EventTracker: EventVault Explorer

Introduction and Usage for v8.0
Introduction

EventVault Explorer is designed to make the log search faster and easier for the user. User can search for more specific data with the help of EventVault Explorer. The search criteria set by user will be saved for future reference in the database.

EventVault Explorer can also be configured to use remote MS SQL Server database.

Purpose

This document will guide you to search for logs in the EventVault Explorer for all EventTracker v8.x versions.

Audience

EventTracker Enterprise users who wish to use EventVault Explorer to search for logs.
# Table of Contents

EventVault Explorer ............................................................................................................................... 3  
Execute search in EventVault Explorer .......................................................................................................................... 3  
  Search CAB files, through ‘New Search’ tab................................................................................................................. 3  
  Search CAB files, through ‘Search History’ tab ........................................................................................................... 10  
  Refine Criteria - Metadata........................................................................................................................................ 12  
  Refine Criteria - Advanced Search......................................................................................................................... 14  
  Refine Criteria - Category ....................................................................................................................................... 15  
  Refine Criteria - SQL Query................................................................................................................................. 16  
Configure EventVault Explorer to use remote SQL Server .......................................................................................... 17  
  In SQL Server system............................................................................................................................................... 18  
  In EventTracker server........................................................................................................................................... 18
EventVault Explorer

Existing Report/Log Search architecture goes through the typical CAB file processing for generating report or finding out specific data based on the given criteria. In real time environments (on heavy load scenarios, unknown conditions and multiple searches) this process takes lot of time and does not solve the immediate queries. Easy way to process quickly is to have the archived events in a cache, so that redundant processing of CAB files is eliminated.

Based on the given criteria, EventVault generates search result from cache and saves the search results as Search history for future reference.

Run ad-hoc reports and save the data in a database. You can further drill-down the cached data by,

- Specifying location, words, exact word/phrase or range of Event Id, in Advance search
- Selecting existing Category
- Constructing your own SQL Query

User can also configure EventVault Explorer to use remote MS SQL server database.

Execute search in EventVault Explorer

This option helps you to search CAB files.

Search CAB files, through ’New Search’ tab

1. Log on to EventTracker Enterprise.
2. Select the Reports menu, and then select Explorer.
   EventTracker displays the EventVault Explorer window.
3. Click the **New Search** tab.
4. In **Duration** tab, select any one option to specify the time range to generate the results from metadata.
   - Select interval- Select the number of days/weeks/months from the dropdown
   - Select date range- Select the date and time for which the data needs to be searched.

5. To search between specific time range, select **Limit to time range** option.
6. In **Systems** tab, select Groups/ Systems/Sites/All Systems to fetch records based on the input selection/criteria.
7. Click **Refine/Filter** tab, and set the refine and/or filter criteria for the search result.

8. For future reference, provide an appropriate description for the search criteria in the **Description**.
   
   This is not a mandatory field.

9. Click the **Search** button.
   
   EventTracker displays the **Disk cost analysis** pop-up window.
10. Click **OK**.
   
   EventTracker displays information message box.

11. Click the **OK** button.
   
   EventTracker displays **Search History** tab with the result set.
12. Click the **Status** hyperlink.

   EventTracker displays EventVault Explorer processing status message box.

**NOTE:** Before performing the Search, make sure you have proper permission to the user database.
<table>
<thead>
<tr>
<th>Status</th>
<th>For</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing</td>
<td>Cab Extraction</td>
</tr>
<tr>
<td>Exception Occurred</td>
<td>Failed</td>
</tr>
<tr>
<td>Status of unpacking Archives</td>
<td>All the archives have been processed (unpacked) successfully.</td>
</tr>
</tbody>
</table>

**Search CAB files, through ‘Search History’ tab**

As said earlier, EventTracker saves all your queries and the result set in the data cache. You can reuse the data to further refine the search.

1. Click the **Reports** menu, and then select **Explorer**.
   EventTracker displays the EventVault Explorer.

2. Select **Explore** 🌐 icon.
   Flex Data Refine window displays.
**EXPLORER CRITERIA**

**REPORT TITLE:** Change Audit

- **Log Type:**
  - System (14,760)
  - Security (257)
  - Application (14,355)
  - Microsoft-Windows-TaskScheduler/Operational (15)
  - TechSmith (1)
  - Microsoft-Windows-Bits-Client/Operational (11)
  - Microsoft-Windows-Diagnostics

- **Event Type:**
  - Error (91)
  - Warning (171)
  - Information (28,897)
  - Audit Success (149)
  - Audit Failure (112)
  - Verbose (1)

- **Category:**
  - 0 (1,049)
  - 32770 (1)
  - 49499 (1)
  - 49152 (2)
  - 32768 (4)
  - 2 (28,363)

- **Event Id**
  - 0 (3)
  - 4 (11)
  - 16 (11)
  - 29 (1)
  - 35 (1)
  - 101 (4)
  - 11 (1)

- **Source**
  - Application Popup (1)
  - EventTracker (29,107)
  - Intrusion (3)
  - Microsoft-Windows-Bits-Client (11)
  - Microsoft-Windows-Diagnostics-Performance (1)
  - Microsoft-Windows-GroupPolicy (3)

- **Domain**
  - TCODS (9,536)
  - LPE (467)
  - NT AUTHORITY (1,808)

- **Computer**
  - TCODS-H (29,411)

**Event description:**

**Filter description:**

**From:** 11/18/2015 06:59:48 PM  
**To:** 11/19/2015 06:59:48 PM

- Limit to time range

**Search Criteria**

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Systems</th>
<th>Action</th>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Start time: 11/18/2015 5:59:48 PM  
End time: 11/19/2015 5:59:48 PM | *Site*: TCODS-H  
*Groups*: TCODS  
*Systems*: ESXWNSVNM1, TCODS-H, MCLOON-H  
*Filter*: Event Source (None) | Refine user: None  
Refine info: None | Filter user: None  
Filter info: None  
Filter Event Source(s): None |
### EventTracker: EventVault Explorer

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata</td>
<td>Metadata displays event properties and its count in the search result. You can further narrow down the search criteria by selecting specific event properties.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Refer Advanced Search section in the Log Search User Guide.</td>
</tr>
<tr>
<td>Category</td>
<td>Select a Category or Categories to search associated events.</td>
</tr>
<tr>
<td>SQL Query</td>
<td>Select this option to frame your own query. Available fields in the logs selected are displayed to aid you in framing queries. Follow the examples to avoid errors and make sensible yet powerful queries.</td>
</tr>
</tbody>
</table>

1. Click the **New Search** button to go the **New Search** tab in EventVault Explorer.
   
   (OR)
   
   Click **Search** to see the search result based on the given search criteria.
   
   EventTracker displays the result set.

   **NOTE:**
   
   EventTracker saves the searches in the database.

**Refine Criteria - Metadata**

The event properties in the search result are in the form of precooked metadata which are readily available for further refinement. Each event property displays the number of occurrences in the respective search result. Different event properties can be combined together to get a refined result. The search/refine process can be limited to a defined time range.
EXPLORER CRITERIA

REPORT TITLE: Logs - Detail hourly

System:
- MCOON-II (355)
- 9001 (2)
- 7536 (2)
- 7066 (8)
- 7026 (1)
- 7017 (2)
- 7011 (1)
- 7009 (1)

Event ID:
- TechSmith Uploader Service (1)
- TechSmith Updater (4)
- SideBySide (2)
- Service Control Manager (5)
- MCOON-II (1)
- Microsoft-Windows-WMI-Activity (66)
- Microsoft-Windows-WMI (1)

Source:
- SYSTEM (305)
- sunanda (19)
- N/A (20)
- LOCAL SERVICE (11)

User:
- SYSTEM (305)
- sunanda (19)
- N/A (20)
- LOCAL SERVICE (11)

From 11/30/2015 08:11:46 AM To 12/01/2015 12:32:02 PM

SEARCH CRITERIA

<table>
<thead>
<tr>
<th>TIME RANGE</th>
<th>SYSTEMS</th>
<th>REFINE</th>
<th>FILTER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time: 12/1/2015 2:00:00 PM</td>
<td>MCOON-II Groups:ETvTracker</td>
<td>None</td>
<td>Filter user: None</td>
<td></td>
</tr>
<tr>
<td>End time: 12/1/2015 3:00:00 PM</td>
<td></td>
<td>Refine info: None</td>
<td>Filter info: None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Filter Event (0): None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Filter Event Source (0): None</td>
<td></td>
</tr>
</tbody>
</table>

Figure 12
Refine Criteria - Advanced Search

Advanced search helps you to refine the results by providing any of the standard or custom columns. It also helps you to fetch the result which contains an exact word or part of the word/phrase, and event id range.

![EXPLORER CRITERIA](image)

**SEARCH CRITERIA**

<table>
<thead>
<tr>
<th>TIME RANGE</th>
<th>SYSTEMS</th>
<th>REFINE</th>
<th>FILTER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time: 11/30/2015 2:34:39 PM</td>
<td>*System=McLoid-H, Group=TOONS, System=mcast1, McLoid-H, McLoid-II, TOONS.LOCAL, vwwes3.xm9</td>
<td>Refine user: None Refine info: None</td>
<td>Filter user: None Filter info: None Filter Event info: None Filter Event Source: None</td>
<td></td>
</tr>
</tbody>
</table>
Refine Criteria - Category

This option helps you to get the results based on the selected category.

EXPLORER CRITERIA

REPORT TITLE: Login Failure

- Metadata
- Advanced Search
- Category
- SQL Query

Total log count: 13,404

SELECT CATEGORY

SYSTEMS

- MCLUDON-11
- All

From: 11/30/2015 02:34:30 PM   To: 12/01/2015 02:34:30 PM

Limit to time range

SEARCH  NEW SEARCH  CLOSE

SEARCH CRITERIA

<table>
<thead>
<tr>
<th>TIME RANGE</th>
<th>SYSTEMS</th>
<th>REFINE</th>
<th>FILTER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Start time: 11/30/2015 2:34:30 PM  
End time: 12/1/2015 2:34:30 PM | *Sites=MCLUDON-11, Groups=TOONS, Systems=ESWINSR01, MCLUDON-11, MCLUDON-11, TOONS\LOCAL, vmses3-win11 | Refine user: None  
Refine info: None | Filter user: None  
Filter info: None  
Filter Event Id(s): None  
Filter Event Source(s): None |
Refine Criteria - SQL Query

This option helps you to get the results based on custom SQL query. Users are given an option to form their own SQL query based on the event properties.

Your result based on the custom query i.e. "EventId=9001" will be listed.
Configure EventVault Explorer to use remote SQL Server

The SQL Server Express Edition has maximum database size limitation of 4 GB. Hence, to overcome this limitation an option is provided to use Remote SQL Server, which can be SQL Server Enterprise Full Edition. Unlike SQL Server Express edition, SQL Server Enterprise Edition does not have any size limitation.

Before you begin, read the below points carefully.

NOTE:

- MS SQL Server Enterprise 2005/2008/2012 is supported.
- For best performance the instance of MS SQL server Enterprise should be dedicated for this usage.
- The MS SQL server instance should be accessible from the EventTracker server, preferably via fully qualified domain name (FQDN).
- Window's authentication is used for connecting to the MS SQL server.

For successful configuration, follow the steps given below:
In SQL Server system

- Grant user (User used for EventTracker configuration) Sysadmin access on remote SQL server.
- Create folder on remote SQL server system to store EventVault Explorer database file and give user (User used for EventTracker configuration) full access on folder created on remote system.

In EventTracker server

1. Click the **Reports** menu, and then click on **Explorer**.
   The **EventVault Explorer** window will appear on the screen.

2. Click **Configuration** hyperlink.
   **EventVault Explorer Configuration** dialog box appears on the screen.
3. Select **SQL Server Enterprise** option.
   This enables the EventVault Explorer to use the SQL Server Database.

4. Enter host server name in **Host Server Name:** box.
   Host Server name might be remote system's address or IP address of SQL server.
   Example: mcloon.Toons.local

5. Enter SQL server instance name in **SQL Server Instance Name:** box.
   If a specific instance name was provided while installing SQL server, then provide the same name here.

6. Enter database path in **Database path:** box.
   For example, D:\EventVaultD
   This database path should be on SQL server system.
7. To authenticate the SQL server database connection, click the **Test Connection** button.

8. Enter any number in **Max history count** box.

   Max history count is the number of searches performed on cache databases, which can be active at any given point of time. A new search cannot be performed once it exceeds the max history count.

9. To save the configuration, click the **Save** button.

10. Change EventTracker Reporter service logon account to the User account (**ET Admin**) which has permission on Remote SQL server.

    Follow the steps given below to enable **ET Admin** user account.

    a. Enter **services.msc** command in **Run** dialog box.
b. In Services window, select EventTracker Reporter.

![EventTracker Reporter](image)

Figure 21

c. Select Log On tab, select This account option, and then type 'TOONS\ET Admin'
d. Click the **Apply** button, and then click the **OK** button.