RSA NetWitness Logs

Event Source Log Configuration Guide

IBM Tivoli Identity Manager

Last Modified: Monday, March 06, 2017

Event Source Product Information:

Vendor: IBM
Event Source: Tivoli Identity Manager
Versions: 5.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ibmtim
Collection Method: ODBC
Event Source Class.Subclass: Security.Access Control

Add IBM TIM as a Data Source using IBM DB2 Database

To add IBM TIM to the RSA NetWitness Suite Collector:

1. Install the IBM DB2 database client.
2. Log on to the IBM DB2 client with administrator credentials.
3. Click **Start** > **All Programs** > **IBM DB2** > **DB2COPY(Default)** > **Setup Tools** > **Configuration Assistant**.
4. Click **Selected** > **Add Database Using Wizard**.
5. To complete the Add Database wizard, follow these steps:
   a. Select **Manually configure a connection to a database**, and click **Next**.
   b. Select **TCP/IP**, and click **Next**.
   c. Enter the hostname and the port number of the IBM DB2 server, and click **Next**.
   d. In the **Database name** field, enter the name of the IBM TIM database, and click **Next**.
   e. To register the database as a data source, follow these steps:
      i. Ensure that **Register this database by CLI/ODBC** is selected.
      ii. Select **As system data source**.
      iii. In the **Data source name** field, enter a name for the data source.

      Note: You will use this name when you configure RSA NetWitness Suite.

      iv. Click **Next**.
   f. To specify the node options, follow these steps:
      i. From the **Operating System** drop-down list, select your operating system.
      ii. In the **Instance name** field, enter the name of the DB2 instance, for example, **DB2**.
      iii. Click **Next**.
   g. To specify the system options, accept all the default values, and click **Next**.

h. Select **Use authentication value in server's DBM Configuration**, and click **Finish**.

i. (Optional) To test the connection, in the Add Database Confirmation window, click **Test Connection**, and follow these step:

   i. Enter the user name and password.

   ii. Click **Test Connection**.

   iii. Click **OK**.

j. Click **Close**.

Configure NetWitness Suite for ODBC Collection

To configure ODBC collection in RSA NetWitness Suite, perform the following procedures:

I. Ensure the required parser is enabled

II. Configure a DSN

III. Add the Event Source Type

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it from RSA NetWitness Suite Live Services.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **ibmtim**.

Configure a DSN

For IBM Tivoli Identity Manager, you can use Oracle or SQL Server:

In both cases, you can follow the procedure below. The procedure differs only for step 8, where you choose the appropriate DSN template.

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.

4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click + to open the **Add DSN** dialog.

   Note: If you need to add a DSN template, see Configure DSNs in the NetWitness User Guide.

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

To fill in the parameters, see one of the following procedures, **Choose an IBM DB2 Database** or **Choose an MS SQL Database**.

Choose an IBM DB2 Database

If you are using an IBM DB2 database, do the following:

1. From the Add DSN dialog box, select either **IBM_DB2_Unix_Template** or **IBM_DB2_Windows_Template**, depending on the platform of your IBM DB2 database server.
2. Fill in the parameters as shown below.

Field	Description
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Collection	**Windows Only.** Enter the name of the IBM DB2 collection.
LocationName	**Windows Only.** Enter the name of the IBM DB2 location.
TcpPort	The default port is **50000**.
IpAddress	Specify the hostname or IP Address of the IBM DB2 database.
Database	Enter the name of the IBM DB2 database you are using with RSA NetWitness Suite.
Driver	You must update the default driver to point to your driver: **ODBCHOME/lib/xxdb2nn.zz**.

Choose a Microsoft SQL Database

If you are using a Microsoft SQL database, do the following:

1. From the Add DSN dialog box, select either **MSSQL_Server_Windows_Template** or **MSSQL_Server_Unix_Template**, depending on the platform of your MS SQL database server.
2. Fill in the parameters as shown below.

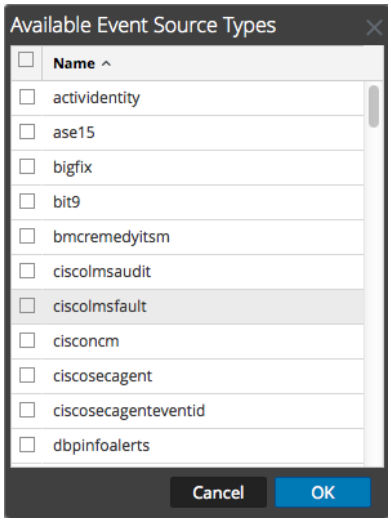
Field	Description
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Driver	**Windows**:Depending on your NetWitness Log Collector version: • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so **Unix**: the default value is **ODBCHOME/lib/xxmssqlnn.zz**.
Database	Enter the name of the MS SQL database you are using with RSA NetWitness Suite. The default values is **MSSQLHost**.
PortNumber	The default port is **1433**.
HostName	Enter the IP address or host name for the MS SQL database. The default value is **localhost**.

Add the Event Source Type

Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.

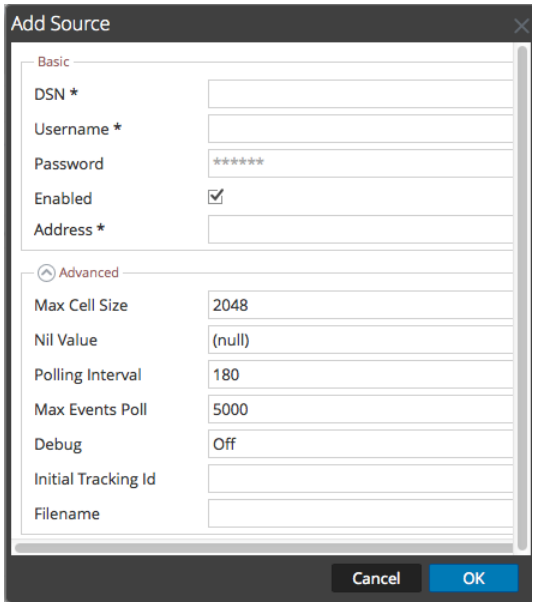
   The Event Categories panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.

   Select **itim** from the **Available Event Source Types** dialog.

7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click + to open the **Add Source** dialog.



9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see ODBC Event Source Configuration Parameters in the NetWitness Suite Log Collection Guide.

Trademarks