RSA NetWitness Platform

Event Source Log Configuration Guide

Oracle Database

Last Modified: Thursday, April 22, 2021

Event Source Product Information:

Vendor: Oracle
Event Source: Oracle
Versions: 8*i*, 9*i*, 10*g*, 11.*xg*, 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)

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

> **Note:** Oracle version 12*c*, 18c, and 19*c* is supported on 10.6.2 and later.

Event Source Log Parser: oracle
Collection Method: Syslog, ODBC, File
Event Source Class.Subclass: Storage.Database

Oracle Overview

Oracle provides several types of auditing. To integrate with the RSA 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 RSA 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 RSA NetWitness Platform for all supported versions of the Oracle database event source. To integrate Oracle file system auditing with the RSA 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 RSA 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 RSA NetWitness Platform for Oracle 10g or 11g. To integrate Oracle database auditing with RSA 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.
- RSA NetWitness Platform automatically deletes all intermediate files associated with this collection method, which can reduce the amount of storage used by RSA 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 RSA 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 RSA 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 RSA 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*

RSA 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*

RSA 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,12*c*,18*c* or 19*c* 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 RSA 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 RSA 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 RSA NetWitness Platform for Oracle ODBC Collection

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 RSA 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 **AUDSYS.UNIFIED_AUDIT_TRAIL** and the **SYS.V_$INSTANCE** view. To grant these privileges, run the following commands:
     ```
     GRANT SELECT ON AUDSYS.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 RSA NetWitness Platform for ODBC Collection from Oracle Database

To configure ODBC collection in RSA 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 RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select 🛠 **(Admin)** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

> **Note:** The required parser is **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.
3. Click ⚙ under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click + to open the **Add DSN** dialog.

   > **Note:** If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in RSA Link.

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template (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.

Field	Description
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

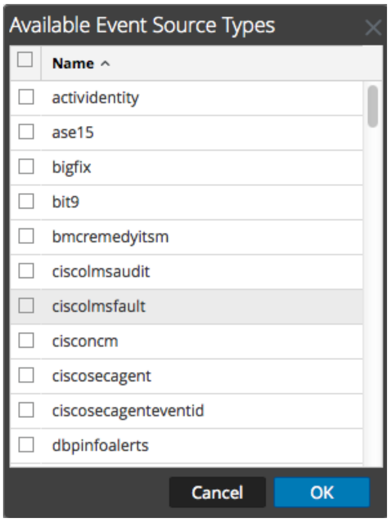
> **Note:** If the necessary event source type is not listed check RSA Live for any related RSA Log Collector content that may apply.

Add the ODBC Event Source Type:

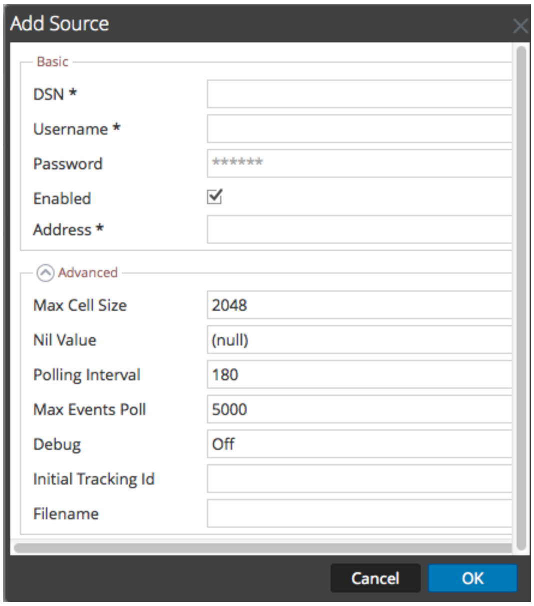
1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.

3. Click ⚙ under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.

   The Event Categories panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.
7. Fill in the parameters and click **Save**.
8. In the **Event Categories** panel, select the event source type that you just added.
9. In the **Sources** panel, click + to open the **Add Source** dialog.



Basic

DSN *	
Username *	
Password	******
Enabled	☑
Address *	

Advanced

Max Cell Size	2048
Nil Value	(null)
Polling Interval	180
Max Events Poll	5000
Debug	Off
Initial Tracking Id	
Filename	

10. Enter the DSN you configured during the **Configure a DSN** procedure.

11. For the other parameters, see ODBC Event Source Configuration Parameters in the SA User Guide.

Restart the ODBC Collection Service

Restart the ODBC collection service:

1. In the **Security Analytics** menu, select **Administration** > **Services**.

2. In the **Services** grid, select a **Log Collector** service.

3. Click ⚙ under **Actions** and select **View** > **System**.

4. 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 RSA 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 RSA NetWitness Platform for Oracle ODBC Collection.

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.db**l 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 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 RSA 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

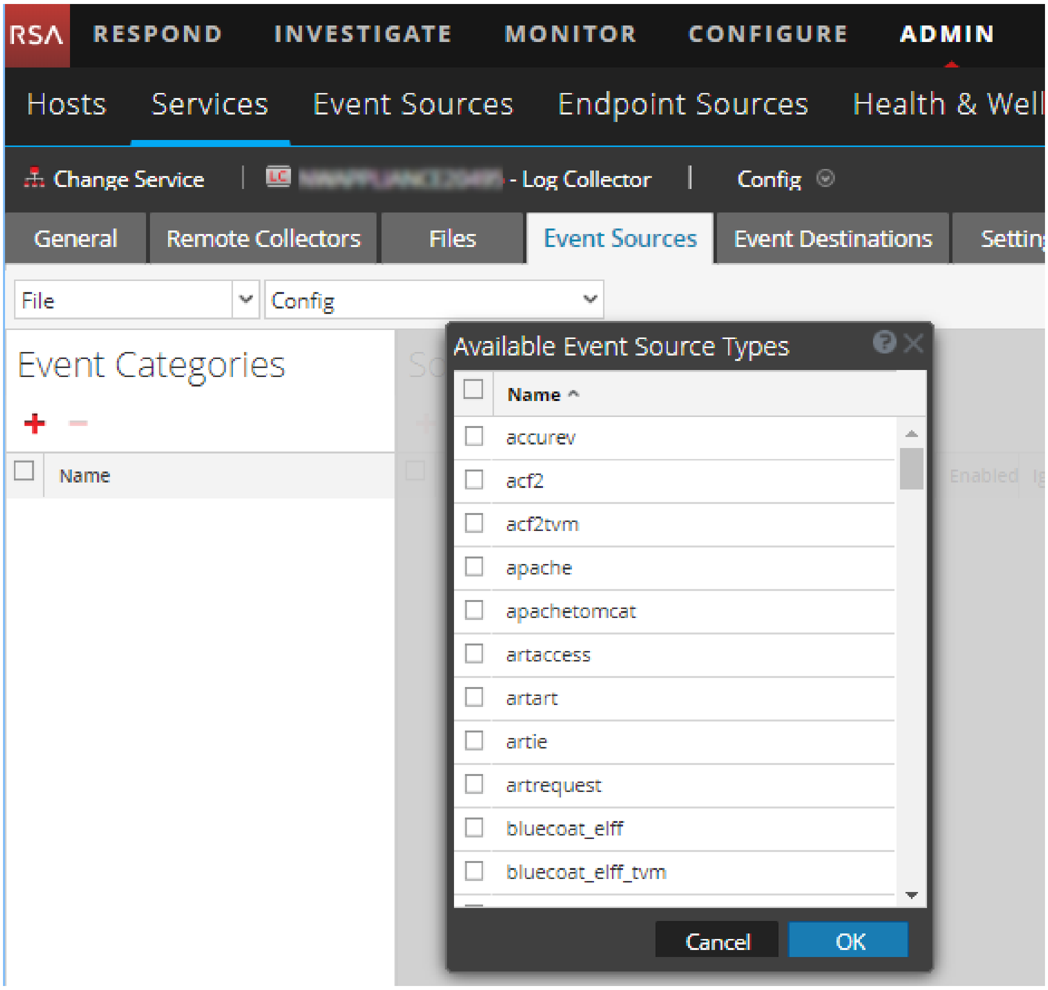
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

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

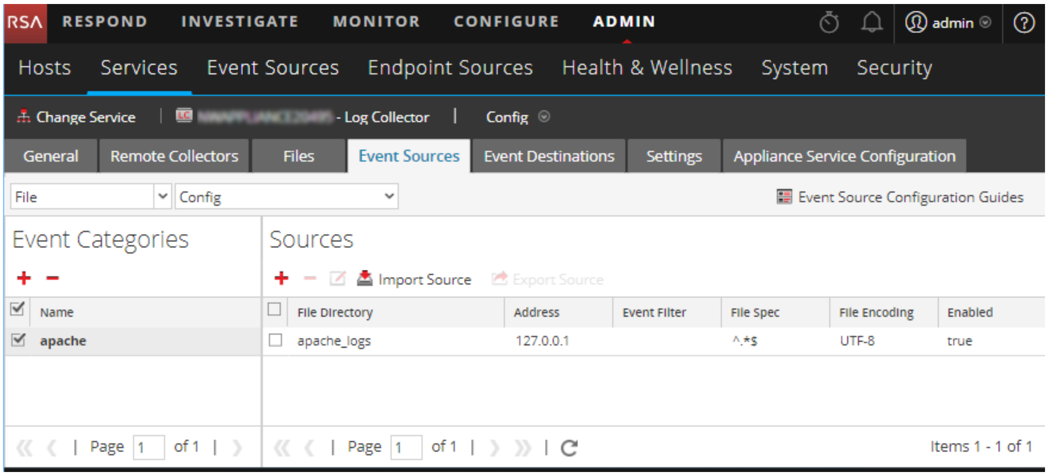
   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.



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

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



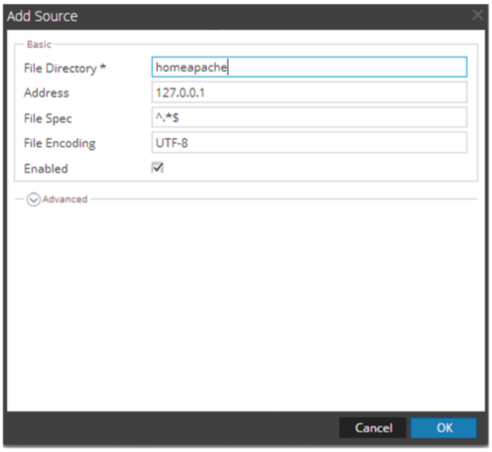
☑	Name
☑	apache

□	File Directory	Address	Event Filter	File Spec	File Encoding	Enabled
□	apache_logs	127.0.0.1		^.*$	UTF-8	true

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.



Add Source

Basic

File Directory * homeapache

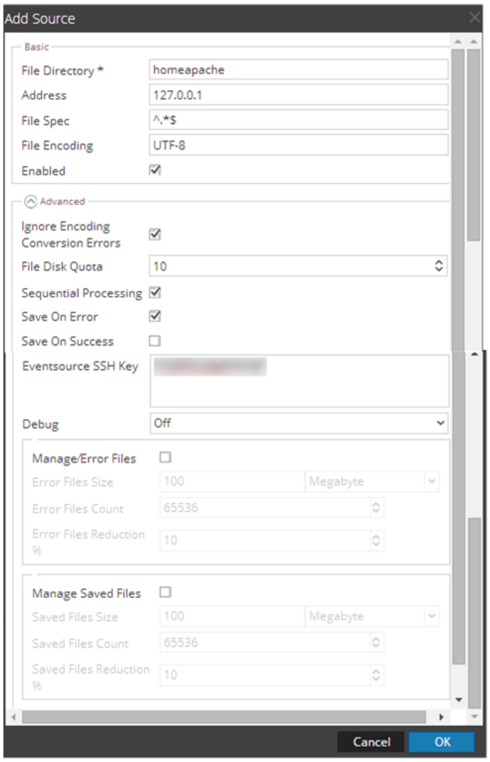
Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced



Add Source

Basic

File Directory * homeapache

Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced

Ignore Encoding Conversion Errors ☑

File Disk Quota 10

Sequential Processing ☑

Save On Error ☑

Save On Success □

Eventsource SSH Key [redacted]

Debug Off

Manage/Error Files □

Error Files Size 100 Megabyte

Error Files Count 65536

Error Files Reduction % 10

Manage Saved Files □

Saved Files Size 100 Megabyte

Saved Files Count 65536

Saved Files Reduction % 10

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

8. Configure the RSA NetWitness Platform Upload Directories. After you have added and configured the event source using the RSA 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 RSA 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 RSA 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 RSA NetWitness Platform Log Decoder or RSA 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 RSA NetWitness Platform for ODBC Collection from Oracle Database. When performing that task, remember to select **oracle_fga** from the **Available Event Source Types** dialog,

November 2020

Trademarks

RSA Conference Logo, 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.