EventTracker
Secure. Comply. Succeed.

Reading SQL DB Trace Files Using Direct Log Archiver

Configuration Guide

Publication Date: Nov 19, 2012

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

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

Table of Contents

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.

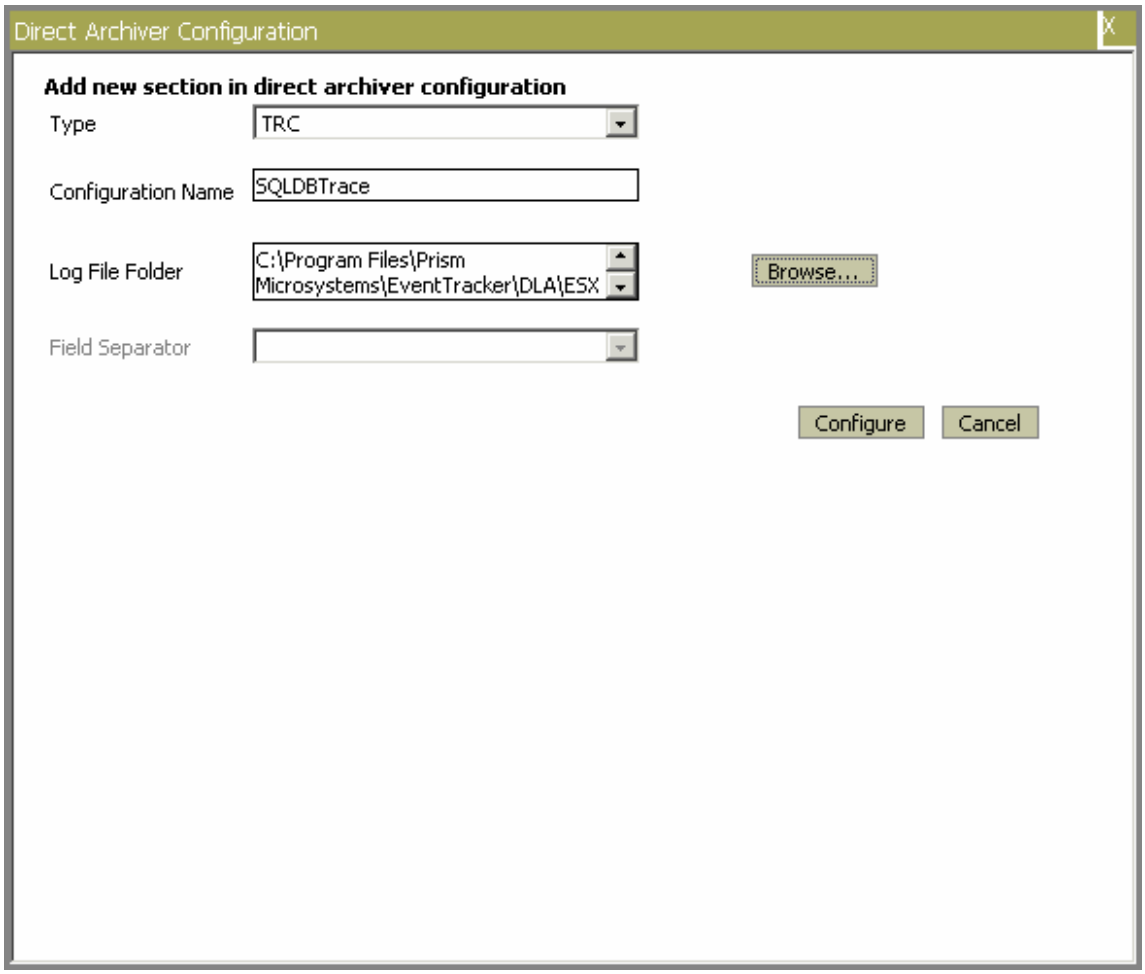

Figure: 1 Direct Archiver Configuration

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

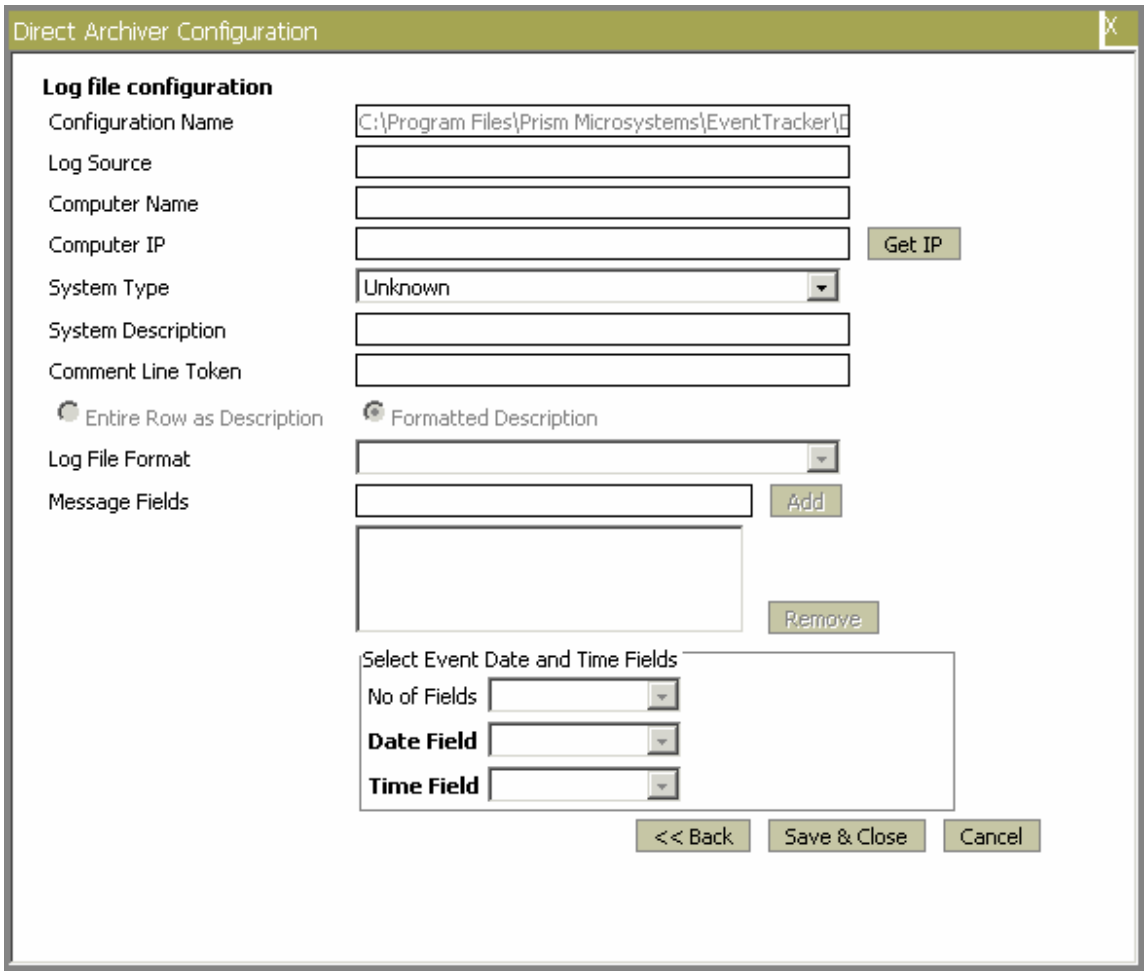

Figure 2

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.

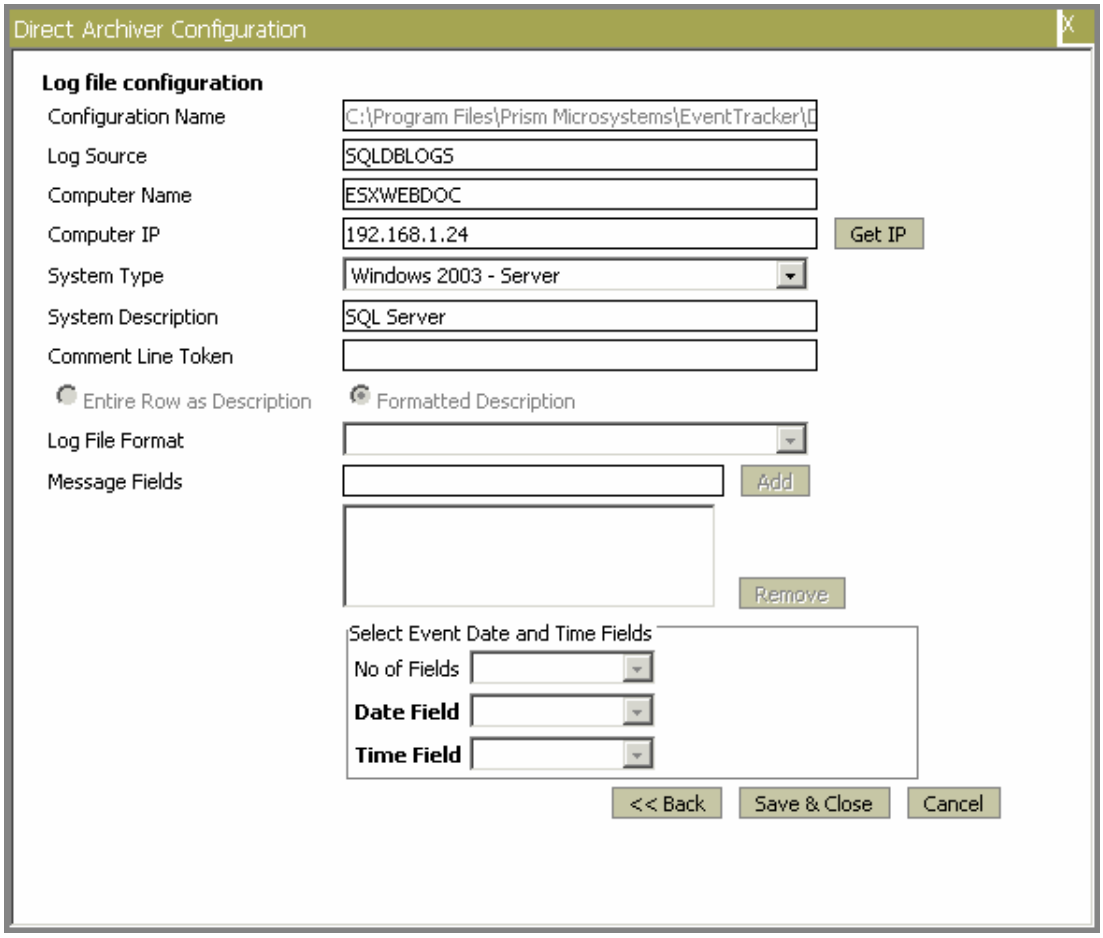

Figure 3

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

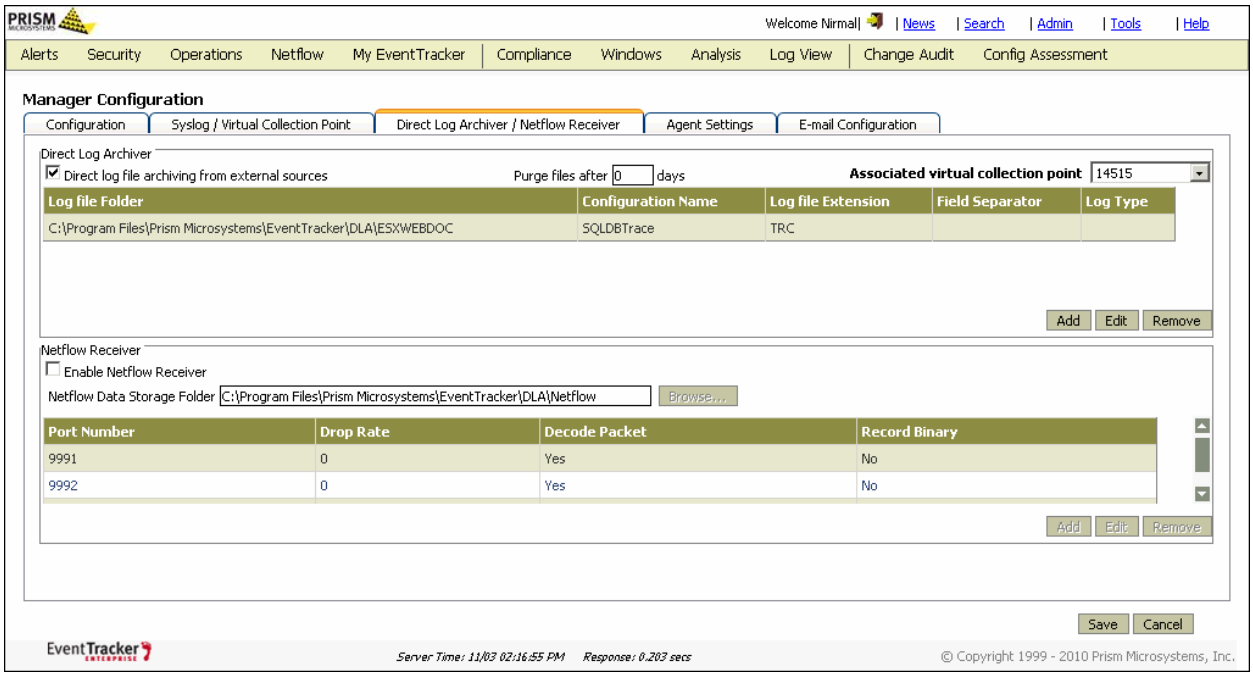

Figure 4

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.

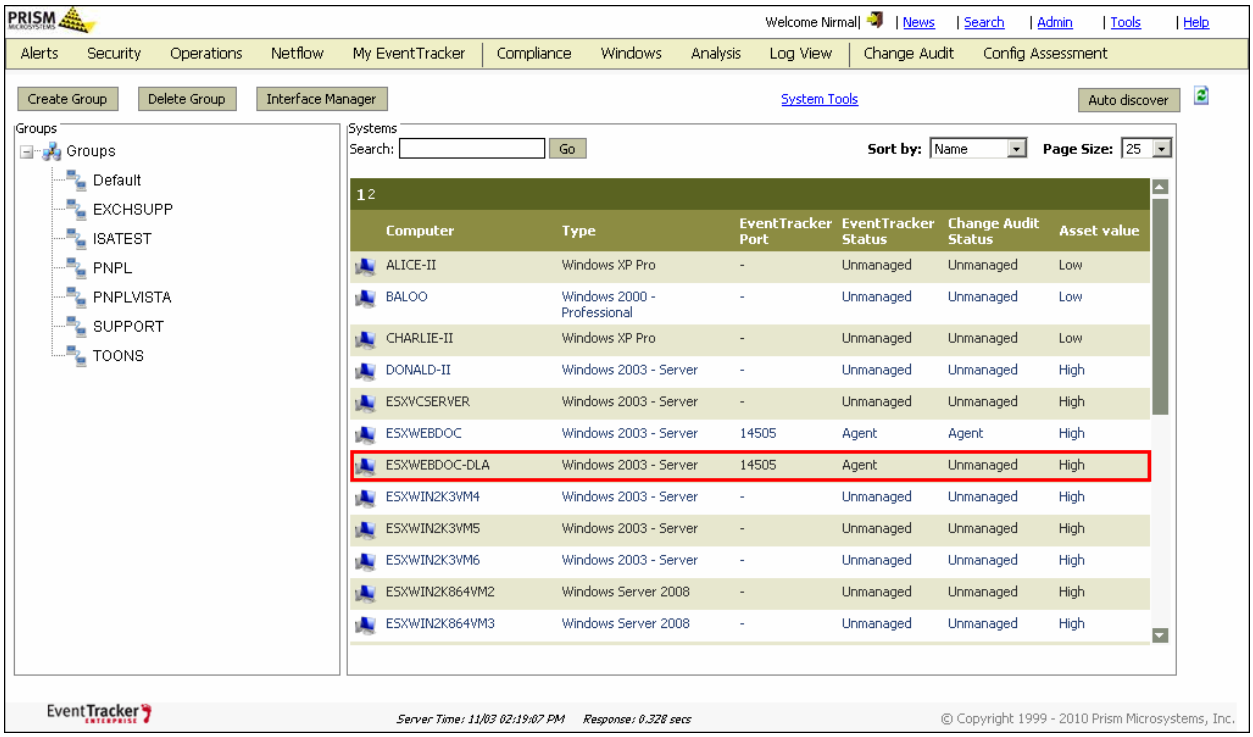

Figure 5

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.

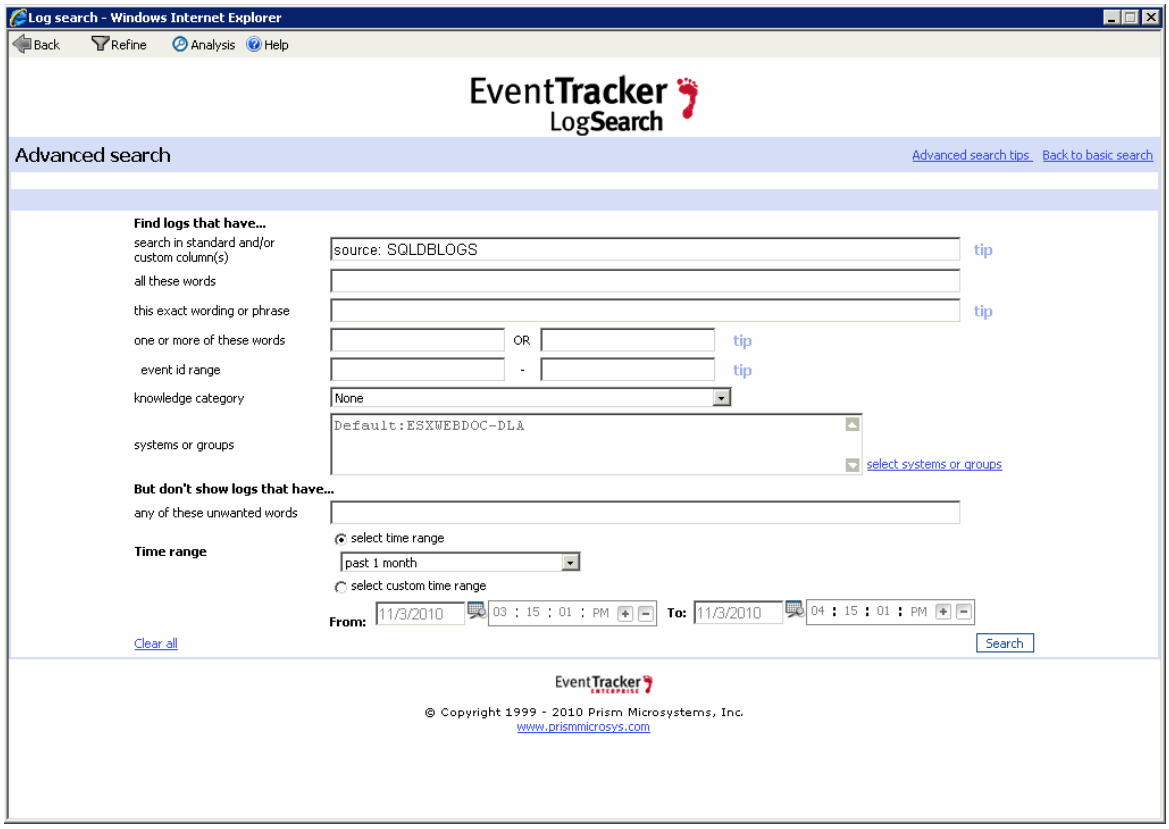

Figure 6

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

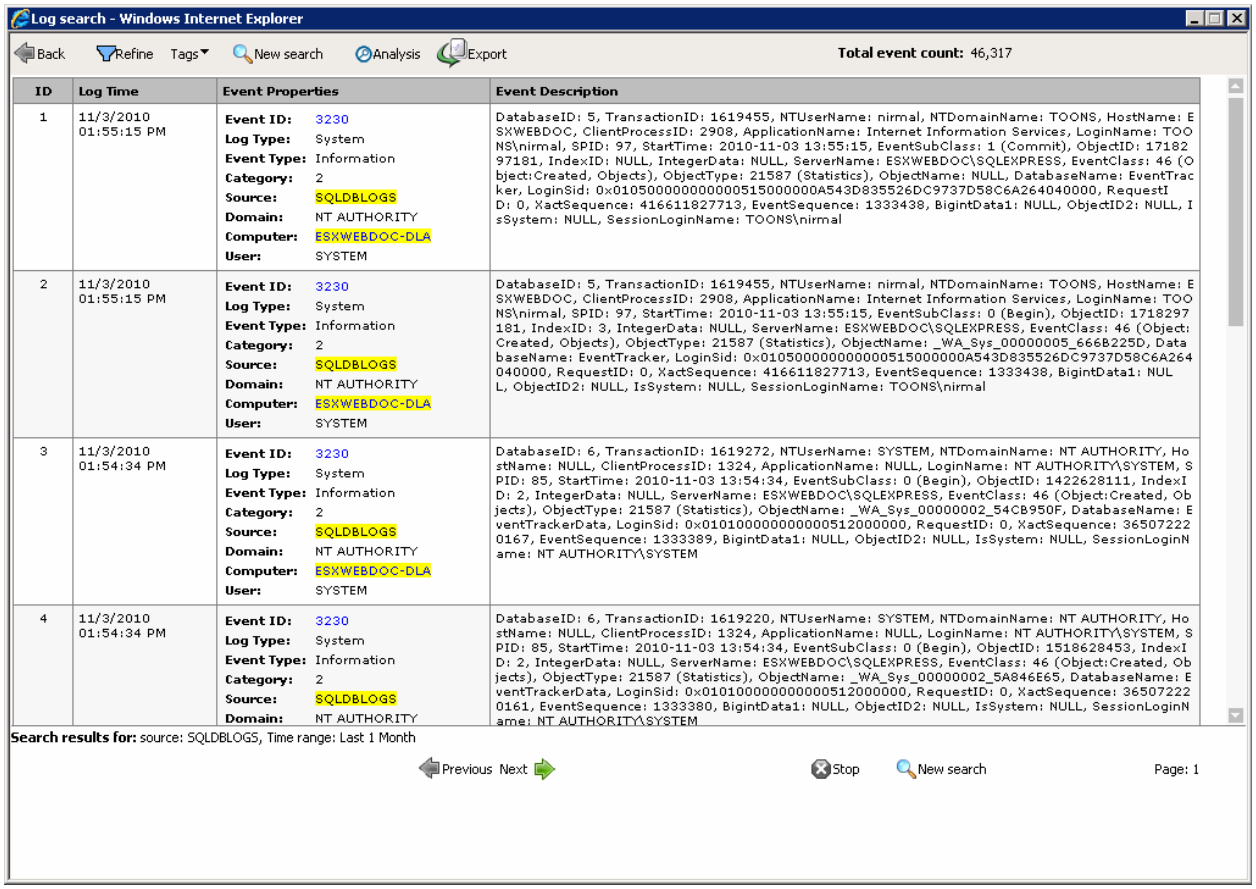
Log search - Windows Internet Explorer
Back
Refine
Tags
New search
Analysis
Export
Total event count: 46,317
ID
Log Time
Event Properties
Event Description
1
11/3/2010 01:55:15 PM
Event ID: 3230
Log Type: System
Event Type: Information
Category: 2
Source: SQLDBLOGS
Domain: NT AUTHORITY
Computer: ESXWEBDOC-DLA
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: 0x0105000000000005150000000A543D835526DC9737D58C6A264040000, 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_666B225D, DatabaseName: EventTracker, LoginSid: 0x0105000000000005150000000A543D835526DC9737D58C6A264040000, 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_5A846E65, 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