RSA NetWitness Platform

Event Source Log Configuration Guide

IBM DB2

Last Modified: Tuesday, September 3, 2019

Event Source Product Information:

Vendor: IBM
Event Source: DB2 Universal Database
Versions: 7,8, 8.1, 9.1, 9.5, 9.7, 10.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Additional Downloads:

- For Windows: DB2GetAudit.vbs, DB2Audit.conf, sftpagent.conf.ibmdb2, DatabaseList.conf
- For AIX: DB2AuditScript.sh, DB2Audit.conf, DatabaseList.conf

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: ibmdb2
Collection Method: File, ODBC
Event Source Class.Subclass: Storage.Database

Configure IBM DB2

To configure file collection, see the instructions below for your platform. To configure ODBC collection on the RSA NetWitness Platform, see Configure NetWitness Platform for ODBC Collection.

I. Configure IBM DB2. Depending on your platform, do one of the following:

- Configure IBM DB2 UDB for Windows, or
- Configure IBM DB2 UDB for AIX

II. Configure RSA NetWitness Platform for SFTP and File Collection

For table reference, see Reference Tables below.

Configure IBM DB2 UDB for Windows

To configure IBM DB2 UDB for Windows, you must complete these tasks:

1. Download and Edit IBM DB2 Scripts
2. Configure the IBM DB2 Audit Facility
3. Set Up the Windows Task Scheduler

Download and Edit IBM DB2 Scripts

To download and edit IBM DB2 scripts:

1. On the IBM DB2 server, create a **DB2_Audit** folder on the C: drive.
2. To download the necessary scripts for IBM DB2, follow these steps:
   a. Download the **DB2GetAudit.vbs** VBScript file and the **DB2Audit.conf** configuration file, and paste the files into the **DB2_Audit** folder.
   b. (Optional) If you want to enable DB Level Auditing, download the **DatabaseList.conf** file. Open the file in a text editor, and add each database at the instance level you want audited, with one database name per line and no special characters.

   Note: For DB Level Auditing to function properly, you must create and activate all the necessary policies for the required tables and databases.
3. In the **DB2_Audit** folder, create a **Data** folder, an **Archive** folder, and an **Archive_BackUp** folder to store, archive, and back up your raw log data.
4. In the **DB2Audit.conf** file, set the following parameters:

   ```
   Bin_Path=Bin_Path
   Data_Path=Data_Path
   Archive_BackUp_Path=Archive_BackUp_Path
   Archive_Path=Archive_Path
   ```

   where:

   - *Bin_Path* is the path to the IBM **Bin** folder.
   - *Data_Path* is the path to the **Data** folder within the **DB2_Audit** folder on your C: drive, for example, C:\DB2_Audit\Data.

- *Archive_BackUp_Path* is the path to the **Archive_BackUp** folder within the **DB2_Audit** folder on your C: drive, for example, C:\DB2_Audit\Archive_BackUp.
- *Archive_Path* is the path to the **Archive** folder within the **DB2_Audit** folder on your C: drive, for example, C:\DB2_Audit\Archive.

5. Click **File** > **Save**.

Configure the IBM DB2 Audit Facility

To configure the IBM DB2 audit facility:

1. On the IBM DB2 server, click **Start** > **All Programs** > **IBM DB2** > **RSADB2** > **Command Line Tools** > **Command Line Processor**.
2. To update the database buffer sites, follow these steps:
   a. In the command prompt, type:

      ```
      update dbm cfg using AUDIT_BUF_SZ 100
      ```

   b. In the command prompt, type:

      ```
      quit
      ```

3. To enable the audit facility, follow these steps:
   a. To reset the audit facility to the default settings, type:

      ```
      db2audit configure reset
      ```

   b. To activate auditing settings, on separate command prompts, type:

      ```
      db2audit configure scope audit status both
      db2audit configure scope checking status both
      db2audit configure scope secmaint status both
      db2audit configure scope sysadmin status both
      db2audit configure scope objmaint status both
      db2audit configure scope validate status both
      db2audit configure scope context status both
      ```

4. To set the data and archive path, type:

   ```
   db2audit configure datapath "Data_Path" archivepath "Archive_Path"
   ```

   where:

   - *Data_Path* is the path to the **Data** folder within your **DB2_Audit** folder on the C: drive.

- *Archive_Path* is the path to the **Archive** folder within your **DB2_Audit** folder on the C: drive.

5. To start the audit facility, type:

```
db2audit start
```

Set Up the Windows Task Scheduler

To set up the Windows Task Scheduler:

1. On the IBM DB2 server, click **Start** > **Settings** > **Control Panel**.
2. Click **Scheduled Task** > **Add Scheduled Task**.
3. In the Scheduled Task Wizard, click **Next**.
4. Select any application from the list, and click **Next**.
5. In the **Type a name for this task** field, type **IBMDB2_Audit**.
6. Under the **Perform this task** field, select **Daily**, and click **Next**.
7. Select the start time and start date, and click **Next**.
8. In the user name and password fields, enter the server logon credentials, and click **Next**.
9. Select **Open advanced properties for this task when I click Finish**, and click **Finish**.
10. On the **Task** tab of the advanced properties window, complete the fields as follows.

Field	Action
Run	Type **"C:\WINDOWS\system32\wscript.exe DB2GetAudit.vbs"**
Start	Enter the path to the **DB2_Audit** folder.

11. On the **Schedule** tab, click **Advanced**.
12. Select **Repeat task**, and complete the fields as follows.

Field	Action
Every	Select **6 hours** as the frequency of time the RSA NetWitness Platform uses to collect logs from IBM DB2. **Note:** If the time increment for event collection is greater than 6 hours, the database buffer that is set to 100 when configuring the audit facility must be increased.

Field	Action
Until	Select **Duration**.
Hour(s)	Type **24**.

13. Click **Apply**.

Configure IBM DB2 UDB for AIX

To configure IBM DB2 UDB for AIX, you must complete these tasks:

1. Download and Edit IBM DB2 Scripts
2. Configure the IBM DB2 Audit Facility
3. Configure the DB2 Audit Script as a cron job

Download and Edit IBM DB2 Scripts

To download and edit IBM DB2 scripts:

1. On the IBM DB2 server, create a **DB2Audit** directory in your home directory. Ensure that the directory name contains no spaces or underscores, for example, /home/*db2user*/DB2Audit, where *db2user* is your DB2 instance name.
2. Download the **DB2AuditScript.sh** shell script file and the **DB2Audit.conf** configuration file RSA Link here: https://community.rsa.com/docs/DOC-45601.
3. (Optional) If you want to enable DB Level Auditing, download the **DatabaseList.conf** file. Open the file in a text editor, and add each database at the instance level you want audited, with one database name per line and no special characters.

   Note: For DB Level Auditing to function properly, you must create and activate all the necessary policies for the required tables and databases.
4. Copy these files into the **DB2Audit** directory.
5. In the **DB2Audit** directory, create a **Data** directory, an **Archive** directory, and an **Archive_BackUp** directory to store, archive, and back up your raw log data.
6. Open the **DB2Audit.conf** file, and set the following parameters:

   ```
   Bin_Path=Bin_Path
    Data_Path=Data_Path
    Archive_BackUp_Path=Archive_BackUp_Path
    Archive_Path=Archive_Path
   ```

   where:

   - *Bin_Path* is the path to the IBM **adm** directory where the IBM db2audit script resides, for example, /home/db2user/sqllib/adm.
   - *Data_Path* is the path to the configured **Data** directory mentioned in the configuration file, **DB2Audit.conf**, for example, /home/db2user/DB2AuditData/.

- *Archive_BackUp_Path* is the path to the configured **Archive_BackUp** directory mentioned in the **DB2Audit.conf** configuration file, for example, /home/db2user/DB2ArchiveBackup.
- *Archive_Path* is the path to the configured **Archive** directory mentioned in the **DB2Audit.conf** configuration file, for example, /home/db2user/DB2AuditArchive.

Configure the IBM DB2 Audit Facility

To configure the IBM DB2 Audit Facility:

1. On the IBM DB2 server, from the Terminal or Console, type:

   ```
   db2
   ```

   Note: If the path is set, the DB2 Command Line Processor opens with a prompt that looks like **db2 =>**.

   If the Command Line Processor displays the message, "db2 not found", either set the system path to include the DB2 Bin path, for example, /opt/IBM/db2/V9.X/bin, or you can change directories to **/opt/IBM/db2/V9.X/bin**, and type **./db2**.

2. To update the database buffer sites, follow these steps:

   a. Open a command prompt, and type:

   ```
   update dbm cfg using AUDIT_BUF_SZ 100
   ```

   b. In the command prompt, type:

   ```
   quit
   ```

3. To enable the audit facility, follow these steps:

   a. To reset the audit facility to the default settings, open a command prompt, and type:

   ```
   db2audit configure reset
   ```

   b. To activate auditing settings, on separate command prompts, type:

   ```
   db2audit configure scope audit status both
   db2audit configure scope checking status both
   db2audit configure scope secmaint status both
   db2audit configure scope sysadmin status both
   db2audit configure scope objmaint status both
   db2audit configure scope validate status both
   db2audit configure scope context status both
   ```

4. To set the data and archive path, type:

   ```
   db2audit configure datapath Data_Path archivepath Archive_Path
   ```

   where:

- *Data_Path* is the path to the configured **Data** directory set in the **DB2Audit.conf** file.
- *Archive_Path* is the path to the configured **Archive** directory set in the **DB2Audit.conf** file.

5. To start the audit facility, open a command prompt, and type:

```
db2audit start
```

Configure the DB2 Audit Script as a cron Job

To configure the DB2 audit script as a cron job:

1. Add the following paths to your **PATH** environment variable:

/home/*db2user*/bin
/home/*db2user*/sqllib/bin
/home/*db2user*/sqllib/adm
/home/*db2user*/sqllib/misc
/home/*db2user*/sqllib/db2tss/bin

> **Note:** You may want to edit the **.profile** file in your **/home** directory to add these to the **PATH** environment variable so that the paths are sourced when you log on to the shell. This ensures that the cron daemon has access to the files in these paths to execute your DB2 Audit commands.
>
> A typical line in the **.profile** file in your **/home** directory looks like the following:
>
> **PATH=/home/db2user/bin:/home/db2user/sqllib/bin:/home/db2user/sqllib/adm:/home/db2user/sqllib/**
> **misc:/home/db2user/sqllib/db2tss/bin**
>
> **export PATH**

2. Configure the cron job. For information on how to configure a cron job, go to:

   http://publib.boulder.ibm.com/infocenter/aix/v6r1/index.jsp?topic=/com.ibm.aix.cmds/doc/aixcmds1/crontab.htm

   When you specify a line for running this script, the line should look like the following:

   10 0-23 * * * . ~/.profile;*command or script*/*DB2AuditScript.sh_path*

   where:

   - *command or script* is the command or script to be executed.
   - *DB2AuditScript.sh_path* is the path of the **DB2AuditScript.sh** file.

Warning: The **. ~/.profile;** portion of this line is read as **<period><space><tilde><slash><period>profile<semicolon>**.

All of the words denote their exact symbols, including space, so a line in your **.cron** file for this script should look like the following:

10 10 * * * . ~/.profile;/home/*db2user*/DB2Audit/DB2AuditScript.sh

This line runs the script on the tenth minute of the tenth hour, every day.

Configure NetWitness Platform for SFTP and File Collection

Set up the SFTP Agent, and configure the Log Collector for File Collection.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SFTP Shell Script File Transfer

Configure the Log Collector for File Collection

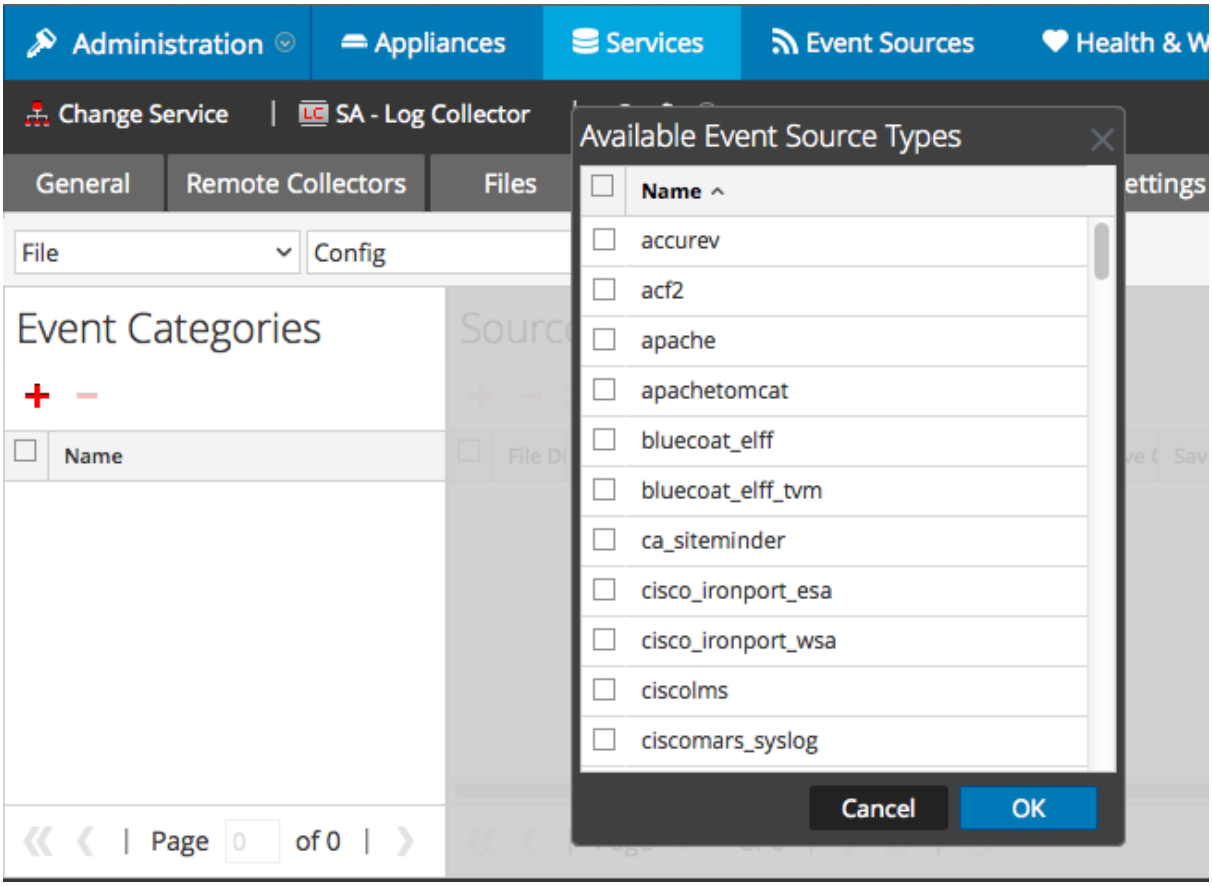
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.

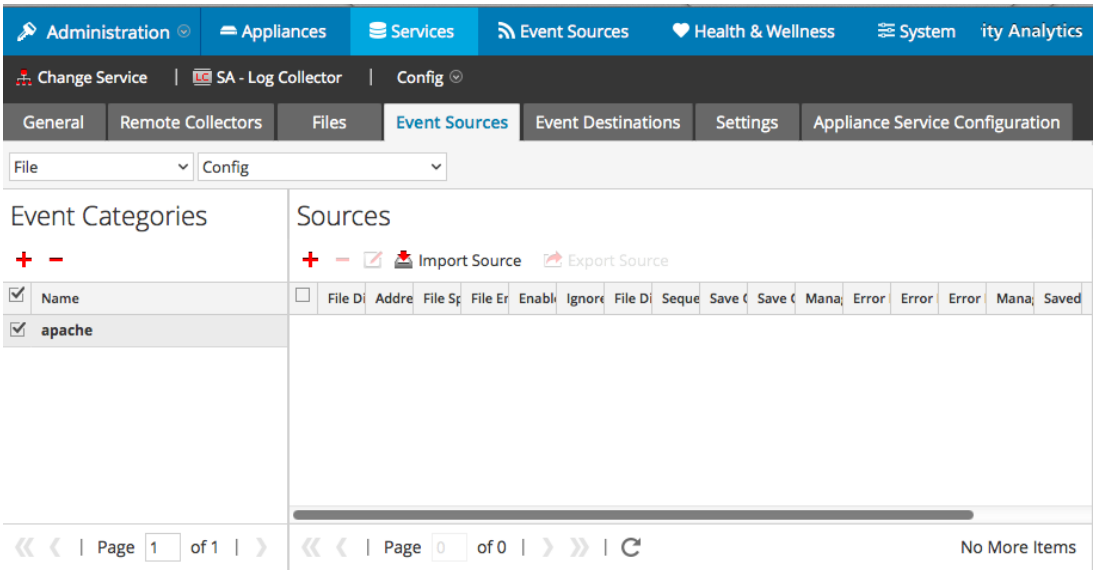


5. Select the correct type from the list, and click **OK**.

   Select **ibmdb2** from the **Available Event Source Types** dialog.

   The newly added event source type is displayed in the Event Categories panel.

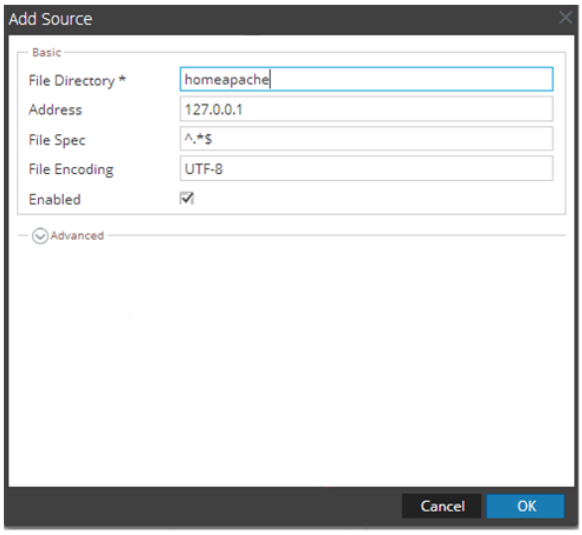
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

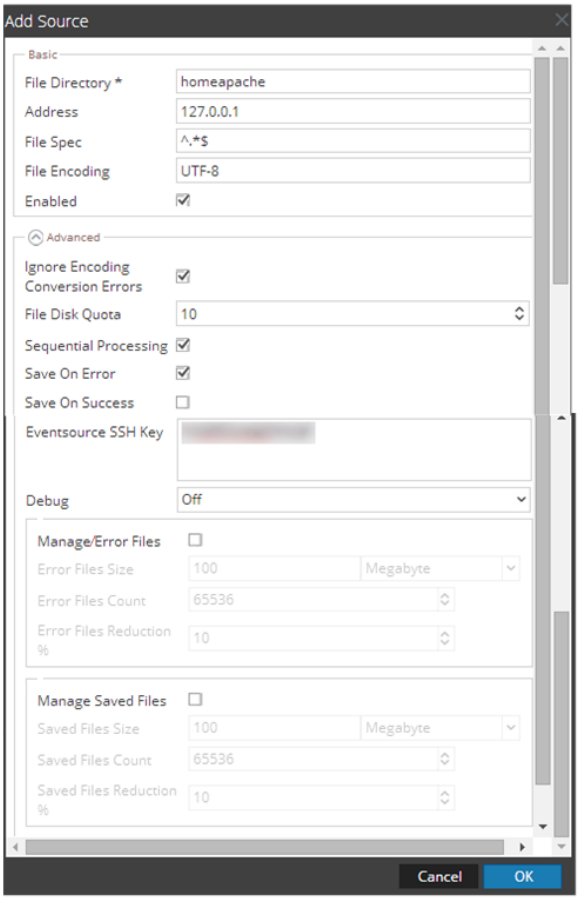


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

   Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.





7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Configure NetWitness Platform for ODBC Collection

To configure ODBC collection in RSA NetWitness, 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 in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **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 **ibmdb2**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **ADMIN** > **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 the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in RSA Link.

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**.

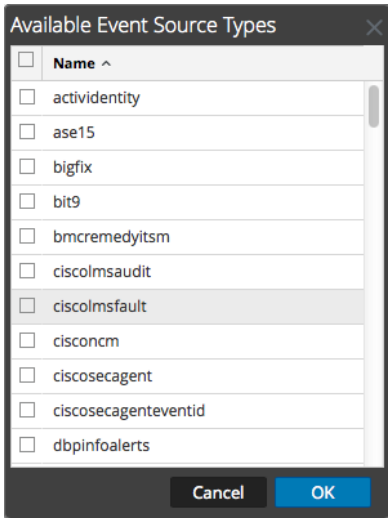
Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the database used by DB2
PortNumber	Specify the Port Number. The default port number is **50000**
HostName	Specify the hostname or IP Address of DB2
Driver	Depending on your NetWitness Log Collector version: • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3db227.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3db226.so

Add the Event Source Type

Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **ADMIN** > **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.

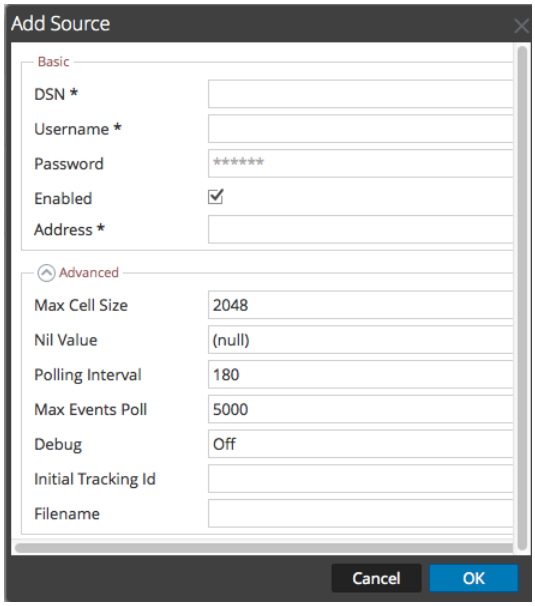


6. Choose the log collector configuration type for your event source type and click **OK**.

   In the **Available Event Source Types** dialog, select **ibmdb2**.

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 the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Reference Tables

This event source collects data from the **ibmdb2.xml** table, using the following typespec files:

- AUDIT.AUDIT
- AUDIT.SYSADMIN
- AUDIT.VALIDATE
- AUDIT.OBJMAINT
- AUDIT.SECMAINT

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.