

Reading SQL DB Trace Files Using Direct Log Archiver

Configuration Guide

Abstract

The purpose of this document is to help users configure EventTracker Direct Log Archiver to read SQL DB trace files.

Target Audience

- Users of EventTracker v7.x who wish to configure DLA to read SQL DB trace files
- Technical evaluator of EventTracker who seeks to understand how the feature is implemented

The information contained in this document represents the current view of Prism Microsystems, Inc. on the issues discussed as of the date of publication. Because Prism Microsystems, Inc. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, Inc. and Prism Microsystems, Inc. cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems, Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this Guide may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, Inc. the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2013 Prism Microsystems, Inc. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

SQL Trace file	3
Advantages of SQL Trace Files	3
How Reading SQL DB Trace is Implemented in EventTracker	4
Move Trace Files to EventTracker Manager System	4
How to Use Direct Log Archiver	5
Create VCP Port for DLA.....	5
Associate the VCP Port with DLA.....	5
Configure DLA	5
Search DLA Events	10

SQL Trace file

Default trace file provides troubleshooting assistance to database administrators by ensuring that they have the log data necessary to diagnose problems the first time they occur. Trace files are usually located in the default install directory, for example, ...\\Program Files\\Microsoft SQL Server\\MSSQL10.MSSQLSERVER\\MSSQL\\Log\\log_xxx.trc

Advantages of SQL Trace Files

- Default trace can be queried to find
- DDL changes at Database, Schema and Object level
- Configuration changes at SQL Server Instance, Database, Schema and Object Level
- Login creation, modifications, and failures
- Performance issues
- Database file growth or shrinkage
- DBCC operations

How Reading SQL DB Trace is Implemented in EventTracker

A SQL Trace file contains trace information of a SQL server instance (applicable to all database instances) and the contents are not plain text, but a binary dump.

EventTracker DLA,

- Reads these files with the use of in-built SQL stored procedures, by importing them into a temporary table in EventTrackerData database
- Extracts necessary columns
- Frames the event and insert into cache mdb maintained for DLA events Per system DLA configuration is required if trace files are transferred from multiple SQL systems.

For more information on Direct Log Archiver, refer

<http://www.eventtracker.com/wp-content/uploads/2013/01/EventTracker-v7.0-Enterprise-Direct-Log-Archiver.pdf>

Move Trace Files to EventTracker Manager System

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

- Manually move log files to the target location.
- 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.
- Upload log files through FTP.
- Configure EventTracker Agent – File Transfer (Other files) facility to transfer log files at scheduled interval or On Demand. Store files from different systems respectively under ...\\Prism Microsystems\\EventTracker\\DLA\\SystemName folder.

For more information on Agent DLA, refer

<http://www.eventtracker.com/wp-content/uploads/2013/01/EventTracker-v7.0-Enterprise-Agent-DLA.pdf>

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

How to Use Direct Log Archiver

On the EventTracker Manager System,

- Create VCP Port for DLA
- Associate the VCP Port with DLA
- Configure DLA
- Run a log search / analysis to view the processed events.

Create VCP Port for DLA

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. Click **Add** under Virtual Collection Points. EventTracker displays the Receiver Port pop-up window.
6. Type the port number and a brief description, for example, 14515, DLA respectively in the **Port Number** and **Description** fields.
7. Click **Save**. EventTracker adds the port to the Virtual Collection Points pool.
8. Click **Save** on the Manager Configuration page.

Associate the VCP Port with DLA

1. Click the **Direct Log Archiver / NetFlow Receiver** tab.
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. Click **Add**.
EventTracker displays the Direct Archiver Configuration pop-up window.
2. Select the log file extension as "TRC" from the **Type** drop-down list.

3. Type the name of the configuration file with extension in the **Configuration Name** field. Direct Log Archiver creates an ini file with the name you provide.
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: 1 Direct Archiver Configuration

5. Click **Configure**.
EventTracker displays Direct Archiver Configuration window with more configuration options.

The screenshot shows the 'Direct Archiver Configuration' window. It features a 'Log file configuration' section with the following fields and controls:

- Configuration Name:** C:\Program Files\Prism Microsystems\EventTracker\
- Log Source:** (Empty text box)
- Computer Name:** (Empty text box)
- Computer IP:** (Empty text box) with a **Get IP** button to its right.
- System Type:** Unknown (Dropdown menu)
- System Description:** (Empty text box)
- Comment Line Token:** (Empty text box)
- Description Format:** Two radio buttons: 'Entire Row as Description' (selected) and 'Formatted Description'.
- Log File Format:** (Empty dropdown menu)
- Message Fields:** (Empty text box) with an **Add** button to its right.
- Message Fields List:** (Empty list box) with a **Remove** button to its right.
- Select Event Date and Time Fields:** A sub-section containing:
 - No of Fields:** (Empty dropdown menu)
 - Date Field:** (Empty dropdown menu)
 - Time Field:** (Empty dropdown menu)

At the bottom of the window are three buttons: **<< Back**, **Save & Close**, and **Cancel**.

Figure 2

Section	Description
Configuration Name	Name of the log file configuration
Log Source	Source of the logs
Computer Name	Name of the computer from where the logs originated
Computer IP	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.
System Type	Select the operating system of the computer.
System Description	Type the system description. The description should be informative for future reference
Comment Line Token	Type the character that is used to comment a line. Direct Log Archiver will ignore these comments

6. Enter/select appropriately in the relevant fields.

Direct Archiver Configuration

Log file configuration

Configuration Name: C:\Program Files\Prism Microsystems\EventTracker\

Log Source: SQLDBLOGS

Computer Name: ESXWEBDOC

Computer IP: 192.168.1.24

System Type: Windows 2003 - Server

System Description: SQL Server

Comment Line Token:

Entire Row as Description Formatted Description

Log File Format:

Message Fields:

Select Event Date and Time Fields

No of Fields:

Date Field:

Time Field:

Figure 3

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

The screenshot shows the 'Manager Configuration' window in EventTracker. The 'Direct Log Archiver / Netflow Receiver' tab is active. Under 'Direct Log Archiver', the 'Direct log file archiving from external sources' checkbox is checked. The 'Purge files after' is set to 0 days, and the 'Associated virtual collection point' is set to 14515. A table lists the log file configuration:

Log file Folder	Configuration Name	Log file Extension	Field Separator	Log Type
C:\Program Files\Prism Microsystems\EventTracker\DLA\ESXWEBDOC	SQLDBTrace	TRC		

Below this, the 'Netflow Receiver' section has the 'Enable Netflow Receiver' checkbox unchecked. The 'Netflow Data Storage Folder' is set to C:\Program Files\Prism Microsystems\EventTracker\DLA\Netflow. A table lists the port configurations:

Port Number	Drop Rate	Decode Packet	Record Binary
9991	0	Yes	No
9992	0	Yes	No

At the bottom, the status bar shows 'Server Time: 11/03 02:16:55 PM' and 'Response: 0.203 secs'.

Figure 4

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

EventTracker creates a DLA system instance with the computer name you have provided.

The screenshot shows the 'System Tools' window in EventTracker. A search bar is present, and the systems are sorted by Name. The page size is set to 25. A table lists the discovered systems:

Computer	Type	EventTracker Port	EventTracker Status	Change Audit Status	Asset value
ALICE-II	Windows XP Pro	-	Unmanaged	Unmanaged	Low
BALOO	Windows 2000 - Professional	-	Unmanaged	Unmanaged	Low
CHARLIE-II	Windows XP Pro	-	Unmanaged	Unmanaged	Low
DONALD-II	Windows 2003 - Server	-	Unmanaged	Unmanaged	High
ESXWCSEVER	Windows 2003 - Server	-	Unmanaged	Unmanaged	High
ESXWEBDOC	Windows 2003 - Server	14505	Agent	Agent	High
ESXWEBDOC-DLA	Windows 2003 - Server	14505	Agent	Unmanaged	High
ESXWIN2K3VM4	Windows 2003 - Server	-	Unmanaged	Unmanaged	High
ESXWIN2K3VM5	Windows 2003 - Server	-	Unmanaged	Unmanaged	High
ESXWIN2K3VM6	Windows 2003 - Server	-	Unmanaged	Unmanaged	High
ESXWIN2K864VM2	Windows Server 2008	-	Unmanaged	Unmanaged	High
ESXWIN2K864VM3	Windows Server 2008	-	Unmanaged	Unmanaged	High

The 'ESXWEBDOC-DLA' system is highlighted with a red box. The status bar at the bottom shows 'Server Time: 11/03 02:19:07 PM' and 'Response: 0.328 secs'.

Figure 5

Search DLA Events

1. Log on to EventTracker.
2. Click the **Search** hyperlink at the upper-right corner. EventTracker opens the Log Search browser.
3. Click the **Advanced Search** hyperlink.
4. Set the search criteria. For example, type the source as you have provided in the DLA configuration in the **search in standard and/or custom column(s)** field and select the DLA system.

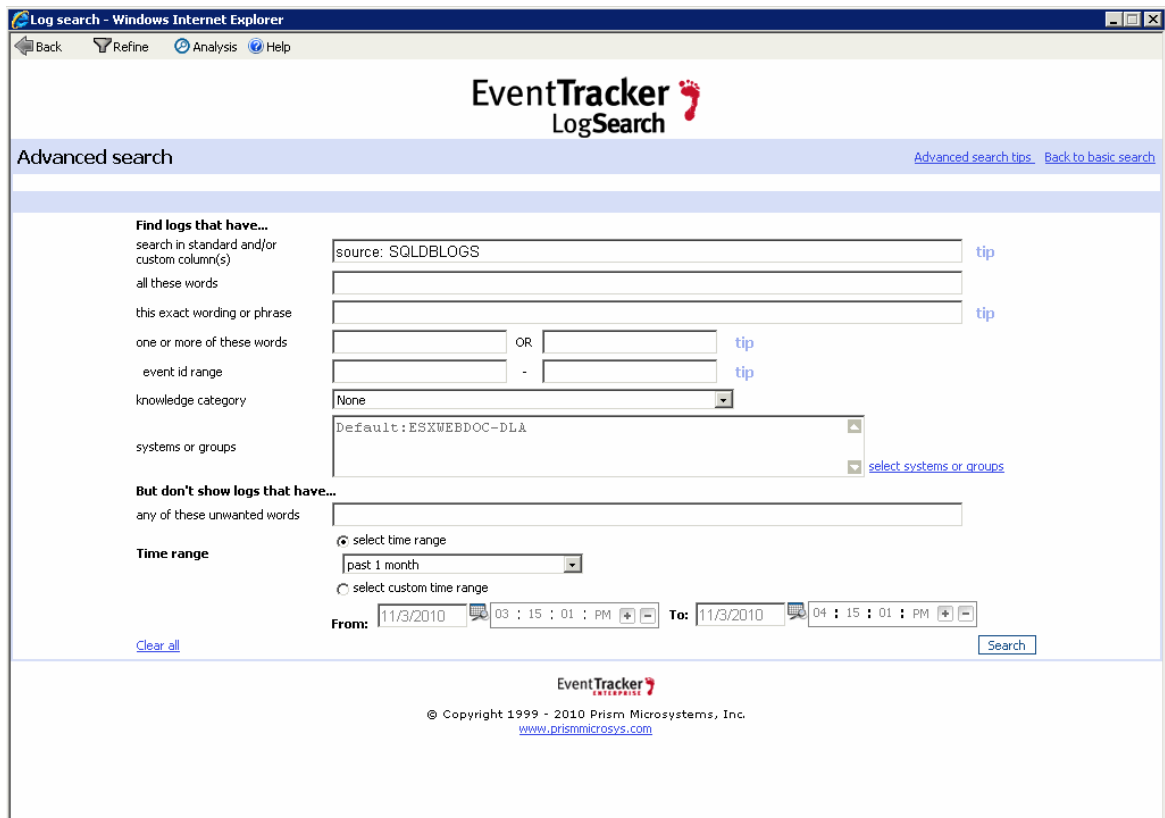


Figure 6

5. Click **Search**. Log Search Utility displays the search result.

Log search - Windows Internet Explorer			
Total event count: 46,317			
ID	Log Time	Event Properties	Event Description
1	11/3/2010 01:55:15 PM	Event ID: 3230 Log Type: System Event Type: Information Category: 2 Source: SQLDBLOGS Domain: NT AUTHORITY Computer: ESXWEBDOC-DLA User: SYSTEM	DatabaseID: 5, TransactionID: 1619455, NTUserName: nirmal, NTDomainName: TOONS, HostName: ESXWEBDOC, ClientProcessID: 2908, ApplicationName: Internet Information Services, LoginName: TOONS\nirmal, SPID: 97, StartTime: 2010-11-03 13:55:15, EventSubClass: 1 (Commit), ObjectID: 1718297181, IndexID: NULL, IntegerData: NULL, ServerName: ESXWEBDOC\SQLEXPRESS, EventClass: 46 (Object:Created, Objects), ObjectType: 21587 (Statistics), ObjectName: NULL, DatabaseName: EventTracker, LoginSid: 0x010500000000000515000000A543D835526DC9737D58C6A264040000, RequestID: 0, XactSequence: 416611827713, EventSequence: 1333438, BigintData1: NULL, ObjectID2: NULL, IsSystem: NULL, SessionLoginName: TOONS\nirmal
2	11/3/2010 01:55:15 PM	Event ID: 3230 Log Type: System Event Type: Information Category: 2 Source: SQLDBLOGS Domain: NT AUTHORITY Computer: ESXWEBDOC-DLA User: SYSTEM	DatabaseID: 5, TransactionID: 1619455, NTUserName: nirmal, NTDomainName: TOONS, HostName: ESXWEBDOC, ClientProcessID: 2908, ApplicationName: Internet Information Services, LoginName: TOONS\nirmal, SPID: 97, StartTime: 2010-11-03 13:55:15, EventSubClass: 0 (Begin), ObjectID: 1718297181, IndexID: 3, IntegerData: NULL, ServerName: ESXWEBDOC\SQLEXPRESS, EventClass: 46 (Object:Created, Objects), ObjectType: 21587 (Statistics), ObjectName: _WA_Sys_00000005_6668225D, DatabaseName: EventTracker, LoginSid: 0x010500000000000515000000A543D835526DC9737D58C6A264040000, RequestID: 0, XactSequence: 416611827713, EventSequence: 1333438, BigintData1: NULL, ObjectID2: NULL, IsSystem: NULL, SessionLoginName: TOONS\nirmal
3	11/3/2010 01:54:34 PM	Event ID: 3230 Log Type: System Event Type: Information Category: 2 Source: SQLDBLOGS Domain: NT AUTHORITY Computer: ESXWEBDOC-DLA User: SYSTEM	DatabaseID: 6, TransactionID: 1619272, NTUserName: SYSTEM, NTDomainName: NT AUTHORITY, HostName: NULL, ClientProcessID: 1324, ApplicationName: NULL, LoginName: NT AUTHORITY\SYSTEM, SPID: 85, StartTime: 2010-11-03 13:54:34, EventSubClass: 0 (Begin), ObjectID: 1422628111, IndexID: 2, IntegerData: NULL, ServerName: ESXWEBDOC\SQLEXPRESS, EventClass: 46 (Object:Created, Objects), ObjectType: 21587 (Statistics), ObjectName: _WA_Sys_00000002_54CB950F, DatabaseName: EventTrackerData, LoginSid: 0x010100000000000512000000, RequestID: 0, XactSequence: 365072220167, EventSequence: 1333389, BigintData1: NULL, ObjectID2: NULL, IsSystem: NULL, SessionLoginName: NT AUTHORITY\SYSTEM
4	11/3/2010 01:54:34 PM	Event ID: 3230 Log Type: System Event Type: Information Category: 2 Source: SQLDBLOGS Domain: NT AUTHORITY	DatabaseID: 6, TransactionID: 1619220, NTUserName: SYSTEM, NTDomainName: NT AUTHORITY, HostName: NULL, ClientProcessID: 1324, ApplicationName: NULL, LoginName: NT AUTHORITY\SYSTEM, SPID: 85, StartTime: 2010-11-03 13:54:34, EventSubClass: 0 (Begin), ObjectID: 1518628453, IndexID: 2, IntegerData: NULL, ServerName: ESXWEBDOC\SQLEXPRESS, EventClass: 46 (Object:Created, Objects), ObjectType: 21587 (Statistics), ObjectName: _WA_Sys_00000002_5A8466E5, DatabaseName: EventTrackerData, LoginSid: 0x010100000000000512000000, RequestID: 0, XactSequence: 365072220161, EventSequence: 1333380, BigintData1: NULL, ObjectID2: NULL, IsSystem: NULL, SessionLoginName: NT AUTHORITY\SYSTEM

Search results for: source: SQLDBLOGS, Time range: Last 1 Month

◀ Previous Next ▶ Stop 🔍 New search Page: 1

Figure 7