NetWitness® Platform

Oracle Database Event Source Log Configuration Guide

NETWITNESS
Platform

Oracle Database

Event Source Product Information:

Vendor: Oracle

Event Source: Oracle

Versions: 8*i*, 9*i*, 10*g*, 11.x*g*, 12*c* (Mixed mode auditing and Unified auditing on Windows), 12*c* (Unified auditing on Unix), 18c (Unified auditing on Unix and Windows),19c (Unified auditing on Unix and Windows)

Additional Downloads:
nicsftpagent.conf.oracle,
nicsftpagent.conf.oraclexml (for XML Auditing)

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 or later

Event Source Log Parser: oracle

Collection Method: Syslog, ODBC, File and 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.

November 2024

Contents

Oracle Overview

Oracle provides several types of auditing. To integrate with the NetWitness Platform, you can choose among several collection methods, depending on the kind of Oracle auditing method that you want to use.

Note: In Oracle, you must select exactly one method of auditing: database, file system, or syslog. In addition, you can optionally choose fine-grain auditing.

File System Auditing

If you are using file system auditing on an Oracle Windows or Unix platform, you can collect messages through the NetWitness Platform File Reader Service. Collecting messages in this manner has the following advantages:

- File system auditing collects messages for all of the database instances on an Oracle Server. If you use database auditing, you must configure collection for each database instance on the Oracle Server.
- File system auditing allows you to collect administrator messages, in addition to the database messages.
- File system auditing allows collection of shutdown and restart messages.

Collection of file system messages is supported in the NetWitness Platform for all supported versions of the Oracle database event source. To integrate Oracle file system auditing with the NetWitness Platform, see Configure Oracle 8i, 9i,10g, 11g for File System Auditing.

Database Auditing

If you are using database auditing on an Oracle Windows or Unix platform, you can collect messages through the NetWitness Platform ODBC Service. Collecting messages in this manner 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.

Collection of database messages is supported in NetWitness Platform for Oracle 10g or 11g. To integrate Oracle database auditing with NetWitness Platform, see Configure Oracle 10g or 11g for Database Auditing.

XML Auditing

Collection of messages from an XML file is very similar to collecting via Database Auditing. If you are using Oracle 10 or 11g on a Windows or UNIX platform (or Oracle 12*c* Mixed mode auditing on Windows), you can configure this method. Collecting messages in this manner has the following advantages:

- This method is file-based, and therefore avoids the overhead associated with calls to the database.
- NetWitness Platform automatically deletes all intermediate files associated with this collection method, which can reduce the amount of storage used by NetWitness Platform.

If you configure XML auditing, you do not need to configure Database Auditing, as both methods collect the same messages. To integrate XML Auditing with NetWitness Platform, see Configure Oracle 10g or 11g for XML Auditing.

Syslog Auditing

If you are using syslog auditing on an Oracle 10g or 11g version on a Unix platform, you can collect messages through syslog collection. Collecting messages in this manner has the following advantages:

- Syslog auditing is very similar to file system auditing, and thus provides most of the same advantages.
- Syslog auditing is the easiest collection method to configure on NetWitness Platform. For details, see Configure Oracle 10g or 11g for Syslog Auditing.

IMPORTANT: Oracle 10*g* and 11*g* for Syslog Auditing does not work for Solaris. The integration of Oracle and Solaris produces multi-line logs which are not supported by NetWitness Platform.

Fine Grained Auditing

In addition to choosing one of the primary auditing methods, Oracle provides fine-grained auditing. This type of auditing is useful when you are adding specific rules, for example to closely monitor the actions of a user or small group of users.

If you are using the Content 2.0 version of the Oracle definition files, and Oracle version 10g or 11g, then you can configure fine-grained auditing. For details, see Configure Oracle 10g or 11g for Fine Grain Auditing.

Windows Mixed Mode Auditing for Oracle version 12*c*

NetWitness has added the following support for Oracle 12c on Microsoft Windows in Mixed mode auditing:

- Database auditing via ODBC Collection
- XML auditing via File Collection
- Fine Grained Auditing via ODBC Collection

Unified Auditing for Oracle Version 18*c* or 19*c*

NetWitness has added support for Oracle 18c or 19*c* on Windows and Unix in Unified Auditing:

- Database auditing via ODBC Collection

Unified Auditing for Oracle version 12*c*,18*c* or 19*c*

Oracle Database 12*c*,18*c* or 19*c* Unified Auditing enables selective and effective auditing inside the Oracle database, using policies and conditions. The new policy-based syntax simplifies management of auditing within the database and provides the ability to accelerate auditing based on conditions.

For example, audit policies can be configured to audit based on specific IP addresses, programs, time periods, or connection types (such as proxy authentication).

Note: On a Windows system, in Oracle version 12*c* you can either collect using Mixed mode auditing or Unified Auditing.

To collect logs in Unified Auditing mode (on Windows or Unix), you must use ODBC collection from the **UNIFIED_AUDIT_TRAIL** table.

Configure Oracle 10g 11g,12c,18c or 19c for Database Auditing

These configuration instructions apply to Oracle 10*g* or 11*g* on UNIX, or on Windows systems that are collecting events through the NetWitness Platform ODBC Service and that use database auditing as the Oracle auditing method.

These configuration instructions apply to Oracle 10*g* or 11*g* on UNIX.

These configuration instructions apply to the following:

- Oracle 10*g* or 11*g* on UNIX
- Oracle 12*c* Mixed mode auditing on Windows platforms that collect events through the NetWitness Platform ODBC Service and use database auditing as the Oracle auditing method.
- Oracle 18c Unified Auditing on UNIX or Windows
- Oracle 19c Unified Auditing on UNIX or Windows
- To configure unified auditing see Configure Oracle 12*c*, 18*c* or 19*c* for Unified Auditing.

See the following sections for details:

- Set up the Oracle event source
- Configure NetWitness Platform for ODBC Collection from Oracle Database

Set up the Oracle Event Source

Perform the following procedure on the Oracle host.

To configure Oracle for database auditing:

1. Determine how database parameters are stored and set in your version of Oracle:
   - Database parameters are stored in the **init*ORACLE_SID*.ora** file, which typically resides in **$ORACLE_HOME/dbs** on UNIX systems or **%ORACLE_HOME%\database** on Windows systems. To set parameters, you edit this file.
   - 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 **init*ORACLE_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 12c, 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 ODBC connection parameters are set up correctly in the Oracle Net Configuration Assistant.

    Note: In addition to the parameters as documented in the Oracle documentation, make sure to set up the Listener on port 1521.

Configure NetWitness Platform for ODBC Collection from Oracle Database

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

I. Ensure the required parser is enabled

II. Configure a DSN

III. Add the Event Source Type

IV. Restart the ODBC Collection Service

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 NetWitness Platform Live.

Ensure that the parser for your event source is available:

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 **oracle**.

Configure a DSN

Create the ODBC data source with the user **audit_reader** (created when you **Set up the Oracle Event Source**). You must add one data source for each Oracle server.

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select (Admin) > **Services**.
2. In the Services grid, select a Log Collector service and from the **Actions** ( ) menu, choose **View** > **Config** > **Event Sources**.
3. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
4. The DSNs panel is displayed with the existing DSNs, if any.
5. Click + to open the **Add DSN** dialog.

   Note: To add a DSN template, see the **Configure a DSN** topic in the *Log Collection Configuration Guide*, available in NetWitness Community.
6. Choose a **DSN Template** from the drop down menu and enter a name for the DSN. (Use this name when you set up the ODBC event source type.)
7. Fill in the parameters and click **Save**.

Field	Description
DSN Template (Security Analytics 10.4 and newer)	Choose the correct Oracle template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
ServiceName	Enter the service name
PortNumber	The default port number is **1521**
HostName	Specify the hostname or IP Address of the Oracle database
Edition Name	Enter the name of the Oracle edition **IMPORTANT:** If you are using version 11g or 18c, DO NOT enter an edition. If you enter a value, collection will not work.
Driver	If you choose one of the native templates, select one of the following drivers, depending on your NetWitness Log Collector version and Oracle version: • For Oracle Database versions 12c or 19c, use **/opt/netwitness/odbc/lib/R3ora28.so**. This driver is included with NetWitness Platform version **11.2.1/10.6.6.1** and later. • For Oracle Database version 18c, use **/opt/netwitness/odbc/lib/R3ora28.so** or **/opt/netwitness/odbc/lib/R3ora27.so** • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3ora27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3ora26.so If you choose one of the server templates, you need to point to the correct driver file on the Oracle server.

Add the Event Source Type

In step 6 below, select one of the following from the **Available Event Source Types** dialog:

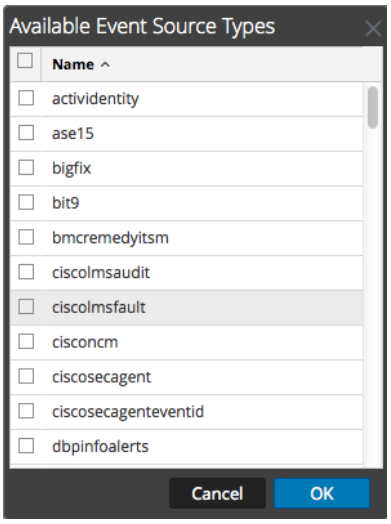
- **oracle_unified_audit_19c** for Oracle v19c Unified Auditing
- **oracle_unified_audit_18c** for Oracle v18c Unified Auditing
- **oracle_unified_audit_12c** for Oracle 12c Unified auditing: going forward, use this file, as this will be updated via live, while **oracle_12c_auditing** will no longer be updated
- **oracle_11g_auditing** for Oracle v11g and v12c Mixed mode auditing
- **oracle_10g_auditing** for Oracle 10g
- **oracle_9i_auditing** for Oracle 9i
- **oracle_8i_auditing** for Oracle 8i

Note: If the necessary event source type is not listed check NetWitness Live for any related NetWitness Log Collector content that may apply.

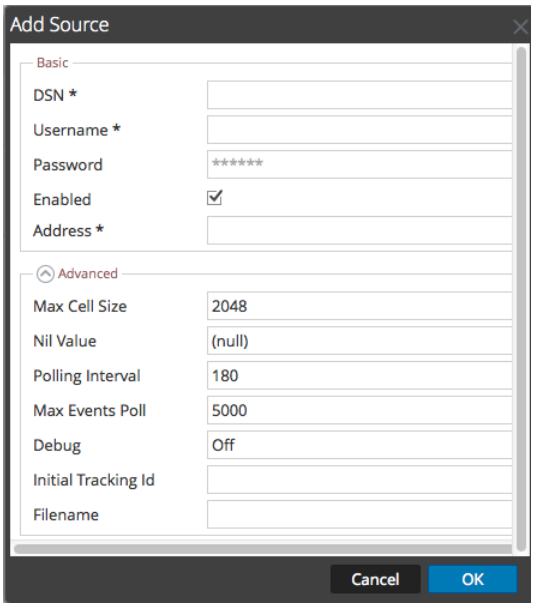
Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select (Admin) > **Services**.
2. In the Services grid, select a Log Collector service, and from the **Actions** ( ) menu, choose **View** > **Config** > **Event Sources**
3. 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.
4. Click + to open the **Available Event Source Types** dialog.



5. Select **mswsus** and click **OK**.
6. Fill in the parameters and click **Save**.
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 *Log Collection Configuration Guide*.

Restart the ODBC Collection Service

Restart the ODBC collection service:

1. In the **Security Analytics** menu, select (Admin) > **Services**.
2. In the Services grid, select a Log Collector service, and from the **Actions** ( ) menu, choose **View** > **System**.
3. Click **Collection** > **ODBC**.
   - If the available choice is **Start**, click **Start** to start ODBC collection.
   - If the available choices are **Stop** and **Pause**, click **Stop**, wait a few moments, and then click **Start**.

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

These configuration instructions apply to Oracle 12*c*, 18*c* or 19*c* on Windows or Unix systems that are collecting events through the NetWitness Platform ODBC Service and that use unified auditing as the Oracle auditing method.

After you configure the Oracle event source, you must perform the steps described in Configure NetWitness Platform for ODBC Collection from Oracle Database.

Windows: Configure Oracle 12*c*, 18*c* or 19*c* for Unified Auditing

If you are running Oracle on Windows, perform the following procedure on the Oracle host.

To enable Oracle unified auditing on Windows:

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

Unix: Configure Oracle 12*c*, 18*c* or 19*c* for Unified Auditing

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

To enable Oracle unified auditing on Unix:

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.

Configure Oracle 10*g*, 11*g*, or 12*c* for XML Auditing

Configuration Instructions for XML Auditing

These configuration instructions apply to the following:

- Oracle 10*g*, or 11*g* on UNIX
- Oracle 12*c* Mixed mode auditing on Windows platforms that collect events through the NIC File Reader Service and use XML auditing as the Oracle auditing method.

To configure Oracle for XML auditing:

1. On the Oracle host, perform the following steps:

   a. Determine how database parameters are stored and set in your version of Oracle:

      - Database parameters are stored in the **init*ORACLE_SID*.ora** file, which typically resides in **$ORACLE_HOME/dbs**. To set parameters, you edit this file.
      - 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 **init*ORACLE_SID*.ora** file.

   b. Do one of the following to set the **AUDIT_TRAIL** parameter to **OS**:

      - If Oracle is using a normal parameter file, edit the file to set **AUDIT_TRAIL** as follows:

        ```
        AUDIT_TRAIL = XML
        ```

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

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

   c. Do one of the following to set the **AUDIT_FILE_DEST** parameter to ***directory***, where directory is the directory where you want Oracle to generate audit (**ora_pid.xml**) files:

      - If Oracle is using a normal parameter file, edit the file to set **AUDIT_FILE_DEST** as follows:

        ```
        AUDIT_FILE_DEST = directory
        ```

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

        ```
        ALTER SYSTEM SET AUDIT_FILE_DEST=directory SCOPE=SPFILE;
        ```

        Note: On some operating systems, certain messages will always be logged to the default location **$ORACLE_HOME/rdbms/audit**, regardless of the **AUDIT_FILE_DEST** parameter.

   d. (Optional) To enable full auditing of administrative accounts, do one of the following to set the **AUDIT_SYS_OPERATIONS** parameter:

- If Oracle is using a normal parameter file, edit the file to set **AUDIT_SYS_OPERATIONS** as follows:

  ```
  AUDIT_SYS_OPERATIONS = TRUE
  ```

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

  ```
  ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE;
  ```

By default, the **AUDIT_TRAIL** parameter sends only the following messages to the audit log:

- Connections to the instance with administrator privileges
- Database startup
- Database shutdown

If full auditing of administrative accounts is enabled, all users who connect to the database with SYS or as SYSDBA or SYSOPER have their commands written to an **ora_*pid*.xml** file.

e. Using a tool such as SQL*Plus, connect to the monitored instance as a privileged user.

f. To enable auditing for logon and logoff functions only, run the following command:

```
audit session
```

g. Disconnect from and reconnect to the instance. Oracle begins generating audit logs.

h. Restart Oracle.

2. Set up the SFTP Agent Collector on the NetWitness Platform.
   - If you are on a Windows platform, see the Install and Update SFTP Agent topic.
   - If you are on a Linux platform, see the Configure SFTP Shell Script File Transfer topic.
3. Configure the Log Collector for File Collection, as described in the following section.

Configure the Log Collector for File Collection

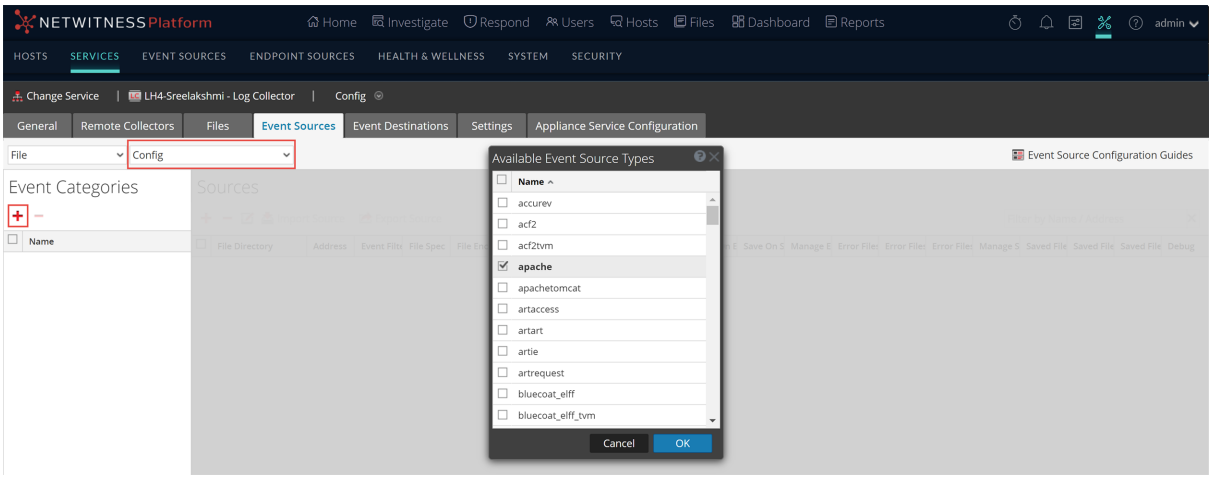
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the NetWitness Platform menu, select  (Admin) > **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.

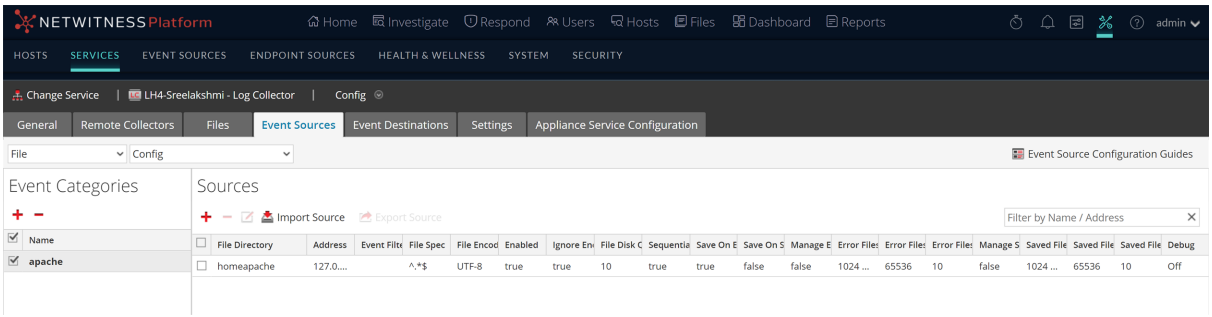
   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.



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

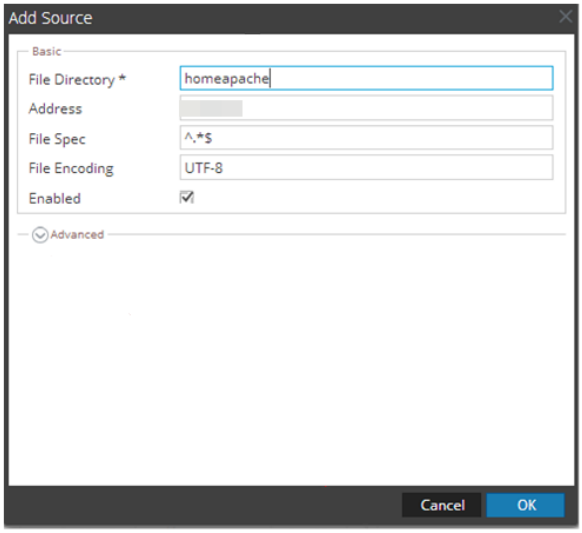
   The newly added event source type is displayed in the Event Categories panel.

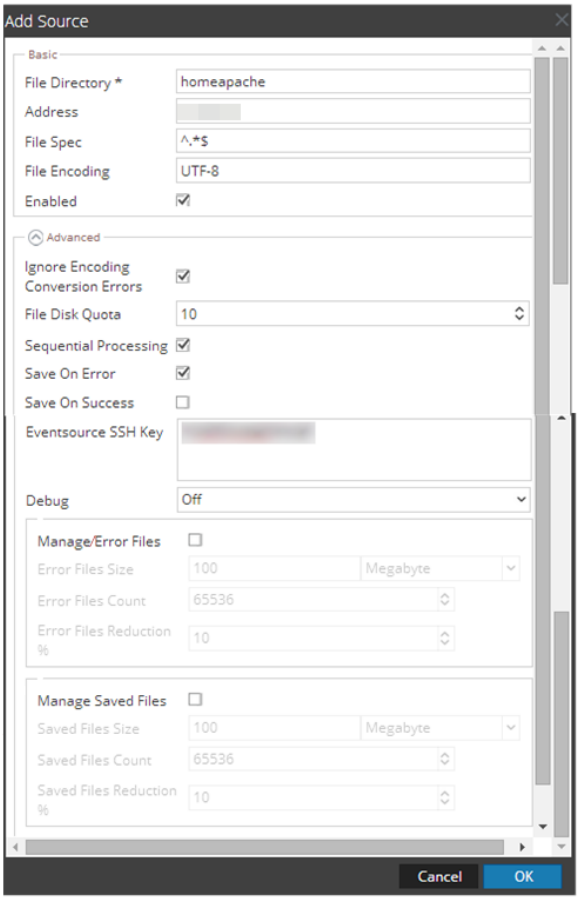


   Select **oraclexml** from the **Available Event Source Types** dialog.

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

   The Add Source dialog is displayed.





7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
8. Configure the NetWitness Platform Upload Directories. After you have added and configured the event source using the NetWitness Platform GUI, you must configure the upload directories correctly.
   a. Change to the `/var/netwitness/logcollector` directory.
   b. Change the owner of the upload directory to the **sftp** user:

      ```
      chown sftp /var/netwitness/logcollector/upload
      ```

   c. Change the group for the upload directory to the **sftp** user:

      ```
      chgrp -R sftp /var/netwitness/logcollector/upload
      ```

   d. Ensure the /upload directory has the correct permissions:

      ```
      chmod -R 775 /var/netwitness/logcollector/upload
      ```

   e. **Optional**: Set up a cron job to run the script at the time intervals that you wish. If you set up a cron job, make sure to run it as that **sftp** user.

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

Configure Oracle 8*i*, 9*i*, 10*g*, or 11*g* for File System Auditing

Configuration Instructions for File System Auditing

These configuration instructions apply to Oracle 8*i*, 9*i*,10*g*, or 11*g* on UNIX that uses file system auditing as the Oracle auditing method.

Note: Use Oracle file system auditing only on UNIX systems.

To configure Oracle for file system auditing:

1. On the Oracle host, perform the following steps:
   a. Determine how database parameters are stored and set in your version of Oracle:
      - Database parameters are stored in the **init*ORACLE_SID*.ora** file, which typically resides in **$ORACLE_HOME/dbs**. To set parameters, you edit this file.
      - 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 **init*ORACLE_SID*.ora** file.
   b. Do one of the following to set the **AUDIT_TRAIL** parameter to **OS**:
      - If Oracle is using a normal parameter file, edit the file to set **AUDIT_TRAIL** as follows:
        `AUDIT_TRAIL = OS`
      - If Oracle is using a binary server parameter file, run the following command:
        `ALTER SYSTEM SET AUDIT_TRAIL=OS SCOPE=SPFILE;`
   c. Do one of the following to set the **AUDIT_FILE_DEST** parameter to ***directory***, where directory is the directory where you want Oracle to generate audit (**ora_pid.aud**) files:
      - If Oracle is using a normal parameter file, edit the file to set **AUDIT_FILE_DEST** as follows:
        `AUDIT_FILE_DEST = directory`
      - If Oracle is using a binary server parameter file, run the following command:
        `ALTER SYSTEM SET AUDIT_FILE_DEST=directory SCOPE=SPFILE;`

        Note: On some operating systems, certain messages will always be logged to the default location **$ORACLE_HOME/rdbms/audit**, regardless of the **AUDIT_FILE_DEST** parameter.
   d. (Optional) To enable full auditing of administrative accounts, do one of the following to set the **AUDIT_SYS_OPERATIONS** parameter:

- If Oracle is using a normal parameter file, edit the file to set **AUDIT_SYS_OPERATIONS** as follows:

  ```
  AUDIT_SYS_OPERATIONS = TRUE
  ```

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

  ```
  ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE;
  ```

By default, the **AUDIT_TRAIL** parameter sends only the following messages to the audit log:

- Connections to the instance with administrator privileges
- Database startup
- Database shutdown

If full auditing of administrative accounts is enabled, all users who connect to the database with SYS or as SYSDBA or SYSOPER have their commands written to an **ora_*pid*.aud** file.

e. Using a tool such as SQL*Plus, connect to the monitored instance as a privileged user.

f. To enable auditing for logon and logoff functions only, run the following command:

```
audit session
```

g. Disconnect from and reconnect to the instance. Oracle begins generating audit logs.

h. Restart Oracle.

2. Set up the SFTP Agent Collector on the NetWitness Platform.
   - If you are on a Windows platform, see the Install and Update SFTP Agent topic.
   - If you are on a Linux platform, see the Configure SFTP Shell Script File Transfer topic.
3. Configure the Log Collector for File Collection, as described in the following section.

Configure the Log Collector for File Collection

Perform the Configure the Log Collector for File Collection procedure under **Configure Oracle 10*g*, 11*g*, or 12*c* for XML Auditing**.

In step 5 of that procedure, select **oracle** from the **Available Event Source Types** dialog.

Configure Oracle 10*g* or 11*g* for Syslog Auditing

Warning: Use Oracle syslog auditing only on UNIX systems, except Solaris (Oracle 10*g*).

Note: These configuration instructions support Oracle 10.2.0.1 and 11.0.1.6.

To configure Oracle for syslog auditing:

1. On the Oracle host, perform the following tasks:
   a. Determine how database parameters are stored and set in your version of Oracle:
      - Database parameters are stored in the **init*ORACLE_SID*.ora** file, which typically resides in **$ORACLE_HOME/dbs**. To set parameters, you edit this file.
      - 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.

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

        ```
        AUDIT_TRAIL = OS
        ```

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

        ```
        alter system set audit_trail=os scope=spfile;
        ```

   c. Do one of the following to set the **AUDIT_SYS_OPERATIONS** parameter:
      - If Oracle is using a normal parameter file, set **AUDIT_SYS_OPERATIONS** as follows:

        ```
        AUDIT_SYS_OPERATIONS = TRUE
        ```

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

        ```
        alter system set audit_sys_operations=true scope=spfile;
        ```

   d. Do one of the following to set the **AUDIT_SYSLOG_LEVEL** parameter:
      - If Oracle is using a normal parameter file, set **AUDIT_SYSLOG_LEVEL** as follows:

        ```
        AUDIT_SYSLOG_LEVEL = 'FACILITY.PRIORITY'
        ```

        where *FACILITY* is between LOCAL0 to LOCAL7, USER, or SYSLOG

        and *PRIORITY* is one of the following: NOTICE, INFO, DEBUG, WARNING, ERR, CRIT, ALERT, or EMERG.

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

        ```
        alter system set audit_syslog_level='FACILITY.PRIORITY'
        scope=spfile;
        ```

        where *FACILITY* is between LOCAL0 to LOCAL7, USER, or SYSLOG

and *PRIORITY* is one of the following: NOTICE, INFO, DEBUG, WARNING, ERR, CRIT, ALERT, or EMERG.

Note: For information on values for **AUDIT_SYSLOG_LEVEL**, see http://download.oracle.com/docs/cd/B28359_01/server.111/b28320/initparams016.htm

e. Using a tool such as SQL* PLUS, connect to the monitored instance as a privileged user.

f. Disconnect from and reconnect to the instance. Oracle begins generating audit logs.

g. Restart Oracle.

2. Log on to your Linux machine, and open the **/etc/syslog.conf** file in a text editor.

3. To log all messages at the debug level and higher, add the following line:

   FACILITY.PRIORITY @xxx.xxx.xxx.xxx

   where *FACILITY* is the value you entered in step 1

   PRIORITY is the value you entered in step 1

   xxx.xxx.xxx.xxx is the IP address of the NetWitness Platform Log Decoder or NetWitness Platform Remote Log Collector.

4. Save the file.

5. Open a command prompt, and to restart the syslog service, type:

   ```
   service syslog restart
   ```

Configure Oracle 10*g*, 11*g*, or 12*c* for Fine Grain Auditing

This section describes how to configure Oracle 10*g*, 11*g*, or 12*c* (Mixed mode auditing on Windows) for Fine Grain Auditing.

To set up the Oracle Database and enable policies for Fine Grain Auditing:

1. Create an Oracle database user with the user name **audit_reader**.
2. Grant SELECT privileges for the audit_reader user on the SYS.AUD$ table, grant select on SYS.DBA_FGA_AUDIT_TRAIL to audit_reader, and grant select on SYS.FGA_LOG$ to audit_reader.
3. Enable policies for Fine Grain Auditing.
4. Add Oracle ODBC as a Data Source. Refer to Configure NetWitness Platform for ODBC Collection from Oracle Database. When performing that task, remember to select **oracle_fga** from the **Available Event Source Types** dialog,

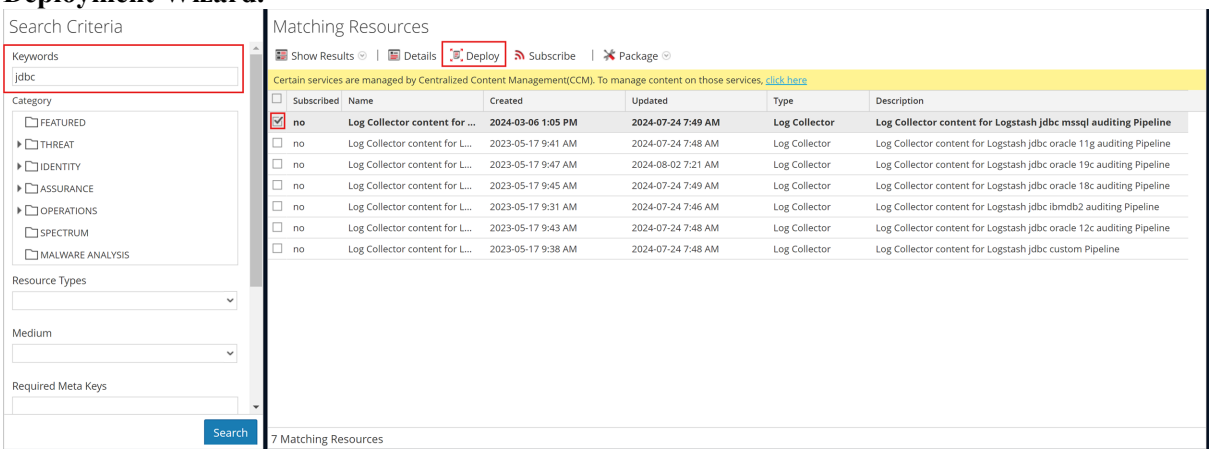
Configure NetWitness Platform for Logstash Collection

Deploy Logstash JDBC Pipeline from NetWitness Live

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

To deploy Logstash JDBC Pipeline files from Live:

1. In the NetWitness Platform 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.**

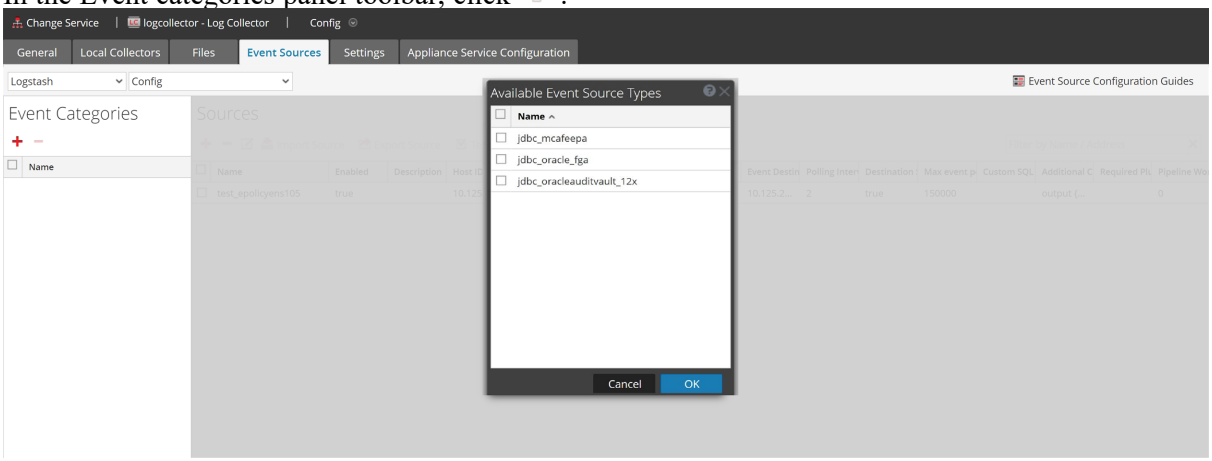


Setup Logstash Oracle Fine Grain Auditing JDBC Event Sources (Pipelines) in NetWitness Platform

To setup the Fine Grain Auditing JDBC Event Source:

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

4. In the Event categories panel toolbar, click  .

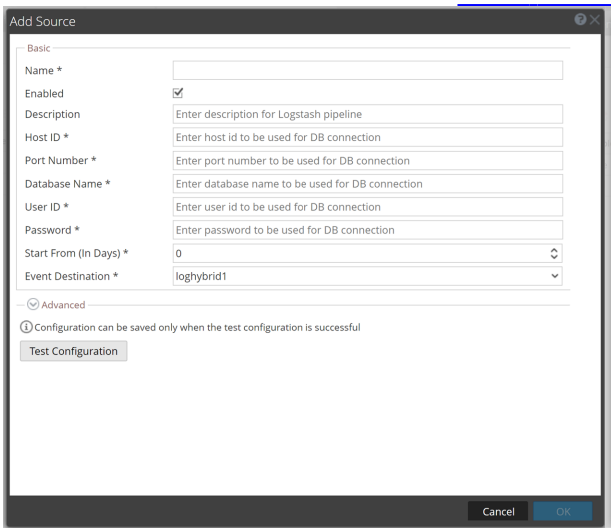


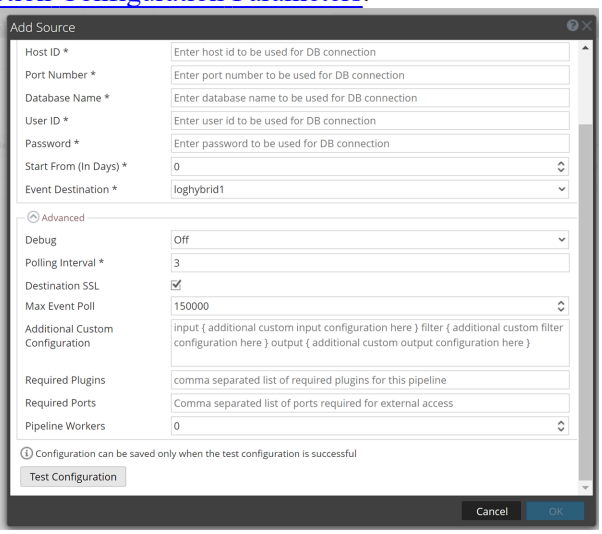
5. Select **jdbc_oracle_fga** from the **Available Event Source Types** list.

6. In the **Sources** panel, click  .

   The **AddSource** dialog box is displayed.

7. Define the Parameter described in the JDBC Collection Configuration Parameters.





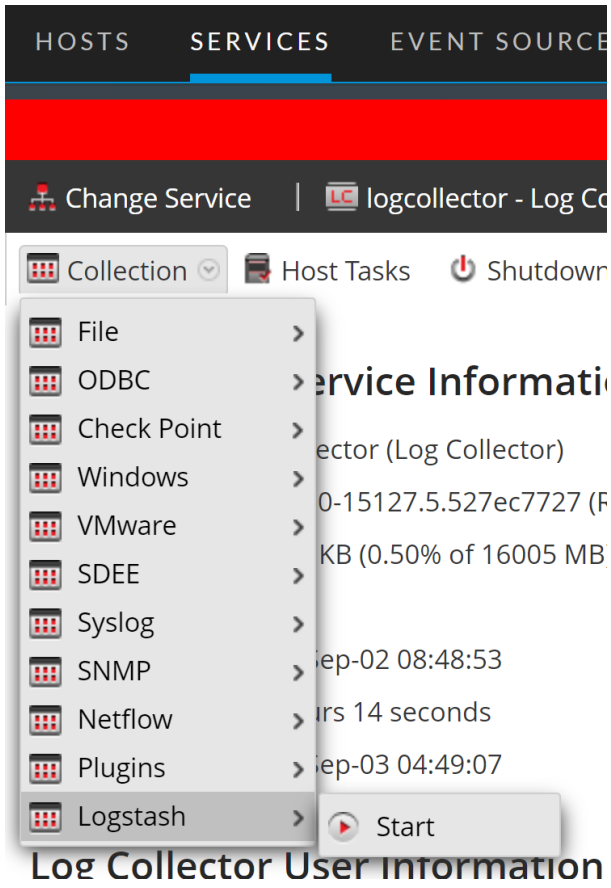
8. Click **Test Configuration**.

   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 displays a Request Timed Out error.

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

10. Save the configuration. From the Actions menu, choose System and in the Collection drop-down menu, select **Logstash > Start** to start the log collection, if it's not started already.



JDBC Collection Configuration Parameters

The tables below list the configuration parameters required for integrating different database event source with NetWitness Platform 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 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 machine where the database server is installed.
Port Number*	Enter the port number that you configured for your event source. The default value of port number is 1433.

Name	Description
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 database.
Password*	Enter the password to log into the database.
PollingInterval*	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.

Name	Description
Polling Interval*	Enter the polling interval in minutes (1-60). This determines how often data is pulled from the database. The default value is set to 3.
Destination SSL	Select the checkbox to communicate using destination SSL.
Max Event Poll	Specify the maximum number of events that can be collected during a polling cycle. By default, this is set to 1,50,000 which is also the maximum value.
Custom SQL Statement*	By default this field is empty. It accepts any valid custom SQL query (overriding the default query) to run and collect data from the 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:

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:

1. In the NetWitness Platform menu, select  **(Admin) > Services**. The Services view is displayed.
2. Select a **Log Decoder** service.
3. Under **Actions**, select **View** > **System**.
4. In the toolbar, click **Start Capture**.

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

Log Decoders can handle events up to 32 KB by default. If your events are being cut off, you need to change the event size.

To change Event Size Limit:

1. At `http://<LogDecoder_IP>:50102/decoder/config` (replace <LogDecoder_IP> with the IP address of your Log Decoder), change the Log Decoder REST configuration.
2. Set `pool.packet.page.size` to 64 KB.
3. Restart the Log Decoder to apply the changes.

Note: If you are collecting events larger than 64 KB, you can reduce the size of incoming data by dropping unnecessary logs or fields from specific event sources.

Ensure the Required Parser is Enabled

Ensure that the parser for your event source is available:

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 **oracle_fga**.

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.