NetWitness® Platform XDR

Oracle JDBC Event Source Log Configuration Guide

NETWITNESS
Platform XDR

Oracle JDBC

Event Source Product Information:

Vendor: Oracle

Event Source: Oracle

Versions: Oracle 11.xg, Oracle 12c, 18c, 19c (Unified auditing on Unix and Windows)

NetWitness Product Information:

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

Event Source Log Parser: Oracle (JSON)

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 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/.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

August 2024

Contents

Configure Oracle Event Source (11g, 12c, 18c, or 19c)

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 Oracle Event Source:

I. Configure Oracle 11g for Database Auditing

II. Configure Oracle 12c, 18c, or 19c for Unified Auditing

III. Deploy Logstash JDBC Pipelines from NetWitness Live

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

V. JDBC Collection Configuration Parameters

VI. Configure NetWitness Platform to Collect Events

VII. Troubleshooting

Configure Oracle 11g for Database Auditing

These configuration instructions apply to Oracle 11g on UNIX, or on Windows systems that are collecting events through the NetWitness Platform Logstash JDBC Service and that use database auditing as the Oracle auditing method.

To configure the Oracle 11g for database auditing:

Note: Perform the following procedure on the Oracle host.

1. Determine how database parameters are stored and set in your version of Oracle:
   - Database parameters are stored in the **initORACLE_SID.ora** file, which typically resides in **$ORACLE_HOME/dbs** on UNIX systems or **%ORACLE_ HOME%\database** on Windows systems. Edit this file to set these parameters.
   - Database parameters can be stored either in a binary server parameter file (**spfile**) or in a normal parameter file (**pfile**). If Oracle is using a binary server parameter file, you set parameters by issuing **ALTER SYSTEM** commands. If Oracle is using a normal parameter file, you set parameters by editing the **initORACLE_ SID.ora** file.

2. Do one of the following to set the **AUDIT_TRAIL** parameter to **DB**:
   - If Oracle is using a normal parameter file, edit the file to set AUDIT_TRAIL as follows:

     ```
     AUDIT_TRAIL = DB
     ```
   - If Oracle is using a binary server parameter file, run the following command:

     ```
     ALTER SYSTEM SET AUDIT_TRAIL=DB SCOPE=SPFILE;
     ```

     Note: If using the NetWitness Platform, **AUDIT_TRAIL** may be set to **DB** or **DBExtended**.
3. Create an Oracle database user with the user name **audit_reader**.
4. Depending on the version, grant below SELECT privileges for the user audit_reader:
   - In Oracle 18c or 19c: Grant **SELECT** privileges for the audit_reader user on the **SYS.UNIFIED_AUDIT_TRAIL** and the **SYS.V_$INSTANCE** view. To grant these privileges, run the following commands:

     ```
     GRANT SELECT ON SYS.UNIFIED_AUDIT_TRAIL to audit_reader;
     GRANT SELECT ON SYS.V_$INSTANCE to audit_reader;
     ```
   - In other lower versions: Grant **SELECT** privileges for the audit_reader user on the **SYS.AUD$** table and the **SYS.V_$INSTANCE** view. To grant these privileges, run the following commands:

     ```
     GRANT SELECT ON SYS.AUD$ to audit_reader;
     GRANT SELECT ON SYS.V_$INSTANCE to audit_reader;
     ```
5. Connect to the monitored instance as a privileged user by using a tool such as SQL*Plus.
6. To enable auditing for logon and logoff functions only, run the following command:

   ```
   audit session
   ```
7. (Optional) To enable auditing for specific user names, run the following commands:

   ```
   AUDIT ALL BY USERNAME BY ACCESS;
   AUDIT SELECT TABLE, UPDATE TABLE, DELETE TABLE BY USERNAME BY ACCESS;
   AUDIT EXECUTE PROCEDURE BY USERNAME BY ACCESS;
   ```

   where username is the user name that you want to audit.

   Note: For information on auditing, go to http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/cfgaudit.htm#BABCBJHG.
8. Disconnect from and reconnect to the instance. Oracle will generate audit logs.
9. Restart Oracle.
10. Ensure that JDBC connection parameters are set up correctly in the Oracle Net Configuration Assistant.

Configure Oracle 12c, 18c, or 19c for Unified Auditing

These configuration instructions apply to Oracle 12c, 18c, or19c on Windows or Unix systems that are collecting events through the RSA NetWitness Platform JDBC Service and that use unified auditing as the Oracle auditing method.

To configure the Oracle 12c, 18c, or 19c for unified auditing in Windows:

1. Shutdown the database.
2. Stop the Oracle service.
3. Stop the listener.
4. In Oracle 12c, 18c, or 19c, rename the **dll** files on the Windows system accordingly:
   - For 12c, **%ORACLE_HOME%/bin/orauniaud12.dll.dbl** file to **%ORACLE_HOME%/bin/orauniaud12.dll**
   - For 18c, **%ORACLE_HOME%/bin/orauniaud18.dll.dbl** file to **%ORACLE_HOME%/bin/orauniaud18.dll**
   - For 19c, **%ORACLE_HOME%/bin/orauniaud19.dll.dbl** file to **%ORACLE_HOME%/bin/orauniaud19.dll**
5. Restart the items you stopped earlier.
   - Start the listener.
   - Start the Oracle service.
   - Start up the database.

To configure the Oracle 12c, 18c, or 19c for unified auditing in Unix:

Note: If you are running Oracle on Unix, perform the following procedure on the Oracle host.

1. Run the following commands to link the database into the Unix kernel:

```
cd $ORACLE_HOME/rdbms/lib
make -f ins_rdbms.mk uniaud_on ioracle ORACLE_HOME=$ORACLE_HOME
```

2. Restart the Oracle database.

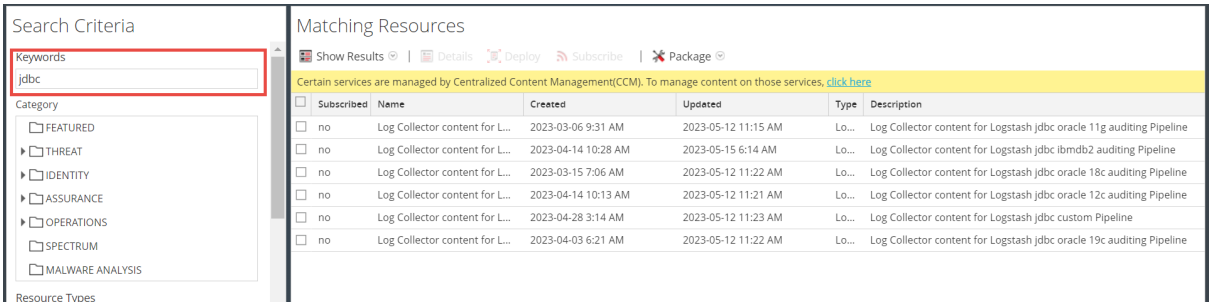
Deploy Logstash JDBC Pipelines from NetWitness Live

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 Pipeline files.
3. Select the item returned from the search based on the DB version.
4. Click **Deploy** to deploy the Logstash JDBC Pipeline files to the appropriate Log Collector in the

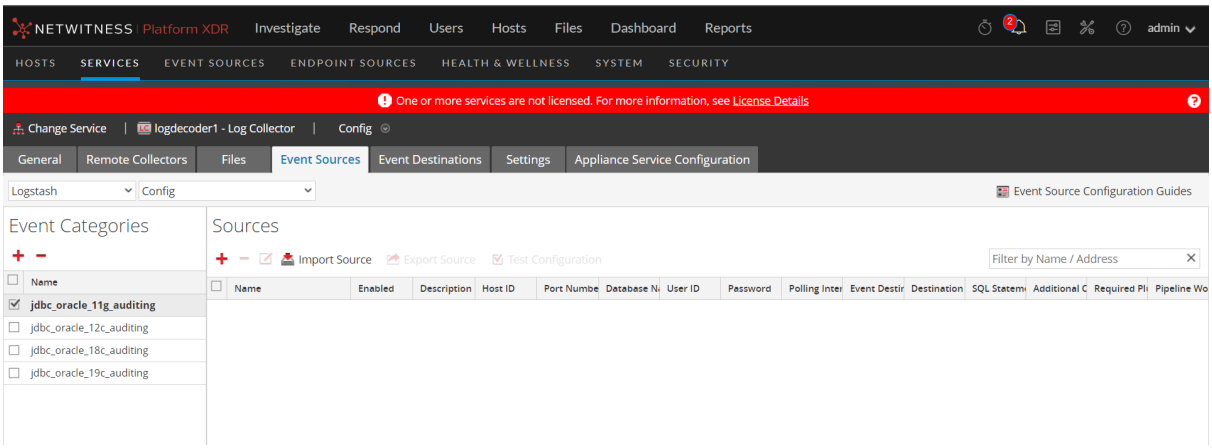
Deployment Wizard.



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

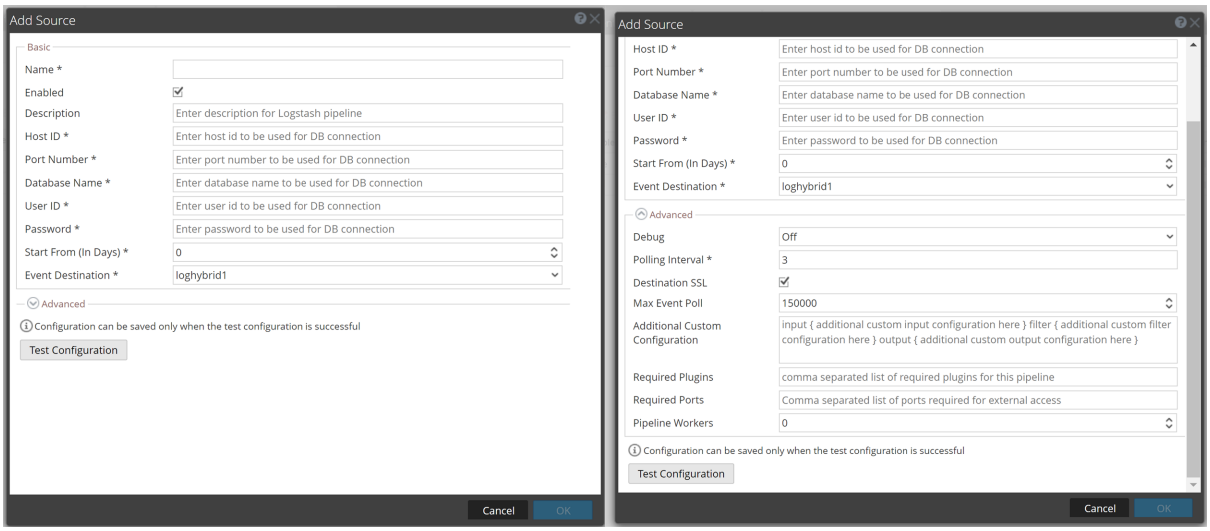
To set up the Oracle JDBC Event Source:

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 Oracle Pipelines** based on the db versions (jdbc_oracle_11g_auditing, jdbc_oracle_12c_auditing, jdbc_oracle_18c_auditing, or jdbc_oracle_19c_auditing) from the list and in the **Sources** panel, click + .

   The **Add Source** dialog is displayed.

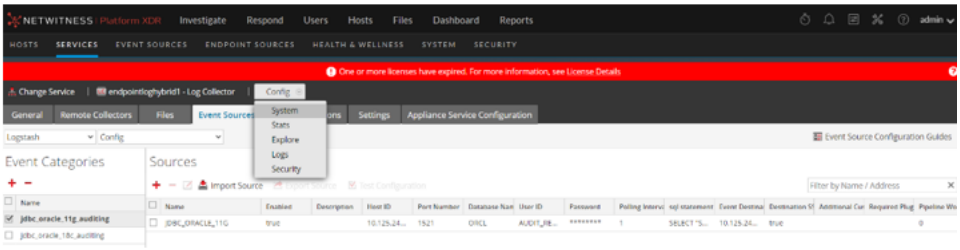


6. Define the parameter value described in JDBC Collection Configuration Parameters.
7. Click **Test Configuration**.

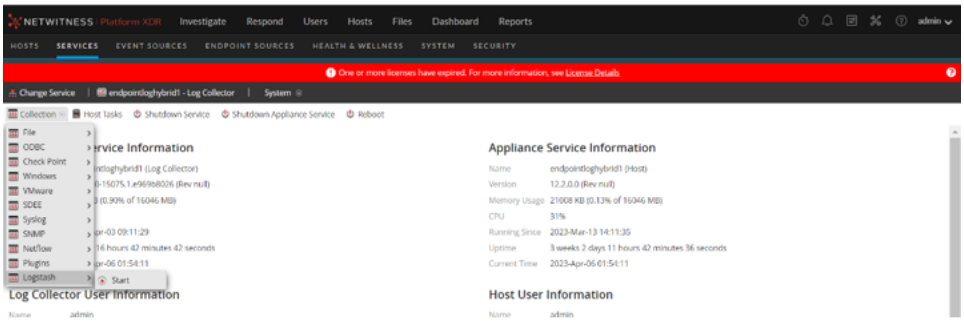
   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information based on message shown and retry.

   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.



JDBC Collection Configuration Parameters

The tables below list the configuration parameters required for integrating Oracle event source (Oracle 11g, 12c, 18c, or 19c) with NetWitness Platform XDR through JDBC 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 checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Description	Enter a text description for the event source.
Host ID*	Enter the IP address of the machine where the oracle database server is installed.
Port Number*	Enter the port number that you configured for your event sources. The default value of port number is 1521.
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 tables 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.
Max Event Poll	The maximum number of events to pull from the event source during one polling cycle. The default value is 150000.
Custom SQL Statement*	By default, this is an empty text area field. This field will take any valid custom SQL query to run and collect the data from database.
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.

   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.

Troubleshooting

Issue	Explanation
Collection from the JDBC pipeline is not happening	Follow these steps to check if collection from the JDBC pipeline is not happening: • Check if the logstash protocol is started from **Logcollector->System->Collection->Logstash**. • Check if the destination host while creating the logstash pipeline is selected correctly. • From backend, check for any errors in **pipeline.conf** file located in the path **/var/log/logstash/<logstash jdbc pipeline>.log**. • Check for incorrect username in the configuration. If the user name configuration is incorrect, the below warning and error message is displayed in the back-end:

```
[2024-07-19T10:38:59,981][WARN ][logstash.inputs.jdbc     ] Exception when executing
JDBC query {:exception=>Sequel::DatabaseConnectionError,
:message=>"Java::JavaSql::SQLException: ORA-01017: invalid username/password; logon
denied\n", :cause=>"#<Java::JavaSql::SQLException: ORA-01017: invalid
username/password; logon denied\n>"}
[2024-07-19T10:39:00,365][ERROR][logstash.javapipeline    ] Pipeline error
{:pipeline_id=>"jdbc_oracle_11g_auditing_test", :exception=>#
<LogStash::ConfigurationError: Can't create a connection pool to the database>,
:backtrace=>["/usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/logstash-integration-
jdbc-5.4.8/lib/logstash/inputs/jdbc.rb:318:in `register'",
"/usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/logstash-mixin-
ecs_compatibility_support-1.3.0-
java/lib/logstash/plugin_mixins/ecs_compatibility_support/target_check.rb:48:in
`register'", "/usr/share/logstash/logstash-core/lib/logstash/java_pipeline.rb:237:in
`block in register_plugins'", "org/jruby/RubyArray.java:1989:in `each'",
"/usr/share/logstash/logstash-core/lib/logstash/java_pipeline.rb:236:in
`register_plugins'", "/usr/share/logstash/logstash-
core/lib/logstash/java_pipeline.rb:395:in `start_inputs'",
"/usr/share/logstash/logstash-core/lib/logstash/java_pipeline.rb:320:in
`start_workers'", "/usr/share/logstash/logstash-
core/lib/logstash/java_pipeline.rb:194:in `run'", "/usr/share/logstash/logstash-
core/lib/logstash/java_pipeline.rb:146:in `block in start'"], "pipeline.sources"=>
["/etc/logstash/conf.d/pipelines/jdbc_oracle_11g_auditing_test/pipeline.conf"],
:thread=>"#<Thread:0x4928ba3e /usr/share/logstash/logstash-
core/lib/logstash/java_pipeline.rb:134 run>"}
```

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.