP service in Win 2008

1. Select the **Start button**, select **Programs**, and then select **Administrative Tools**.
2. Select **Internet Information Services (IIS) Manager**.
3. Expand the local computer node, expand **Roles** node, and then expand **Sites** folder.
4. Select **Default FTP Site**.

![Image of FTP configuration](image)

Figure 66

5. Select **Advance Settings** to verify the physical path and connections.
6. Select **Basic Settings** and select the path to dump the log files.
7. Select **FTP authentication** and do not allow unauthorized users access FTP site.

![FTP Authentication Configuration](image)

**Figure 69**

8. If anonymous authentication is enabled, then right click **Anonymous authentication** and **Disable** it. (OR)
   - In **Actions** pane, click **Disable**.
9. Double click **FTP Logging** and then select **Enable**, if it is disabled.
10. Select **IPv4 Domain IP and Restrictions** to allow/deny access to certain IP addresses. This option allows/denies computers to communicate with FTP server. You can specify a IP address or Range of IP addresses.

11. To allow certain IP addresses in **Actions** pane, click **Add Allow Entry**.

12. Enter the relevant IP address and then click **OK**.
13. To deny access to certain IP address in **Actions** pane, click **Add Deny Entry**.
14. Enter the relevant IP address and then click **OK**.
Grant User Permission to access FTP site in Win 2008

1. Right click **Default FTP site** and then select **Edit Permissions**.

   ![FTP root properties window displays](image)

   **Figure 47**

   FTP root properties window displays.

2. Select **Security** tab.
3. **Select the Edit button.**

Permissions for ftproot window displays.
4. Click the **Add** button.
   Select Users, Computers, Service Accounts, or Groups displays.

   ![Select Users, Computers, Service Accounts, or Groups](image)

   **Figure 76**

5. **Enter the object names to select** and then click **Check Names**.
   
   Ex: ETAdmin.

   ![Select Users, Computers, Service Accounts, or Groups](image)

   **Figure 77**

6. Click the **OK** button.
7. Select **Full Control** permissions and then click the **Apply** button.
8. Click the OK button and then close **Internet Information Services (IIS) Manager** console.
Install and Configure FTP service in Win 2012

Install FTP service in Win 2012

1. Log on to Win2k12 server.

2. Click on Server Manager icon available in the task bar. Server Dashboard displays.

3. Select Manage, and then select Add Roles and Features. Add Roles and Features Wizard displays.
4. **Click Next >**

Select Installation Type window displays.

‘Role based or feature based selection’ option is selected by default. You can select the installation type as per the requirement.
5. Click **Next >**

Select destination server window displays.
6. Select Local Server from the server pool, and then select Next.
7. In Roles pane, select the Application Server, and then select Web Server (IIS).

**Add Roles and Features Wizard** displays the confirmation message.
8. Click the **Add Features** button.

9. Click **Next >** and then click **Next >** again.

![Add Roles and Features Wizard](image)

10. Select **Web Server Role (IIS)**. Click **Next >**.

11. In **Role Services** pane, scroll down to select **FTP Server**.

12. Select the sub options **FTP Server, FTP Extensibility** and then click **Next >**.
Confirm Installation selection panel displays the confirmation message.

13. Cross check the options and then click the **Install** button.
Confirm installation selections

To install the following roles, role services, or features on selected server, click Install.

- Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

<table>
<thead>
<tr>
<th>Web Server (IIS)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
<td></td>
</tr>
<tr>
<td>Common HTTP Features</td>
<td></td>
</tr>
<tr>
<td>Static Content</td>
<td></td>
</tr>
<tr>
<td>Default Document</td>
<td></td>
</tr>
<tr>
<td>Directory Browsing</td>
<td></td>
</tr>
<tr>
<td>HTTP Errors</td>
<td></td>
</tr>
<tr>
<td>Health and Diagnostics</td>
<td></td>
</tr>
<tr>
<td>HTTP Logging</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
</tbody>
</table>

Export configuration settings
Specify an alternate source path

Figure 87
Example - Enable Automatic Logging (IIS)

This example guides you enable automatic logging facility provided in the IIS Web Server running on a remote computer and configure Direct Log Archiver on EventTracker Manager computer to access and archive those log files.

To enable logging

1. Select the **Start** button, select **Settings**, and then select **Control Panel**.
2. Select **Administrative Tools** and then select **Internet Information Services Manager**.
3. Right-click the **Default Web Site**, and then select **Properties**.
Figure 89

Figure 56
Enable Logging option is selected by default. Active Log Format drop-down list, gives you three options for the log format:

- Microsoft IIS Log Format
- NSCA Common Log File Format
- W3C Extended Log File Format.

The NCSA common log format is nothing more than a simple, plain text log. The IIS log file format is a fixed ASCII text-based format, so you cannot customize it. Because HTTP.sys handles the IIS log file format, this format records HTTP.sys kernel-mode cache hits. The W3C Extended Log File Format option is selected by default. If you need to do process accounting, you must use this log format because it’s the only option that will log process accounting information.

4. Click the Properties button.

![Extended Logging Properties](image.png)

Figure 57

Configure the W3C logging options. The General Properties tab will be selected by default. This tab helps you to keep the log’s physical size under control. You can tell IIS to build a new log on an hourly, daily, weekly, or monthly basis. Other options allow you to use an unlimited log file size, or to start a new log file when the existing log file grows to a predetermined size.

The Use Local Time for Naming And Rollover check box is important because unlike the other two types of logging, W3C logging uses Greenwich Mean Time also known as GMT rather than local time.

Log file directory displays the default path and you can also change the path.
5. To change the path of the directory, click **Browse**.

![Extended Logging Properties](image)

**Figure 58**

6. Select the appropriate folder to store the log files, and then click **Apply**.
   IIS server creates a folder W3SVC1 under c:\LogFiles and moves the log files. Since you’ve selected Daily as the Log Time Period option, IIS server creates log files and names the log files with the date format (yy –year, mm – month and dd – date).

7. To customize the log files, select **Extended Properties** tab.
   Here you can select the desired events to be recorded in the log file.
8. Click **OK**.

9. Click **OK** on the **Default Web Site** Properties window.
DLA for BEA WebLogic logs

Configure Direct Log Archiver for BEA WebLogic logs

1. Associate a Virtual Collection Point.
   For example: 14515
2. Click the Add button.
3. Select the Log File Folder or type the UNC path of the log file root directory on the remote computer.
4. Select the Log File Extension.
   Example: Log
5. Select the Field Separator.
   Example: Space Note that the Field Separator should not be None.
6. Select the configuration file if it does exist in the log file root directory or type name of the configuration file. EventTracker creates the ini file in the log file root directory based on the configuration information you provide in the Log File Configuration window.
7. Click **Configure**.
EventTracker displays the Log File Configuration window.
Enter the required information.

![Direct Archiver Configuration](image)

**Figure 61**

Note that **Message Fields** are not significant for WebLogic logs.

8. Click **Save & Close**.
EventTracker adds the configuration.
Troubleshooting

Problem #1

I’ve configured DLA to process Log Files, but when I tried to generate reports I’m getting “No matching records found’.

Solution

1. Do Log Search for event 3245. The description part of this event will give you the list of log files successfully processed by DLA.
   - Verify if the log file path and name for which you are generating report is listed in the event description. If it is listed, then do the log analysis for event 3230 for that computer and check for the format of the description. This will give you an idea whether the file has been processed or not.

2. Do Log Search for event 3247.
   - If yes, check if the Log On user account configured for EventTracker Scheduler service has permission on the Log Files root directory had you provide UNC path in the configuration file. This user account should have READ & WRITE permission on the Log Files root directory.
   - Verify if the log file(s) is not corrupt.

3. Check if the log file(s) are being pushed to the configured Log Files root directory.

Problem #2

I see that log file(s) are pushed to the Log Files root directory, but it is not processed

Solution:

1. Verify if the extension of the log file and the extension that you have mentioned in the Configuration File (ini) are same.

2. Verify that you have properly configured Log Files root directory in the Configuration File (ini).

3. Check whether the Log File path is configured in DLA configuration.

4. Check whether Log File root directory is accessible from the Manager system.

Problem #3

I can generate log analysis, but when I do custom column analysis I get “No Matching Record Found”.

Solution

Verify that the Column Name and the field Separator are properly configured in the Configuration File (ini).