NetWitness® Platform XDR

IBMDB2 JDBC Event Source Log Configuration Guide

NETWITNESS
Platform XDR

IBMDB2 JDBC

Event Source Product Information:

Vendor: IBM

Event Source: DB2 Universal Database

Additional Downloads :

For Windows: DB2GetAudit.vbs, DB2Audit.conf, sftpagent.conf.ibmdb2, DatabaseList.conf

Versions: IBM 7.0, 8.0, 8.1, 9.1, 9.5, 9.7, 10.x

NetWitness Product Information:

Supported On: NetWitness Platform XDR 12.3 and later (both the Admin Server and Log Collector Node)

Event Source Log Parser: ibmdb2

Collection Method: Logstash

Event Source Class.Subclass: Storage.Database

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

August 2024

Contents

Configure JDBC IBMDB2 Event Source

Database Auditing

If you are using database auditing on an Oracle Windows or Unix platform, you can collect messages through the NetWitness Platform Logstash JDBC Service. Collecting messages through the NetWitness Platform Logstash JDBC Service has the following advantages:

- Database auditing collection is server specific.
- You can collect messages from a Windows platform.
- All messages are in a fixed format, making them easier to read.

You must complete these tasks to configure JDBC IBMDB2 Event Source:

I. Configure IBM DB2 UDB for Windows

II. Deploy Logstash JDBC IBMDB2 Pipelines from NetWitness Live

III. Set Up Logstash JDBC IBMDB2 Event Sources (Pipelines) in NetWitness Platform XDR

IV. JDBC IBMDB2 Collection Configuration Parameters

V. Configure NetWitness Platform to Collect Events

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 IBM DB2 Audit Facility
3. Set Up 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 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 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**, **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	Select the check-box to enable the event source configuration to start collection. The check-box is selected by default.

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.
Until	Select Duration.
Hour(s)	Type 24.

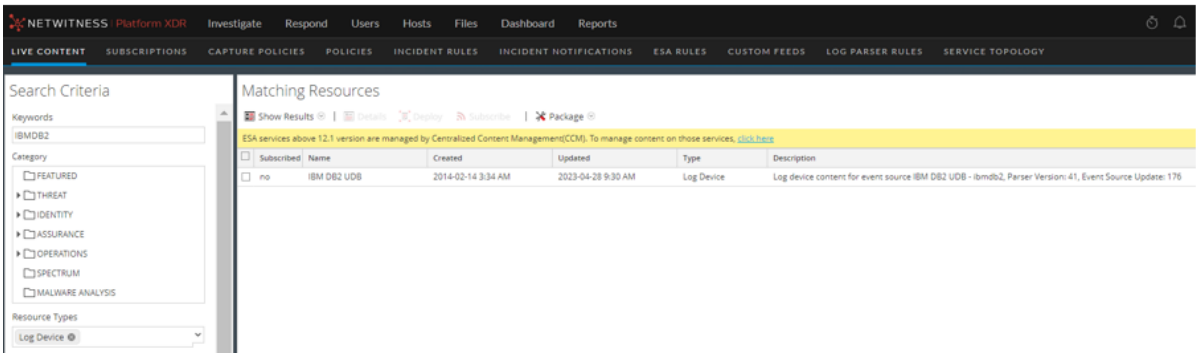
13. Click **Apply**.

Deploy Logstash JDBC IBMDB2 Pipelines from NetWitness Live

Logstash JDBC IBMDB2 Pipeline files requires resources available in Live to collect logs.

To deploy Logstash JDBC IBMDB2 Pipeline files from Live:

1. In the NetWitness Platform XDR menu, select **Configure > Live Content**.
2. Type **IBMDB2** into the Keywords text box and click **Search** to browse Live for Logstash JDBC IBMDB2 Pipeline files.
3. Select the item returned from the search based on the DB version.
4. Click **Deploy** to deploy the Logstash JDBC IBMDB2 Pipeline files to the appropriate Log Collector in the **Deployment Wizard**.



Set Up Logstash JDBC IBMDB2 Event Sources (Pipelines) in NetWitness Platform XDR

You must complete these tasks to set up the JDBC IBMDB2 Event Source (Pipelines) in Netwitness Platform XDR:

1. Configure JDBC IBMDB2 Event Source
2. Add Event Source Type

Enable Parser

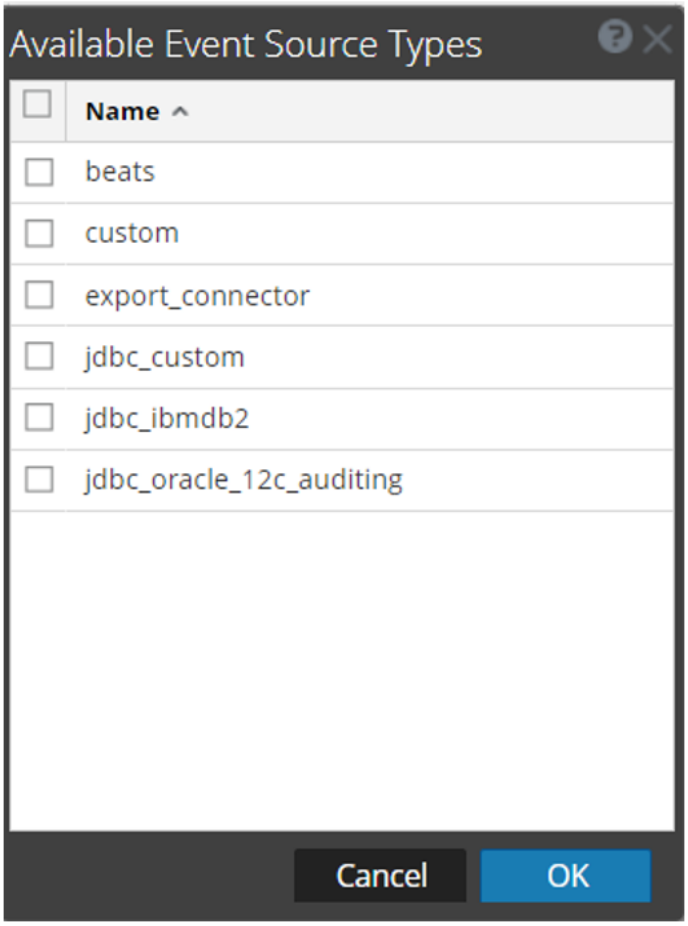
1. If you do not see your parser in the list while performing this procedure, you need to download it from NetWitness Platform XDR website.
2. To enable the parser for your event source:
   a. In the NetWitness Platform XDR menu, select (Admin) > **Services**.
   b. In the **Services** grid, select a **Log Collector** service, and from the **Actions (⚙)** menu, choose **View** > **Config**.
   c. 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.

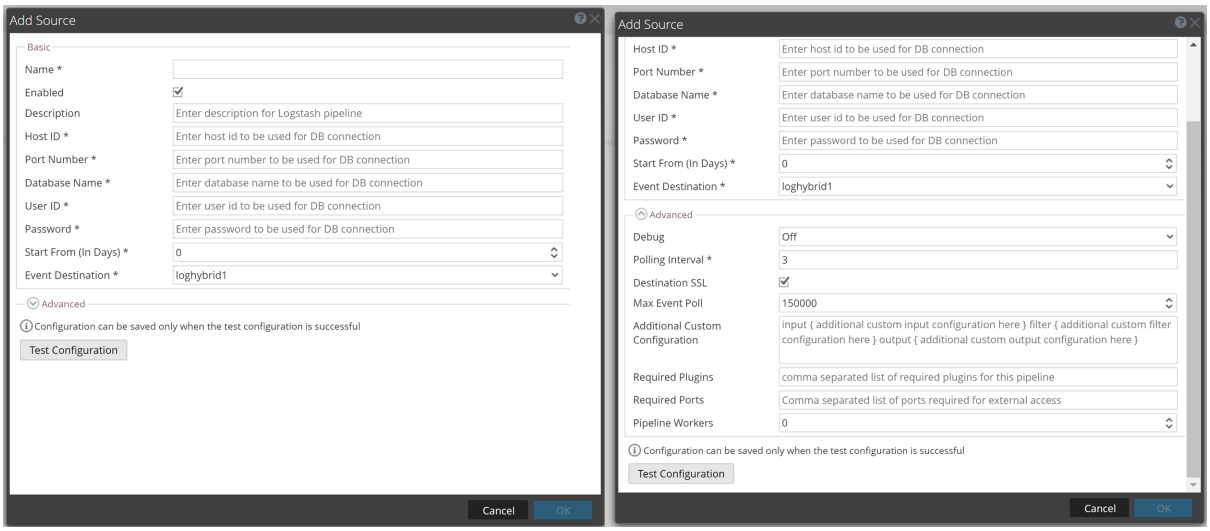
Add Event Source Type

To add the event source type:

1. In the NetWitness Platform XDR menu, select (Admin) > **Services**.
2. In the **Services** grid, select a **Log Collector** service, and from the **Actions (⚙)** menu, choose **View** > **Config**.
3. In the **Event Sources** view, select **Logstash/Config** from the drop-down menu. The **Available Event Source Types** pop-up window is displayed with the existing sources, if any.



4. In the **Event Categories** panel toolbar, click +.
5. Select the log collector configuration type for your event source type and click **OK**. In the **Available Event Source Types** dialog, select **jdbc_ibmdb2**.
6. In the **Event Categories** window, select the event source type that you just added.
7. In the **Sources** panel, click +. The **Add Source** dialog is displayed.

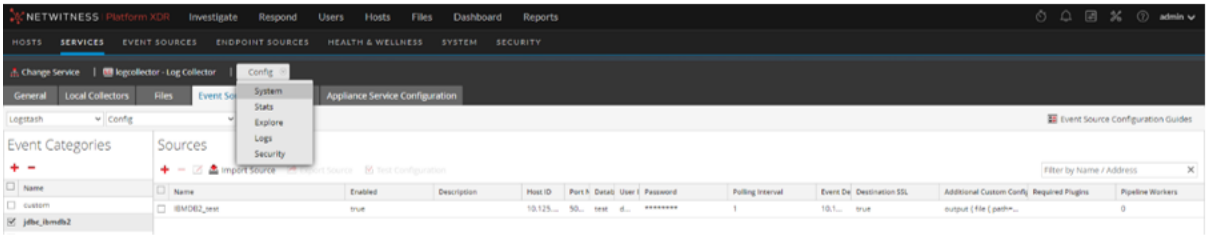


8. Define the parameter value described in JDBC IBMDB2 Collection Configuration Parameters.
9. Click **Test Configuration**.

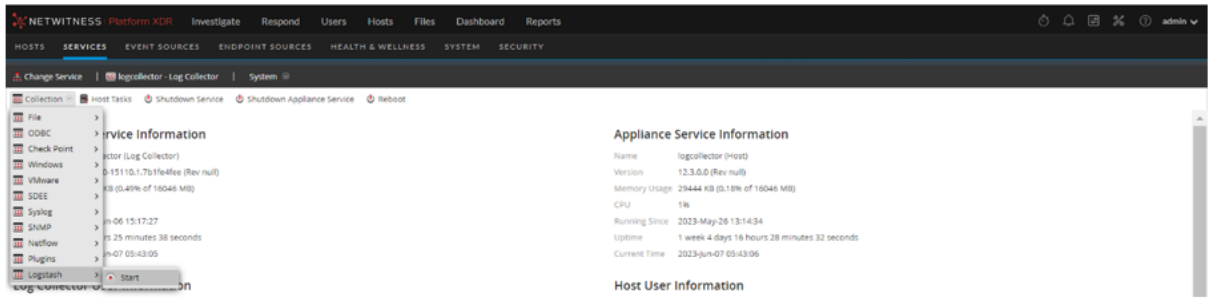
   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information based on message shown and retry.

   Note: The log collector may take 1 to 3 minutes to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform XDR displays a Request Timed Out error.

10. If the test is successful, click **OK**. The new event source is displayed in the **Sources** panel.
11. Save the configuration. From the **Actions** menu, choose **System**.



12. In the **Collection** drop-down menu, select **Logstash > Start** to start the log collection.



JDBC IBMDB2 Collection Configuration Parameters

The tables below list the configuration parameters required for integrating different database event source with NetWitness Platform XDR through JDBC IBMDB2 logstash pipeline.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the check-box to enable the event source configuration to start collection. The check-box is selected by default.
Description	Enter a text description for the event source.
Host ID*	Enter the IP address of the IBM DB2 Server.
Port Number*	Enter the port number that you configured for your event source. The default value of port number is 50000.
Start Date*	Number of days before today to begin data collection (0-90, default: 0). For example, if today is 2024-09-12 and startDate is set as 10, collection starts from 2024-09-02 00:00:00 (YYYY-MM-DD HH:MM:SS). If not set, it takes default value ans starts collection from today 00:00:00.
Database Name*	Enter the name of the database where the audit table exists.
User ID*	Enter the username of Oracle database.
Password*	Enter the password to log into the Oracle database.
Polling Interval*	Polling interval takes the input in minutes. Based on the minutes entered, the pipeline will pull the data from the database. For example, If the polling interval is 1, then the pipeline will pull the data from the database for every 1 minute. If the polling interval is 2, then the pipeline will pull the data from the database for every 2 minute. This filed takes the values between 1 to 60.
Event Destination*	Select the NetWitness Log Collector or Log Decoder to which event needs to be sent from the drop-down list.
Test Configuration	Checks the configuration parameters specified in this dialog to ensure they are correct.

Advanced Parameters

Click  next to **Advanced** to view and edit the advanced parameters, if necessary.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to **On** or **Verbose**) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. **Caution:** Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
Destination SSL	Select the checkbox to communicate using destination SSL.
Additional Custom Configuration	Use this text box for any additional configuration, in case you have multiple inputs or another set of outputs to send somewhere in addition to a NetWitness Log Collector or Log Decoder. For example, you can configure the data to be sent to Elasticsearch. In this case each event that is sent to Netwitness Platform will also be send to Elasticsearch.
Required Plugins	Specify the required plugins in a comma separated list. **Note:** - Backup and restore is not supported for custom plugins. - If the test connection failed due to required plugin is not installed, you must install the required plugin, for more information, see Install or Manage Logstash Plugin.
Required Ports	Enter the list of ports required for external access.
Pipeline Workers	Number of pipeline worker threads allocated for logstash pipeline.

Configure NetWitness Platform to Collect Events

To configure NetWitness platform to collect events:

1. You must start capture on the Log Decoder to which you are sending the Logstash data. To start or restart network capture on a Log Decoder:

   i. In the NetWitness Platform menu, select  **(Admin) > Services**. The Services view is displayed.

   ii. Select a **Log Decoder** service.

   iii. Under **Actions**, select **View** > **System**.

   iv. In the toolbar, click **Start Capture**.

   Note: If the toolbar is displaying the **Stop Capture ()** icon, then capture has already started.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.