Integrating IBM DB2 UDB

EventTracker v7.x

Publication Date: Dec 04, 2014

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

About this Guide

This guide provides instructions to configure IBM DB2 Universal Database (UDB) to send the audit events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and IBM DB2 Universal Database 10.5 and later.

Audience

IBM DB2 Universal Database users, who wish to forward audit messages to EventTracker manager.

Contents

Introduction to IBM DB2 Universal Database

The auditing facility on DB2 UDB allows a Database Administrator (DBA) to maintain an audit trail for a series of pre-defined database events. It is capable of logging database events such as authorization checking, database object maintenance, security maintenance, system administration, and user validation. The audit facility acts at an instance level, recording all instance level activities and database level activities. There are different categories of audit records that might be generated. It is possible to configure fine-grained auditing by selecting the categories of events to be audited.

Prerequisites

Prior to configuring IBM DB2 Database and EventTracker, ensure that you meet the following prerequisites:

1. IBM DB2 UDB v10.5 Enterprise Server Edition running on Windows 7 Professional, Windows Server 2008(x64 bit).
2. Read and Write permissions on DB2 UDB files.
3. A DB2 UDB user with SYSADM authority to use the db2audit command.
4. EventTracker v7.x or later should be installed.
5. Administrative access on EventTracker Enterprise.

Configuration

A. Enabling logging in IBM DB2 UDB

On the DB2 server run the following batch files under administrator privileges,

1. IBM DB2 Audit path.bat:

   This batch file creates three folders for storing data, archive and extracted logs. It enables the auditing and starts logging. The script file has default path as “C:\IBMDB2\Audit\Files\” under which 3 folders would be created. This path is customizable. To customize the path edit the batch file and save it.

   Note: Run this batch file just once to enable the audit logging and configuring the paths.

2. IBM DB2 Audit log extraction.bat:

   This batch file extracts the audit logs under a default folder "C:\IBMDB2\Audit\Files\Extracted\". This path is customizable. To customize the path edit the batch file and save it.

   Note:

   i. Run this batch file periodically for fetching the logs from the IBM DB2 database.
   ii. Your database name may differ from what has been provided in the above mentioned script files. Please change the name from "**sample"** to appropriate name. To change the database name, edit the file **IBM DB2 Audit log extraction.bat** and replace the database name.

To view audit logging configuration use following command

" db2audit describe"

B. Forwarding IBM DB2 UDB audit log to EventTracker using Direct Log Archiver(DLA)

1. Log on to EventTracker Enterprise.
2. Click the **Admin** dropdown at the upper-right corner.
3. Click **Manager**.
4. Click the **Direct Log Archiver / NetFlow Receiver** tab.
5. Select the **Direct log file archiving from external sources** check box.
   EventTracker enables the associated virtual collection point by default it is 14505.

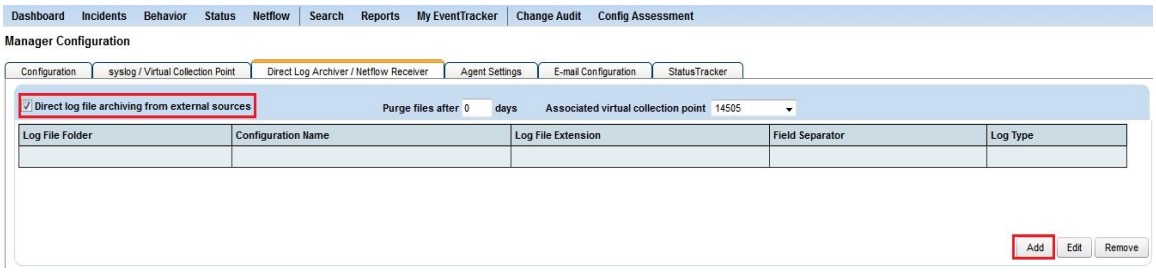

Figure: 01

6. Click on **Add** button at the bottom-right corner.

EventTracker displays the Direct Archiver Configuration pop-up window.

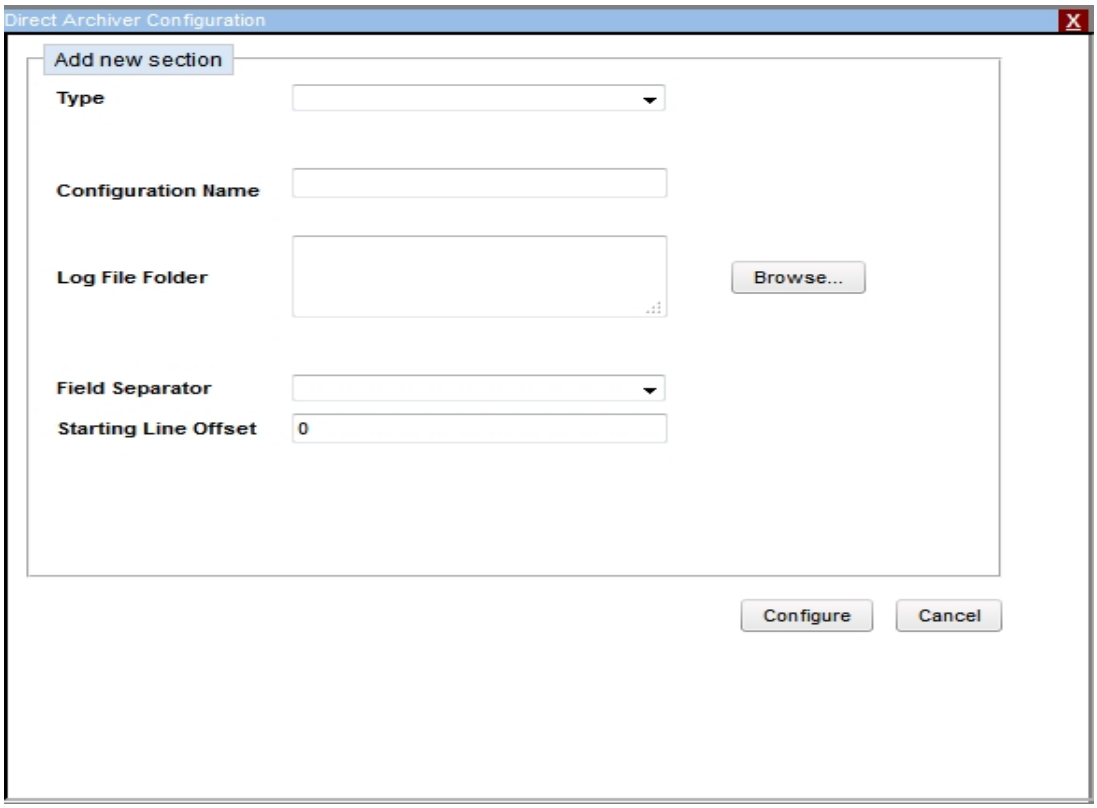

Figure: 02

7. Select 'Others' from the **Type** drop-down list.
8. Write the log file extension as "txt".
9. 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.
10. 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.

11. Select the **Multi Line** from radio button.
12. Starting Line offset is **Zero** by default.
13. Select PREFIX from the Event Separator drop down list.
14. Write the RegEx as ^timestamp=\d{4}-\d{2}-\d{2}-(\d{1,2}.){3} in String or Expression box.

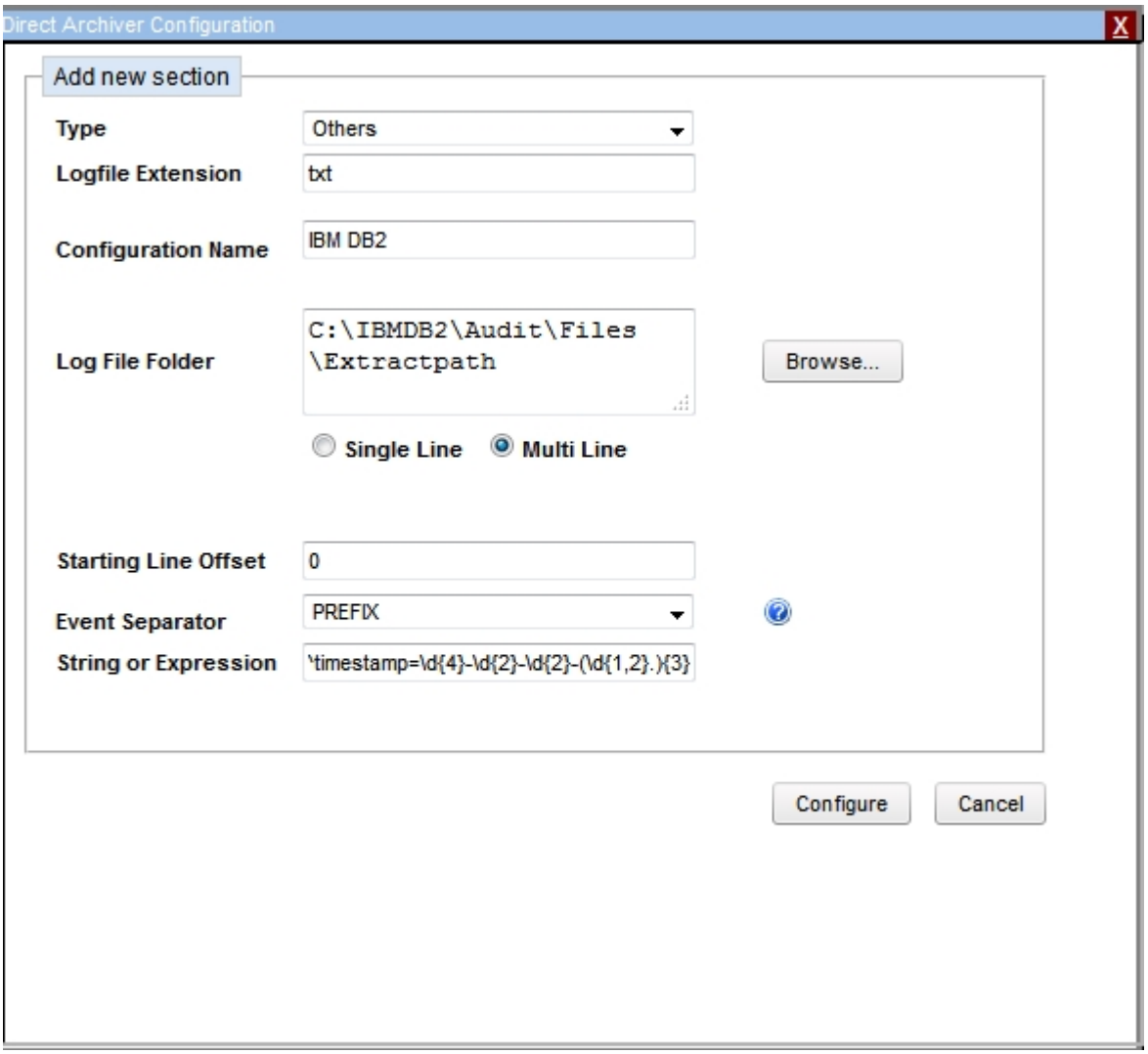

Figure: 03

15. Click on **Configure** button.

EventTracker displays Direct Archiver Configuration window with more configuration options.

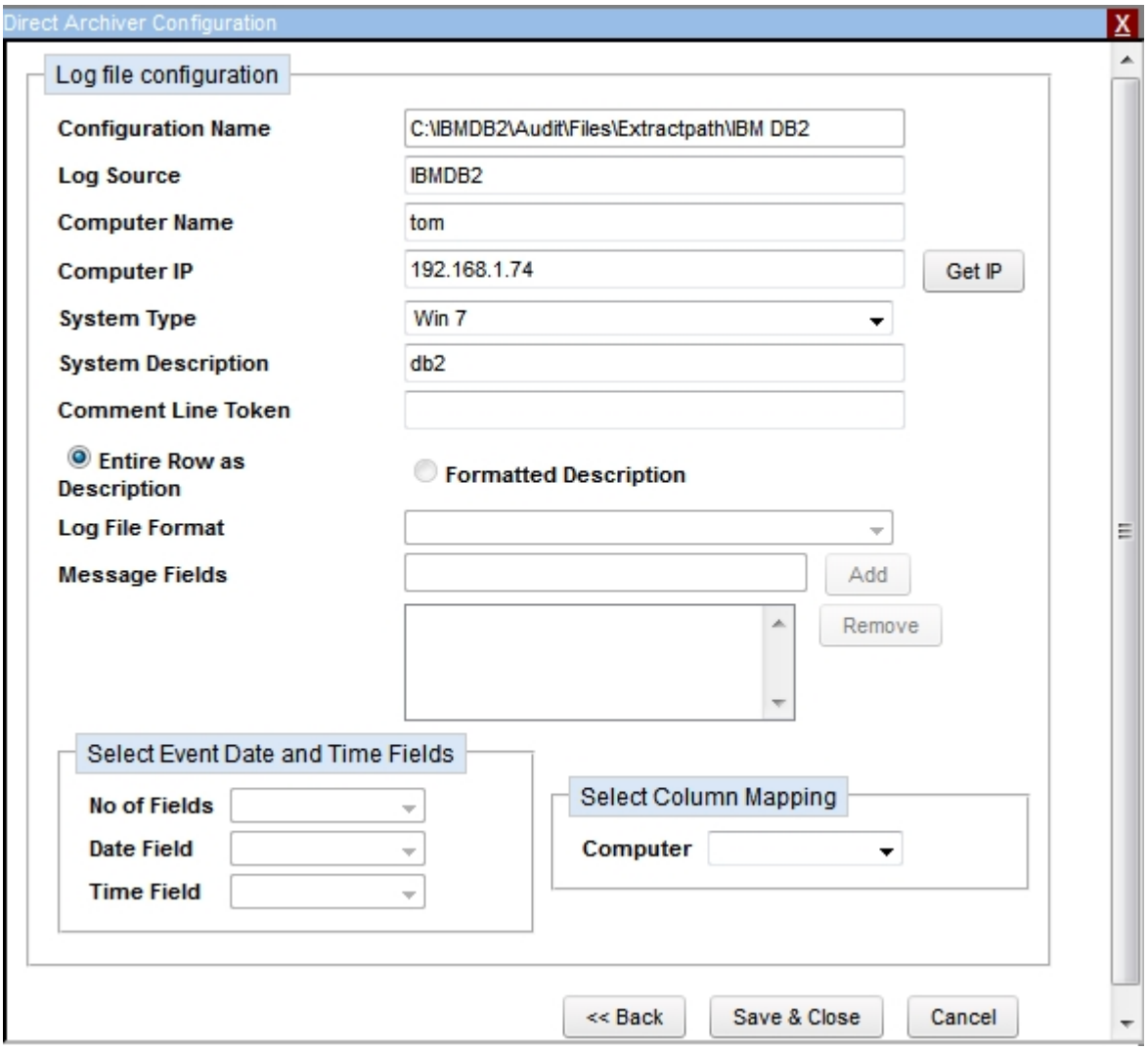
Direct Archiver Configuration
Log file configuration
Configuration Name
C:\IBMDB2\Audit\Files\Extractpath\IBM DB2
Log Source
IBMDB2
Computer Name
tom
Computer IP
192.168.1.74
Get IP
System Type
Win 7
System Description
db2
Comment Line Token
Entire Row as Description
Formatted Description
Log File Format
Message Fields
Add
Remove
Select Event Date and Time Fields
No of Fields
Date Field
Time Field
Select Column Mapping
Computer
<< Back
Save & Close
Cancel

Figure 04

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

16. Enter/select appropriately in the relevant fields.

17. Click **Save & Close**.

    EventTracker adds the DLA settings to the configuration pool.

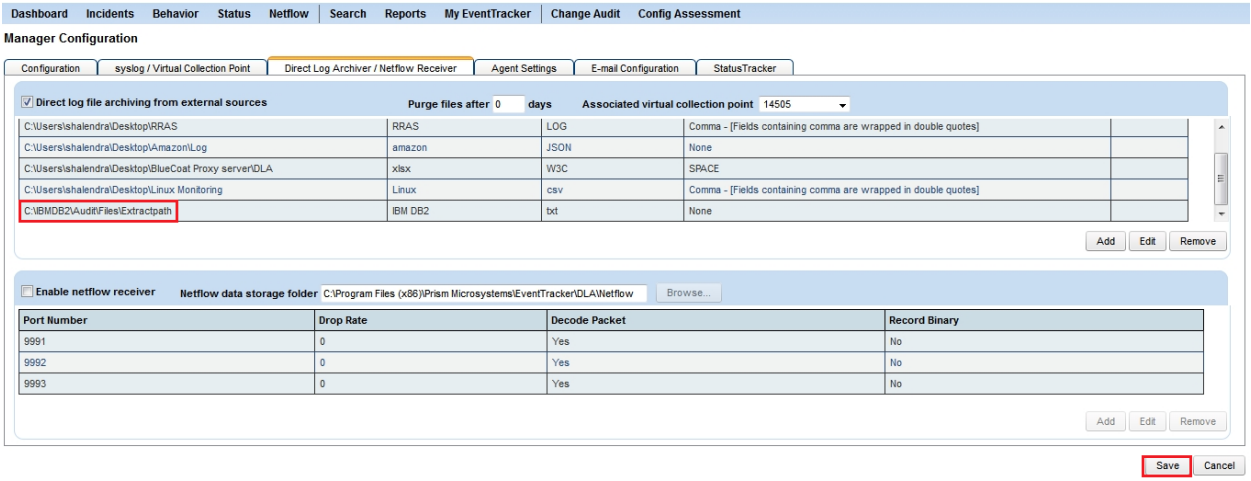

Figure 05

18. Click on Save button to save the configuration of Direct Log Archiver at the bottom-right corner.
19. Click the **Search** tab.
20. EventTracker opens the Log Search browser. And Click on the **Advanced Search** button.

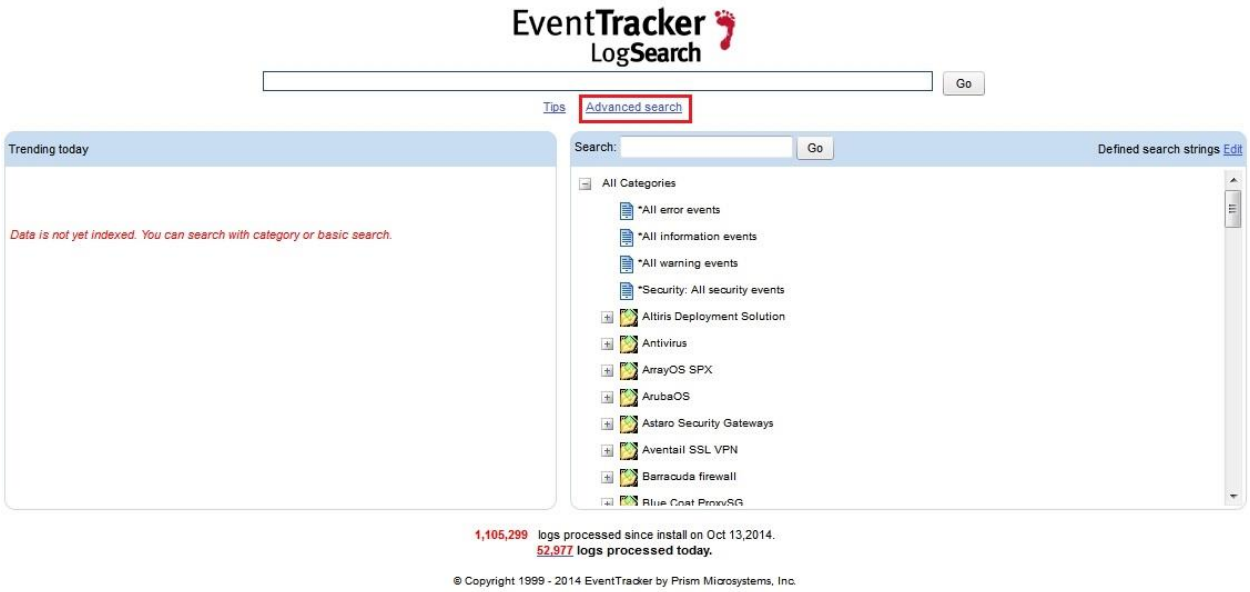

Figure 06

21. Set the search criteria. For example, click on View all system select the specified system, Select the time interval, set the result limit, and enter the search in, operator and search for.

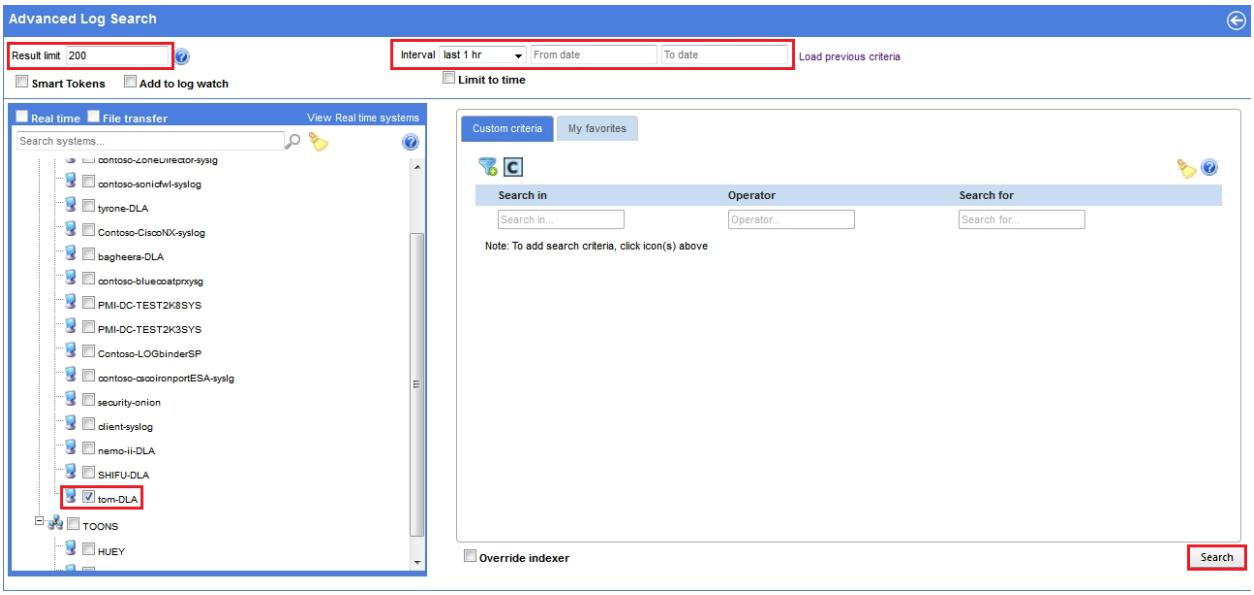

Figure 07

22. Click on **Search** button at the bottom-right corner.

Log Search Utility displays the search result.

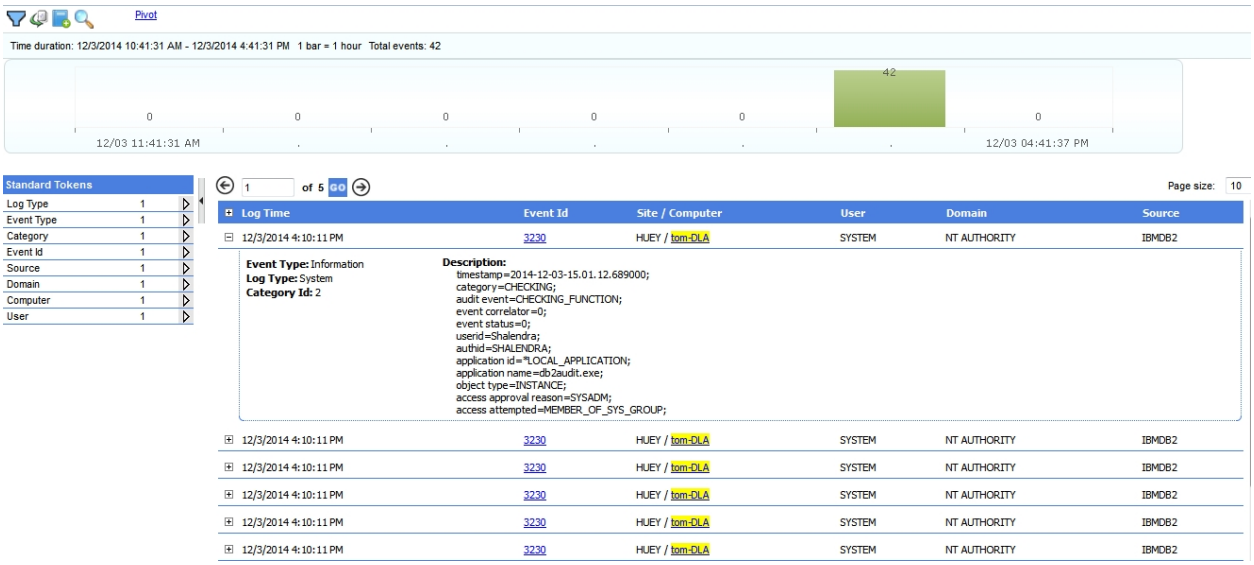

Figure 08

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Categories reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v7.x to support IBM DB2 UDB monitoring.

Categories:

IBM DB2: Admin config updated - This category based report provides information related to admin config updated.

IBM DB2: Admin configuration reset - This category based report provides information related to admin configuration reset.

IBM DB2: Application terminated forcefully - This category based report provides information related to application terminated forcefully.

IBM DB2: Audit facility removed - This category based report provides information related to audit facility removed.

IBM DB2: Audit facility started - This category based report provides information related to audit facility started.

IBM DB2: Audit facility stopped - This category based report provides information related to audit facility stopped.

IBM DB2: Audit policy altered - This category based report provides information related to audit policy altered.

IBM DB2: Audit policy created - This category based report provides information related to audit policy created.

IBM DB2: Audit policy dropped - This category based report provides information related to audit policy dropped.

IBM DB2: Bufferpool dropped - This category based report provides information related to bufferpool dropped.

IBM DB2: Data loaded into a table - This category based report provides information related to data loaded into a table.

IBM DB2: Database altered - This category based report provides information related to database altered.

IBM DB2: Database config updated - This category based report provides information related to database config updated.

IBM DB2: Database configuration reset - This category based report provides information related to database configuration reset.

IBM DB2: Database created - This category based report provides information related to database created.

IBM DB2: Database dropped - This category based report provides information related to database dropped.

IBM DB2: Database manager instance process started - This category based report provides information related to database manager instance process started.

IBM DB2: Database manager instance process stopped - This category based report provides information related to database manager instance process stopped.

IBM DB2: Database manager stopped - This category based report provides information related to database manager stopped.

IBM DB2: Database migrated - This category based report provides information related to database migrated.

IBM DB2: Database restored - This category based report provides information related to database restored.

IBM DB2: Database version updated - This category based report provides information related to database version updated.

IBM DB2: Instance deleted - This category based report provides information related to instance deleted.

IBM DB2: Node added - This category based report provides information related to node added.

IBM DB2: Node group dropped - This category based report provides information related to node group dropped.

IBM DB2: Object altered - This category based report provides information related to object altered.

IBM DB2: Object created - This category based report provides information related to object created.

IBM DB2: Object dropped - This category based report provides information related to object dropped.

IBM DB2: Object renamed - This category based report provides information related to object renamed.

IBM DB2: Security policy altered - This category based report provides information related to security policy altered.

IBM DB2: Specified database activated - This category based report provides information related to specified database activated.

IBM DB2: Specified database deactivated - This category based report provides information related to specified database deactivated.

IBM DB2: System database directory migrated - This category based report provides information related to system database directory migrated.

IBM DB2: Table space dropped - This category based report provides information related to table space dropped.

IBM DB2: Trusted context default role altered - This category based report provides information related to trusted context default role altered.

IBM DB2: User add role altered - This category based report provides information related to user add role altered.

IBM DB2: User added - This category based report provides information related to user added.

IBM DB2: User authentication altered - This category based report provides information related to user authentication altered.

IBM DB2: User drop role altered - This category based report provides information related to user drop role altered.

IBM DB2: User dropped - This category based report provides information related to user dropped.

IBM DB2: User privileges granted for objects - This category based report provides information related to user privileges granted for objects.

Import IBM DB2 UDB knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.
3. Click **Import** tab.
4. Import **Category** as given below.

To import Category

1. Click **Category** option, and then click the browse  button.

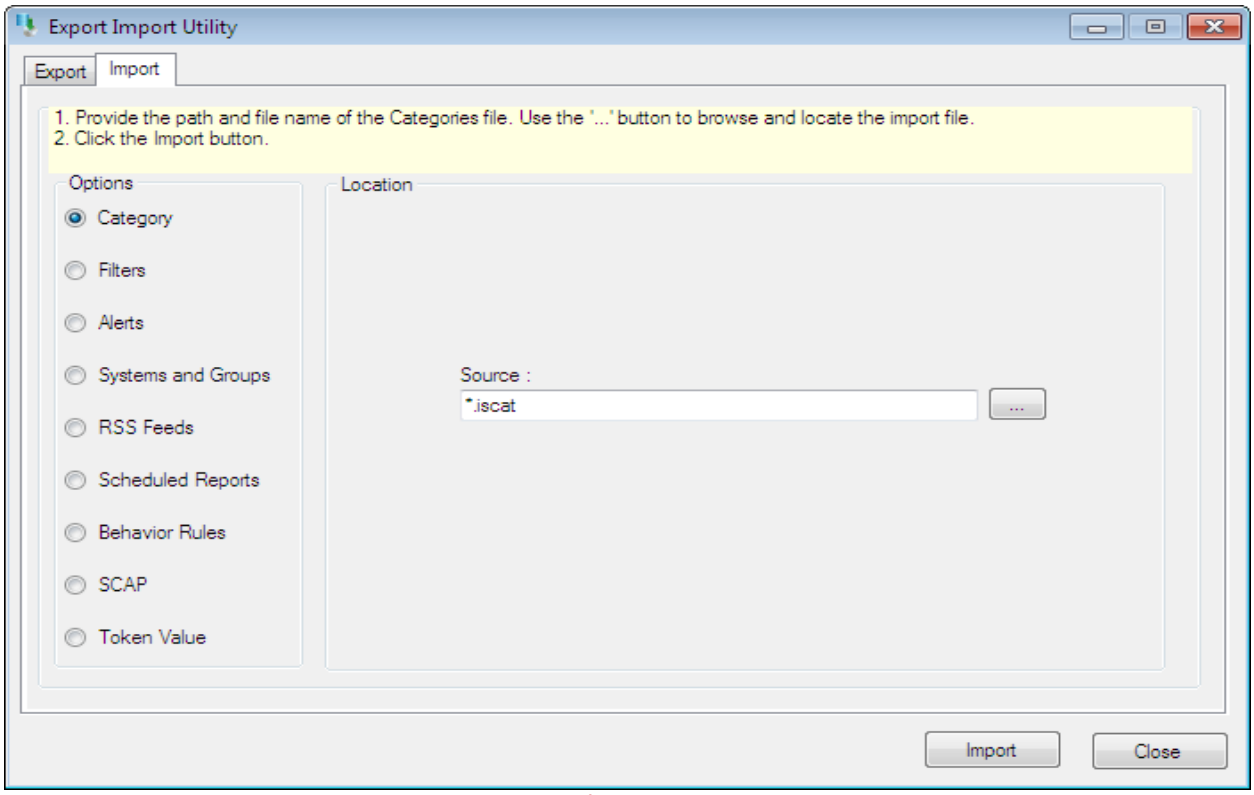

Figure 09

2. Locate All IBM DB2 UDB group of Categories.iscat file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

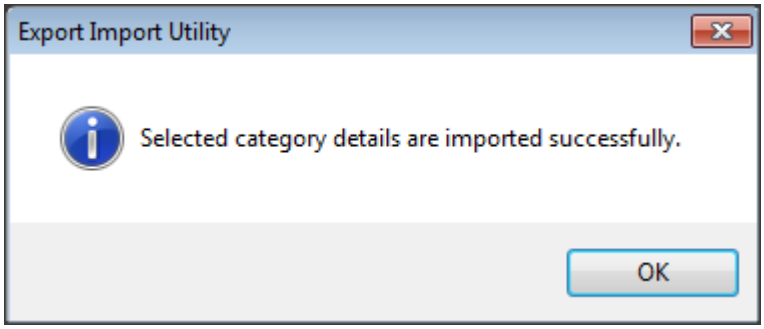

Figure 10

4. Click **OK,** and then click the **Close** button.

Verify IBM DB2 UDB knowledge pack in EventTracker

Verify IBM DB2 UDB Categories

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **IBM DB2 UDB** group folder to view the imported categories.

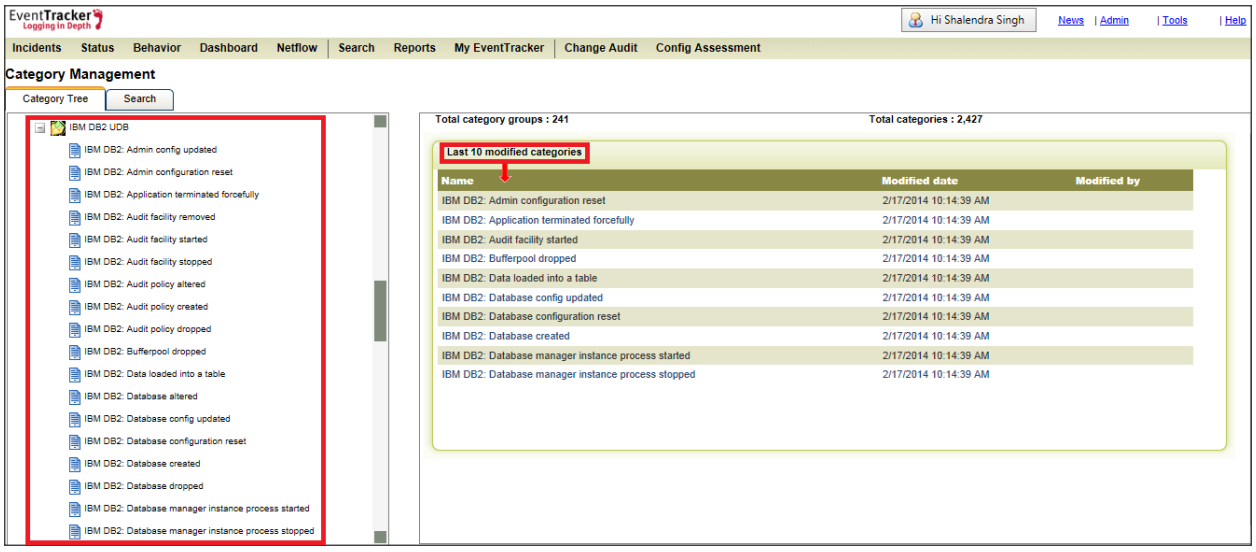

Figure 11