

Integrate Teradata Database Server

EventTracker

About the document

This guide provides instructions to configure Teradata Database Server to send the event logs to EventTracker Enterprise.

Intended audience

Teradata Database Server Administrators, who wish to forward syslog events to EventTracker Manager.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise version 7.X** or later, and **Teradata Database Server 12** or later.

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 must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems 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 paper 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 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, 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 Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

- About the document 1
- Intended audience..... 1
- Scope 1
- Pre-requisite..... 3
- Overview..... 3
- Enable logging to Database Server..... 3
- Schedule Bteq Scripts on Teradata Database 4
 - For Access Log..... 4
 - Configure Teradata Database to send logs to EventTracker..... 5
 - For Event Log..... 8
 - Configure Teradata Database to send event logs to EventTracker 9
 - For Database Query Log (DBQL) 12
 - Configure Teradata Database to send DBQ logs to EventTracker 13
- Verify Teradata Database Server knowledge pack in EventTracker 16
- Sample Analysis Report..... 17
 - Teradata-Audit Setting Changes Report..... 17
 - User Selection 17
 - Detail1 17
 - Teradata Authentication Success Report 19
 - User Selection 19
 - Detail1 19

Pre-requisite

- EventTracker should be installed.
- Teradata Database Server 12 (or later) should be installed.

Overview

In order to monitor Teradata Database 12 or later in EventTracker, you need to perform all the steps as below.

- Enable **Logging** on **Teradata Database Server**.
- Schedule **Bteq** scripts on **Teradata Database Server**.
- Verify **Teradata Database Server** Knowledge Pack in **EventTracker**.

Enable logging to Database Server

- 1 Launch **Teradata Database**.
- 2 Run the **Begin Logging** and **Begin Query Logging** query to enable logging on Teradata.

The query for **Begin Logging** is

BEGIN LOGGING WITH TEXT ON ALL

The query for **Begin Query Logging** is

BEGIN QUERY LOGGING ON ALL

NOTE:

You can use these two queries in different ways on different objects using various keywords and clauses for user specific outputs. For more information on the syntax of these queries, refer to the following link

http://www.coffingdw.com/Teradata_DBA/teradata_dba/chapter_6___query_analysis_and_tools/begin_logging_statement.htm

Schedule Bteq Scripts on Teradata Database

There are three types of logs that can be generated from Teradata Database Server using **Bteq** scripts. They are as follows:

- Access Logs.
- Event Logs.
- Database Query Logs (DBQL)

The following scripts need to be scheduled on Teradata Database Server to extract required data.

For Access Log

```
.LOGON dbc, dbc  
  
database dbc;  
  
.SET WIDTH 3500;  
  
.SET TITLEDASHES OFF;  
  
.SET FORMAT OFF;  
  
.SET FOLDLINE OFF;  
  
.SET SEPARATOR ";;"  
  
.EXPORT REPORT FILE=Reportoutput.csv
```

```
Select LogonDate,LogonTime,TheDate,TheTime,(cast (LogicalHostID as smallint)),(cast (IFPNo as smallint)),(cast (SessionNo as integer)),(cast (UserId as byte(4))),(cast (UserName as varchar(40))),(cast (AccountName as varchar(100))),(cast (AccLogResult as character(1))),SeqInHash,(cast (AccessType as character(2))),(cast (Accesskind as byteint)),(cast (Frequency as character(1))),EventCount,(cast (OwnerName as varchar(40))),(cast
```

```
(DatabaseName as varchar(40)),(cast (TVMName as varchar(120)),(cast (ColumnName as
varchar(120)),(cast (ObjectLevel as character(1)),(cast (ObjectId as byte(4)),(cast (ColumnId as
smallint)),(cast (StatementKind as smallint)),(cast (StatementType as varchar(120)),(cast
(StatementText as varchar(550)),(cast (QueryBand as varchar(550)),(cast (ProxyUser as
varchar(60)),(cast (ConstraintId as byte(4)) from dbc.acclgtbl where LogonDate=Current_Date-
1;
```

.EXPORT RESET

.Quit

.Logoff

Configure Teradata Database to send logs to EventTracker

Transferring Teradata database logs to EventTracker server or by scheduling a task.

1. Create a log folder on any drive and transfer the logs manually.
2. In EventTracker Enterprise, click the **Admin** drop-down, select **Manager**.
3. Select **Direct Log Archiver/Netflow Receiver** tab.

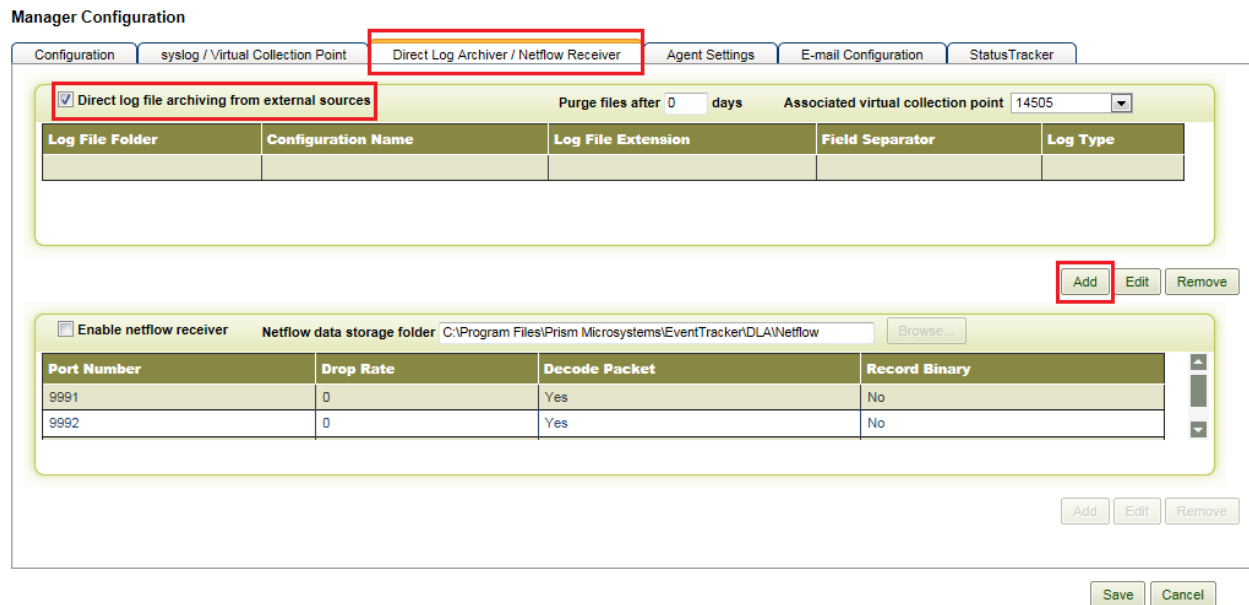


Figure 1

4. Select **Direct log file archiving from external resources** option.

5. Click the **Add** button.

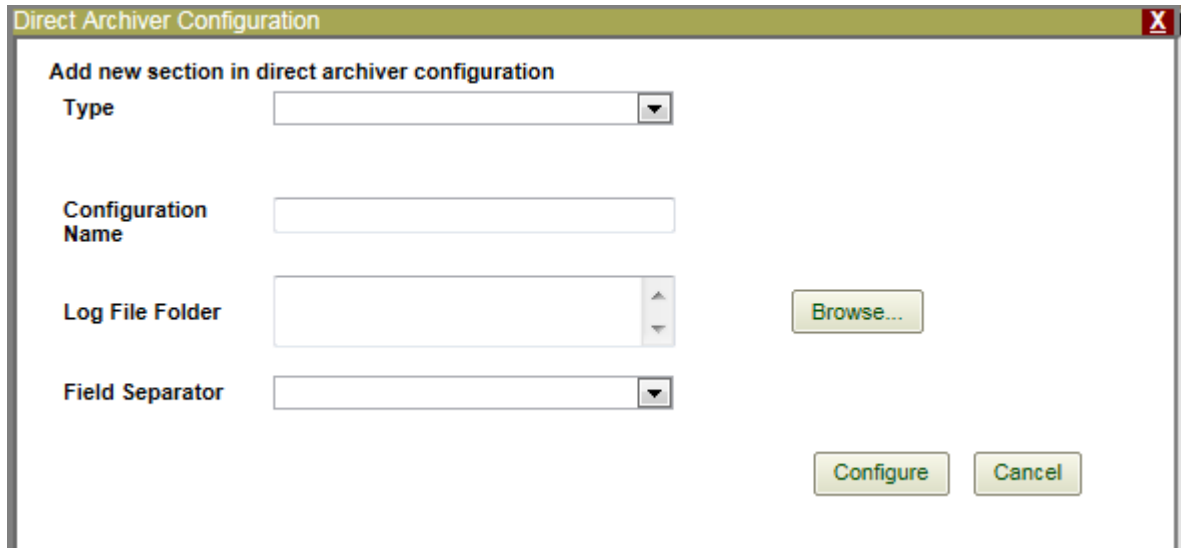


Figure 2

6. Select/enter the appropriate fields. Enter the correct path of the **Log File Folder**.

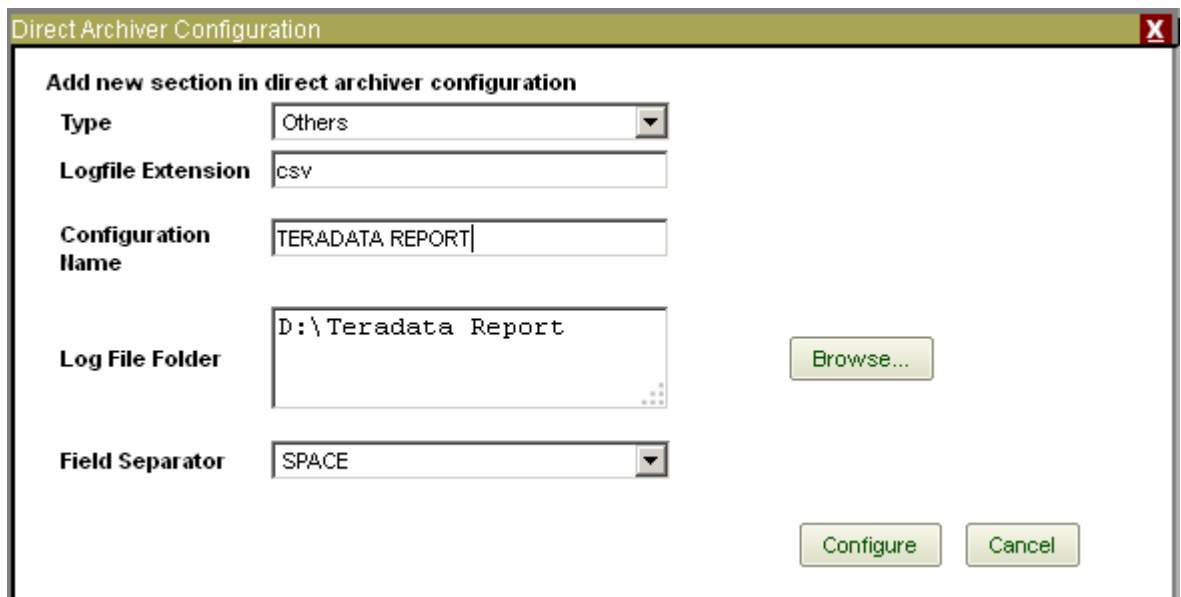


Figure 3

7. Click **Configure**.
8. Select/enter the appropriate fields.

The screenshot shows a window titled "Direct Archiver Configuration" with a close button (X) in the top right corner. The window is divided into several sections:

- Log file configuration**
 - Configuration Name:** D:\Teradata Report\TERADATA REPORT
 - Log Source:** Report Log
 - Computer Name:** SAFARI
 - Computer IP:** 192.168.1.17 (with a "Get IP" button to the right)
 - System Type:** Win 7 (dropdown menu)
 - System Description:** TERADATA Database
 - Comment Line Token:** (empty text field)
- Description Options:**
 - Entire Row as Description
 - Formatted Description
- Log File Format:** Custom Log File Format (dropdown menu)
- Message Fields:**
 - (empty text field) with an "Add" button to the right.
 - A list box containing: Time, Logical Host ID, IFP No, Session ID. To the right of the list box is a "Remove" button.
- Select Event Date and Time Fields:** (highlighted box)
 - No of Fields:** 2 (dropdown menu)
 - Date Field:** Logon Date (dropdown menu)
 - Time Field:** Logon Date (dropdown menu)

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

Figure 4

9. Click **Save &Close** button.

For Event Log

```
.LOGON dbc,dbc
```

```
database dbc;
```

```
.SET WIDTH 3500;
```

```
.SET TITLEDASHES OFF;
```

```
.SET FORMAT OFF;
```

```
.SET FOLDLINE OFF;
```

```
.SET SEPARATOR ',';
```

```
.EXPORT REPORT FILE=eventlog.csv
```

```
Select DateFld,TimeFld,(cast (UserName as varchar(40))),(cast (AccountName as  
varchar(40)),(cast (Event as character(12))),(cast (SessionNo as  
integer)),logondate,LogonTime,(cast (ClientTcpPortNumber as integer)),(cast (clienttdhostname  
as varchar(40))),(cast (clientsystemuserid as varchar(40))),(cast (Authuser as varchar(200))) from  
dbc.eventlog where DateFld=Current_Date-1;
```

```
.EXPORT RESET
```

```
.Quit
```

```
.Logoff
```

Configure Teradata Database to send event logs to EventTracker

Transferring Teradata database Event logs to EventTracker server or by scheduling a task.

1. Create a log folder on any drive and transfer the logs manually.
2. In EventTracker Enterprise, click the **Admin** drop-down, select **Manager**.
3. Select **Direct Log Archiver/Netflow Receiver** tab.

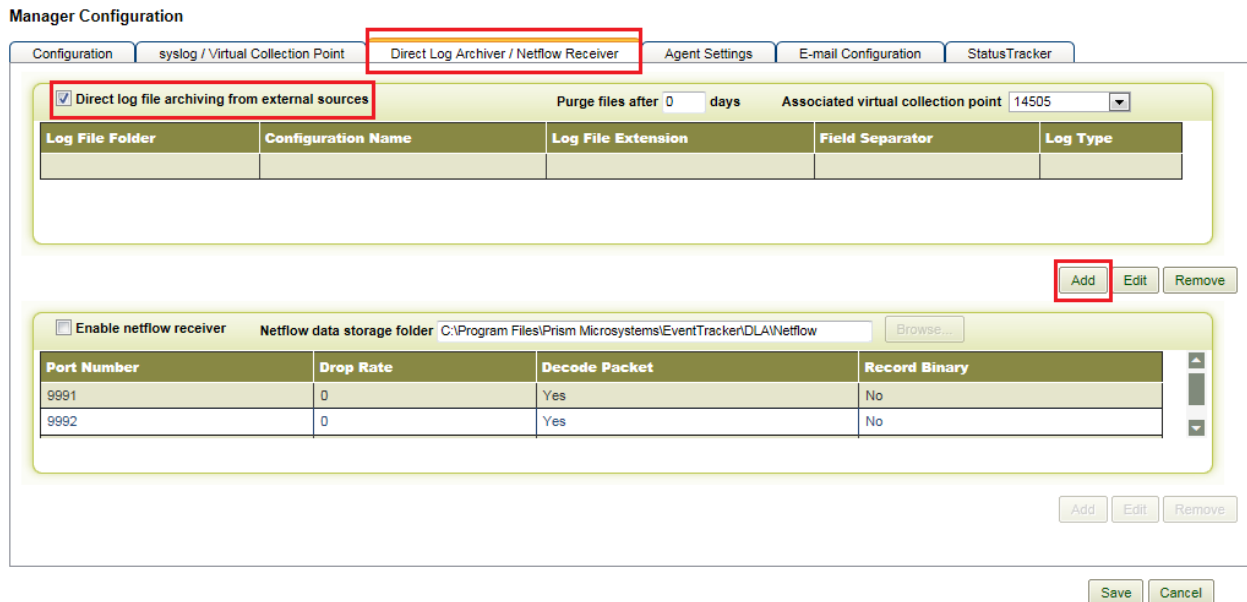


Figure 5

4. Select **Direct log file archiving from external resources** option.
5. Click the **Add** button.

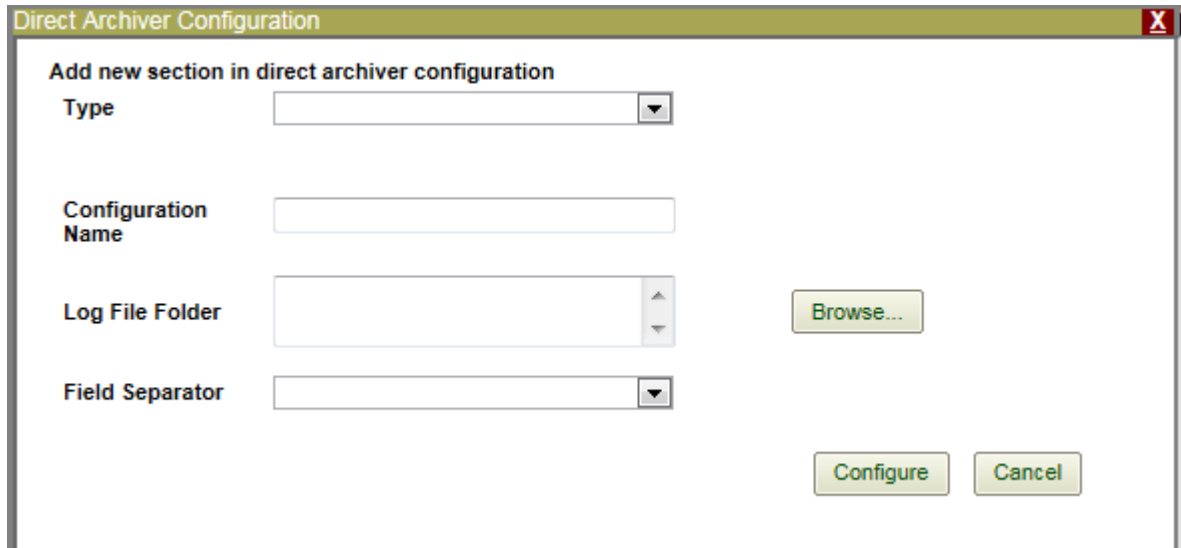


Figure 6

6. Select/enter the appropriate fields. Enter the correct path of the **Log File Folder**.

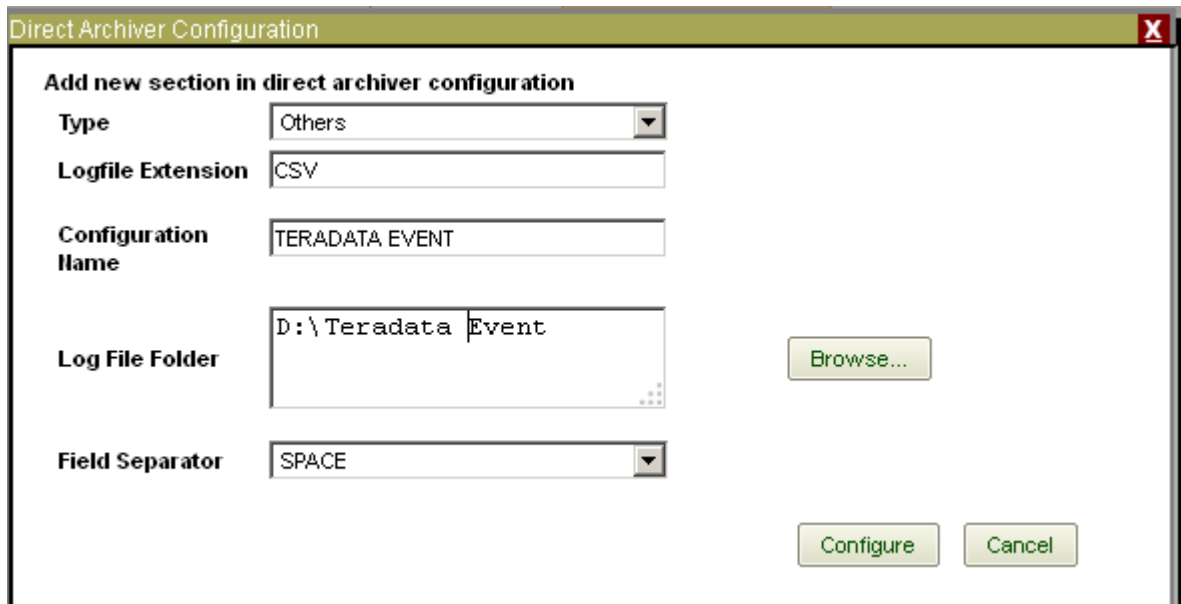


Figure 7

7. Click **Configure**.
8. Select/enter the appropriate fields.

The screenshot shows the 'Direct Archiver Configuration' window. It contains the following fields and controls:

- Log file configuration**
 - Configuration Name:** D:\Teradata\TERADATA
 - Log Source:** EventLog
 - Computer Name:** SAFARI
 - Computer IP:** 192.168.1.17 (with a 'Get IP' button)
 - System Type:** Win 7 (dropdown menu)
 - System Description:** TERADATA Database
 - Comment Line Token:** (empty text box)
- Description Options:**
 - Entire Row as Description
 - Formatted Description
- Log File Format:** Custom Log File Format (dropdown menu)
- Message Fields:**
 - (empty text box) with an 'Add' button
 - Selected fields: Date, Time, User Name, Account Name (list with up/down arrows) with a 'Remove' button
 - Select Event Date and Time Fields:**
 - No of Fields:** 2 (dropdown menu)
 - Date Field:** Date (dropdown menu)
 - Time Field:** Date (dropdown menu)

At the bottom, there are three buttons: '<< Back', 'Save & Close', and 'Cancel'.

Figure 8

9. Click **Save &Close** button.

For Database Query Log (DBQL)

```
.LOGON dbc,dbc
```

```
database dbc;
```

```
.SET WIDTH 3500;
```

```
.SET TITLEDASHES OFF;
```

```
.SET FORMAT OFF;
```

```
.SET FOLDLINE OFF;
```

```
.SET SEPARATOR ";;
```

```
.EXPORT REPORT FILE=dbqllog.csv
```

```
Select (cast (QueryID as decimal(18, 0))),(cast (UserID as byte(4))),(cast (AccString as  
varchar(128))),(cast (ExpandAccString as varchar(128))),(cast (SessionID as integer)),(cast  
(LogonDateTime as timestamp(2))),(cast (StartTime as timestamp(2))),(cast (FirstStepTime as  
timestamp(2))),(cast (FirstRespTime as timestamp(2))),(cast (ErrorCode as integer)),(cast  
(ErrorText as varchar(1024))),(cast (AbortFlag as character(1))),(cast (StatementType as  
character(20))),(cast (QueryText as varchar(10000))),(cast (UserName as varchar(40))),(cast  
(DefaultDatabase as varchar(40))),(cast (StatementGroup as varchar(120))),(cast (KeepFlag as  
character(1))),(cast (QueryRedriven as character(1))) from dbc.dbqllogtbl where  
LogonDateTime=Current_Date-1;
```

```
.EXPORT RESET
```

```
.Quit
```

```
.Logoff
```

Configure Teradata Database to send DBQ logs to EventTracker

Transferring Teradata database DBQ logs to EventTracker server or by scheduling a task.

1. Create a log folder on any drive and transfer the logs manually.
2. In EventTracker Enterprise, click the **Admin** drop-down, select **Manager**.
3. Select **Direct Log Archiver/Netflow Receiver** tab.

Manager Configuration

Configuration syslog / Virtual Collection Point **Direct Log Archiver / Netflow Receiver** Agent Settings E-mail Configuration StatusTracker

Direct log file archiving from external sources Purge files after 0 days Associated virtual collection point 14505

Log File Folder	Configuration Name	Log File Extension	Field Separator	Log Type

Add Edit Remove

Enable netflow receiver Netflow data storage folder C:\Program Files\Prism Microsystems\EventTracker\DLA\Netflow Browse...

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

Add Edit Remove

Save Cancel

Figure 9

4. Select **Direct log file archiving from external resources** option.
5. Click the **Add** button.

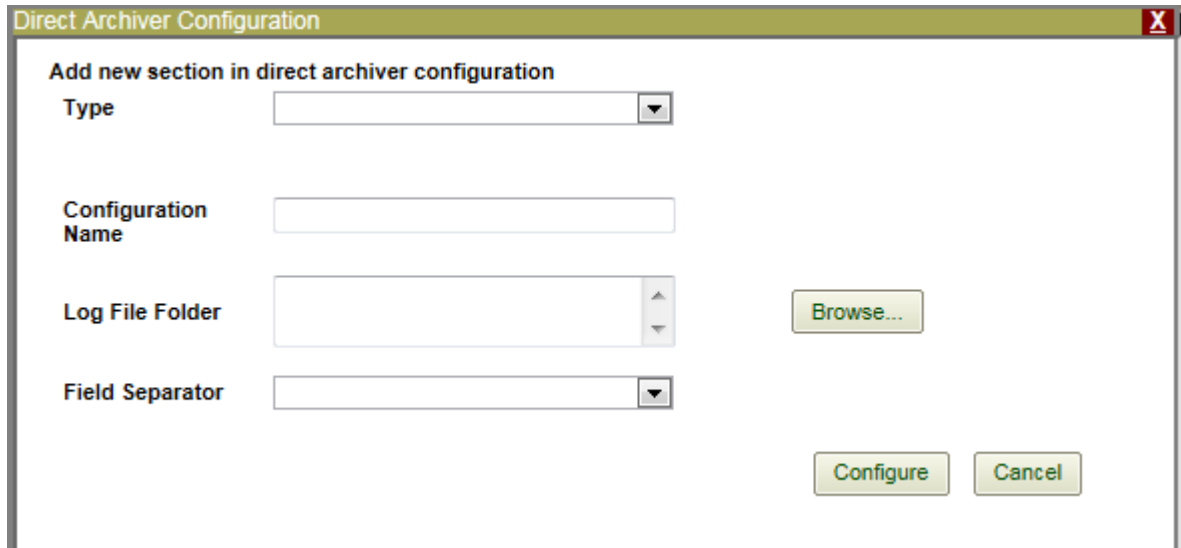


Figure 10

6. Select/enter the appropriate fields. Enter the correct path of the **Log File Folder**.



Figure 11

7. Click **Configure**.
8. Select/enter the appropriate fields.

The screenshot shows the 'Direct Archiver Configuration' window with the following fields and controls:

- Log file configuration**
 - Configuration Name:** D:\Logfiles\TERADATA
 - Log Source:** DBQ Log
 - Computer Name:** SAFARI
 - Computer IP:** 192.168.1.17 (with a 'Get IP' button)
 - System Type:** WIn 7 (dropdown menu)
 - System Description:** TERADATA Database
 - Comment Line Token:** (empty text field)
- Radio Buttons:**
 - Entire Row as Description
 - Formatted Description
- Log File Format:** Custom Log File Format (dropdown menu)
- Message Fields:**
 - (empty text field) with an 'Add' button
 - List of fields: Query ID, User ID, AcctString, ExpandAcctString (with a 'Remove' button)
- Select Event Date and Time Fields:**
 - No of Fields:** 2 (dropdown menu)
 - Date Field:** Query ID (dropdown menu)
 - Time Field:** Query ID (dropdown menu)
- Buttons:** << Back, Save & Close, Cancel

Figure 12

9. Click **Save &Close** button.

Verify Teradata Database Server knowledge pack in EventTracker

1. Logon to Event Tracker Enterprise.
2. Click the **Admin** dropdown, and then click **Category**.
3. In the **Category Tree**, expand **Teradata** group folder to see the categories.

The screenshot displays the 'Category Management' interface in EventTracker. At the top, there is a navigation bar with tabs: Incidents, Status, Behavior, Dashboard, Netflow, Search, Reports, My EventTracker, Change Audit, and Config Assessment. Below this, the 'Category Management' section is active, featuring a 'Category Tree' on the left and a main content area on the right.

The 'Category Tree' on the left shows a hierarchical view with the following categories expanded under 'Teradata':

- Teradata: Audit settings changed
- Teradata: Authentication failure
- Teradata: Authentication success
- Teradata: Database created
- Teradata: Database deleted
- Teradata: Query execution error
- Teradata: Table created
- Teradata: Table deleted
- Teradata: Table modified
- Teradata: User created
- Teradata: User deleted
- Teradata: User password changed
- Teradata: User privilege changed
- Teradata: View information

Other categories visible in the tree include Syslog, Veritas, VMware ESX, and WatchGuard Firebox.

The main content area on the right shows 'Total category groups : 211' and 'Total categories : 2,051'. Below this, a box titled 'Last 10 modified categories' contains a table with the following data:

Name	Modified date	Modified by
Teradata: Audit settings changed	3/21/2013 5:06:48 PM	
Teradata: Authentication failure	3/21/2013 5:06:48 PM	
Teradata: Authentication success	3/21/2013 5:06:48 PM	
Teradata: Database created	3/21/2013 5:06:48 PM	
Teradata: Database deleted	3/21/2013 5:06:48 PM	
Teradata: Query execution error	3/21/2013 5:06:48 PM	
Teradata: Table created	3/21/2013 5:06:48 PM	
Teradata: Table deleted	3/21/2013 5:06:48 PM	
Teradata: Table modified	3/21/2013 5:06:48 PM	
Teradata: User created	3/21/2013 5:06:48 PM	

Figure 13

Sample Analysis Report

Teradata-Audit Setting Changes Report

User Selection

From Date: 12/15/2012 2:44:02 PM

To Date: 3/15/2013 2:44:02 PM

Refine: Match In Event Description = Statement Type: "Begin/End DBQL"

Event ID = 3230

Filter: None

Categories Selected: N/A

Computers Selected: TERADATADBQL-DLA

Description: None

Detail1

LogTime	Database User	DB Account	Error Code	Error	Statement Group	Detailed Query
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"BEGIN QUERY LOGGING ON all;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging with sql on DBC;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging with sql on all;"

03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	dbc;"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"DBC"	"begin query logging on dbc
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"BEGIN QUERY LOGGING ON all;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"0"	"NULL"	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"BEGIN QUERY LOGGING ON all;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"BEGIN QUERY LOGGING WITH SQL ON ALL;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"BEGIN QUERY LOGGING WITH SQL ON ALL;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"Begin query logging on all;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"Begin query logging on all;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"begin query logging on dbc;"
03/12/2013 12:34:20 PM	"DBC"	"DBC"	"3725"	"Statement not allowed for an ANSI session."	"Other"	"BEGIN QUERY LOGGING ON all;"

Teradata Authentication Success Report

User Selection

From Date: 12/15/2012 2:46:31 PM

To Date: 3/15/2013 2:46:31 PM

Limit Time Range: None

Refine: Match In Event Description = Event: Logon

Event ID = 3230

Filter: None

Categories Selected: N/A

Computers Selected: TERADATAEVENTS-DLA

Description: None

Detail1

LogTime	Database User	Database User ID	Authenticated User	Host Name	Database Account
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	TEST	root	TEST	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC

03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC		DBC		DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC

03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC		DBC	DBC	DBC
03/12/2013 12:34:17 PM	DBC	root	DBC	localhost;localhost/127.0.0.1:1025	DBC