

NetWitness[®] Platform XDR

Custom JDBC Event Source Log Configuration Guide

Custom JDBC

Event Source Product Information:

Vendor: Custom

Event Source: Custom

Versions: Any version of Oracle (Unified auditing on Unix and Windows), IBMDB2

NetWitness Product Information:

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

Event Source Log Parser: oracle, ibmdb2 parsers

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

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

July, 2023

Contents

Configure JDBC Custom Event Source	5
Database Auditing	5
JDBC Custom Logstash Pipeline	5
Configure Databases	5
Deploy Logstash JDBC Pipelines from NetWitness Live	5
Set Up Logstash Oracle JDBC Event Sources (Pipelines) in NetWitness Platform XDR	6
Custom JDBC Collection Configuration Parameters	8
Basic Parameters	8
Advanced Parameters	9
Configure NetWitness Platform to Collect Events	11
Getting Help with NetWitness Platform XDR	12
Self-Help Resources	12
Contact NetWitness Support	12
Feedback on Product Documentation	13

Configure JDBC Custom Event Source

Database Auditing

If you are using database auditing on an Oracle Windows or Unix platform, mysql, postgres and so on, 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.

JDBC Custom Logstash Pipeline

The JDBC Custom Logstash pipeline is a flexible data ingestion pipeline that enables users to pull data from any database using Logstash, a popular open-source data processing tool.

The JDBC Custom Logstash pipeline allows customers to configure and customize the pipeline based on their specific database and requirements. This flexibility allows users to leverage different JDBC drivers, classes, log device parsers based on their choice and the databases they are working with.

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

- I. [Configure Databases](#)
- II. [Deploy Logstash JDBC Pipelines from NetWitness Live](#)
- III. [Set Up Logstash Oracle JDBC Event Sources \(Pipelines\) in NetWitness Platform XDR](#)
- IV. [Custom JDBC Collection Configuration Parameters](#)
- V. [Configure NetWitness Platform to Collect Events](#)

Configure Databases

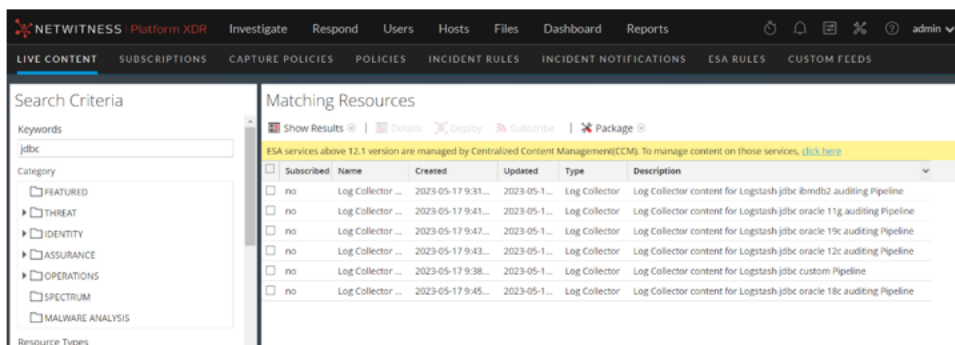
When configuring the event source specific to any database such as Oracle database or IBMDB2, it is recommended to consult the official documentation on the NetWitness community portal or configuration guides provided by the respective vendors.

Deploy Logstash JDBC Pipelines from NetWitness Live

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



To deploy Logstash JDBC Pipeline files from Live:

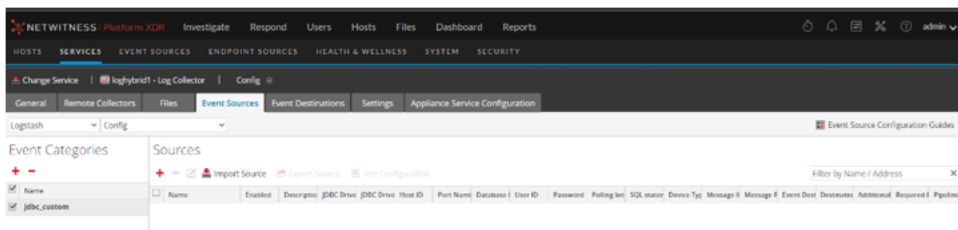
1. In the NetWitness Platform XDR menu, select **Configure > Live Content**.
2. Type **Jdbc** into the Keywords text box and click **Search** to browse Live for Logstash JDBC Custom Pipeline files.
3. Select the JDBC Custom Pipeline item returned from the search .
4. Click **Deploy** to deploy the Logstash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



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

To set up the Oracle JDBC Custom Event Source:

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.
4. In the **Event Categories** panel toolbar, click +.



5. Select **jdbc_custom** from the list and in the **Sources** panel, click + .
The **Add Source** dialog is displayed.

6. Define the parameter value described in [Custom JDBC Collection Configuration Parameters](#).

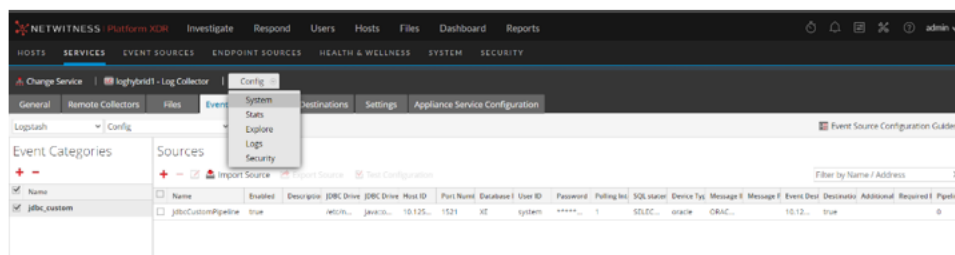
7. Click **Test Configuration**.

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.

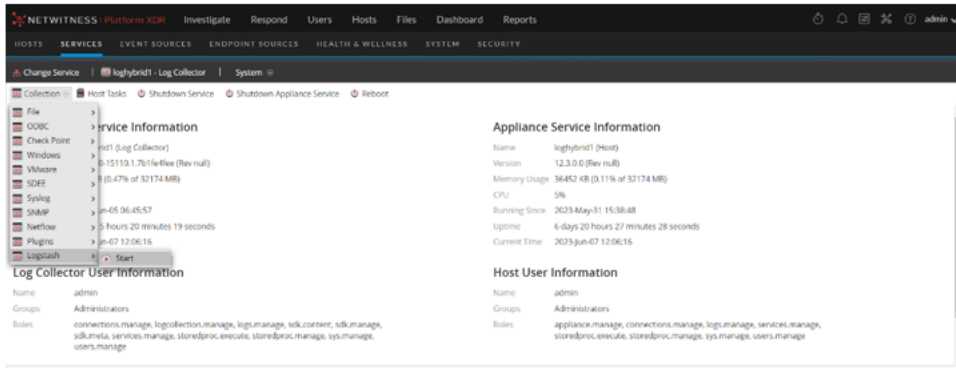
Note: The log collector may take 1 to 3 minutes to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform XDR displays a Request Timed Out error.

8. If the test is successful, click **OK**. The new event source is displayed in the **Sources** panel.

9. Save the configuration. From the **Actions** menu, choose **System**.



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



Custom JDBC Collection Configuration Parameters


The tables below list the configuration parameters required for integrating different database event source with NetWitness Platform XDR through JDBC Custom 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.
JDBC Driver Library*	Enter the JDBC driver library path to interact with a database.
JDBC Driver Class*	Enter the JDBC Driver class to interact with a database.
Host ID*	Enter the IP address of the machine where the Oracle server is installed.
Port Number*	Enter the port number that you configured for your event source. The default value of port number is 1521.
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.

Name	Description
Polling Interval*	<p>Polling interval takes the input in minutes. Based on the minutes entered, the pipeline will pull the data from the database.</p> <p>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 field takes the values between 1 to 60.</p>
SQL Statement*	Enter the SQL statements based on the requirement. Here, the text area field will also supports the new custom query.
Device Type*	Enter the device type of the event source used for parsing.
Message ID	Enter the message group ID to bypass header parsing.
Message Prefix	Enter the prefix added to each message to assist parsing.
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	<p>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.</p> <p>Caution: Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"> • Off = (default) disabled • On = enabled • Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>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.</p>
Destination SSL	Select the checkbox to communicate using destination SSL.

Name	Description
Additional Custom Configuration	<p>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.</p> <p>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.</p>
Required Plugins	<p>Specify the required plugins in a comma separated list.</p> <div data-bbox="431 571 1419 751" style="border: 1px solid green; padding: 5px;"> <p>Note:</p> <ul style="list-style-type: none"> - 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. </div>
Required Ports	<p>Enter the list of ports required for external access.</p>
Pipeline Workers	<p>Number of pipeline worker threads allocated for logstash pipeline.</p>

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 XDR 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.

By default, Log Decoders support events that are up to 32 KB in size. If the events are getting truncated on the Log Decoder, use the following procedure to change the event size:

1. Change LogDecoder REST config at `http://LogDecoder_IP:50102/decoder/config`, where `LogDecoder_IP` is the IP address of your Log Decoder.
2. Set `pool.packet.page.size` to 64 KB.
3. Restart the Log Decoder. This is required after you change the `pool.packet.page` value.

Note: If you are collecting events larger than 64 KB in size, follow instructions above in the Filter out unwanted logs section. You can drop unwanted logs or fields for a specific event source to reduce the size of the incoming data.

Getting Help with NetWitness Platform XDR

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 XDR 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 nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.