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.
# 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

   ```sql
   BEGIN LOGGING WITH TEXT ON ALL
   ```

   The query for **Begin Query Logging** is

   ```sql
   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.
EventTracker - Integrate Teradata Database Server

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))))
```
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.

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

Figure 1
5. Click the **Add** button.

![Figure 2](image.png)

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

![Figure 3](image.png)

7. Click **Configure**.

8. Select/enter the appropriate fields.
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.

4. Select Direct log file archiving from external resources option.
5. Click the Add button.
6. Select/enter the appropriate fields. Enter the correct path of the Log File Folder.

7. Click Configure.
8. Select/enter the appropriate fields.
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=dbqlog.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.dbqlogtbl 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.

4. Select Direct log file archiving from external resources option.
5. Click the Add button.
6. Select/enter the appropriate fields. Enter the correct path of the Log File Folder.

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

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Database User</th>
<th>DB Account</th>
<th>Error Code</th>
<th>Error Description</th>
<th>Statement Group</th>
<th>Detailed Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/12/2013 12:34:20 PM</td>
<td>&quot;DBC&quot;</td>
<td>&quot;DBC&quot;</td>
<td>&quot;3725&quot;</td>
<td>&quot;Statement not allowed for an ANSI session.&quot;</td>
<td>&quot;Other&quot;</td>
<td>&quot;BEGIN QUERY LOGGING ON all;&quot;</td>
</tr>
<tr>
<td>03/12/2013 12:34:20 PM</td>
<td>&quot;DBC&quot;</td>
<td>&quot;DBC&quot;</td>
<td>&quot;3725&quot;</td>
<td>&quot;Statement not allowed for an ANSI session.&quot;</td>
<td>&quot;Other&quot;</td>
<td>&quot;begin query logging on dbc;&quot;</td>
</tr>
<tr>
<td>03/12/2013 12:34:20 PM</td>
<td>&quot;DBC&quot;</td>
<td>&quot;DBC&quot;</td>
<td>&quot;3725&quot;</td>
<td>&quot;Statement not allowed for an ANSI session.&quot;</td>
<td>&quot;Other&quot;</td>
<td>&quot;begin query logging on dbc;&quot;</td>
</tr>
<tr>
<td>03/12/2013 12:34:20 PM</td>
<td>&quot;DBC&quot;</td>
<td>&quot;DBC&quot;</td>
<td>&quot;3725&quot;</td>
<td>&quot;Statement not allowed for an ANSI session.&quot;</td>
<td>&quot;Other&quot;</td>
<td>&quot;begin query logging on dbc;&quot;</td>
</tr>
<tr>
<td>03/12/2013 12:34:20 PM</td>
<td>&quot;DBC&quot;</td>
<td>&quot;DBC&quot;</td>
<td>&quot;3725&quot;</td>
<td>&quot;Statement not allowed for an ANSI session.&quot;</td>
<td>&quot;Other&quot;</td>
<td>&quot;begin query logging with sql on DBC;&quot;</td>
</tr>
<tr>
<td>03/12/2013 12:34:20 PM</td>
<td>&quot;DBC&quot;</td>
<td>&quot;DBC&quot;</td>
<td>&quot;3725&quot;</td>
<td>&quot;Statement not allowed for an ANSI session.&quot;</td>
<td>&quot;Other&quot;</td>
<td>&quot;begin query logging with sql on all;&quot;</td>
</tr>
<tr>
<td>Date</td>
<td>Action</td>
<td>Database</td>
<td>Query ID</td>
<td>Event Type</td>
<td>Message</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>begin</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>begin query logging on dbc;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>BEGIN QUERY LOGGING ON all;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>0</td>
<td>Other</td>
<td>begin query logging on dbc;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>BEGIN QUERY LOGGING WITH SQL ON ALL;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>BEGIN QUERY LOGGING WITH SQL ON ALL;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>BEGIN QUERY LOGGING ON all;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>BEGIN QUERY LOGGING ON all;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>BEGIN QUERY LOGGING ON all;</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>query</td>
<td>DBC</td>
<td>3725</td>
<td>Other</td>
<td>BEGIN QUERY LOGGING ON all;</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Database User</th>
<th>Database User ID</th>
<th>Authenticated User</th>
<th>Host Name</th>
<th>Database Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/12/2013 12:34:17 PM</td>
<td>DBC</td>
<td></td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
</tr>
<tr>
<td>03/12/2013 12:34:17 PM</td>
<td>DBC</td>
<td>root</td>
<td>DBC</td>
<td>localhost;localhost/127.0.0.1:1025</td>
<td>DBC</td>
</tr>
<tr>
<td>03/12/2013 12:34:17 PM</td>
<td>DBC</td>
<td></td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
</tr>
<tr>
<td>03/12/2013 12:34:17 PM</td>
<td>TEST</td>
<td>root</td>
<td>TEST</td>
<td>localhost;localhost/127.0.0.1:1025</td>
<td>DBC</td>
</tr>
<tr>
<td>03/12/2013 12:34:17 PM</td>
<td>DBC</td>
<td></td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
</tr>
<tr>
<td>03/12/2013 12:34:17 PM</td>
<td>DBC</td>
<td>root</td>
<td>DBC</td>
<td>localhost;localhost/127.0.0.1:1025</td>
<td>DBC</td>
</tr>
<tr>
<td>Date</td>
<td>Time</td>
<td>User</td>
<td>Server</td>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>--------</td>
<td>----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Time</td>
<td>User</td>
<td>Connection</td>
<td>Result</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>------</td>
<td>--------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>root localhost;localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>root localhost;localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>DBC localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
<tr>
<td>03/12/2013</td>
<td>12:34:17 PM</td>
<td>DBC</td>
<td>root localhost/127.0.0.1:1025</td>
<td>DBC</td>
<td></td>
</tr>
</tbody>
</table>