RSA NetWitness Platform

Event Source Log Configuration Guide

RSA

Oracle Audit Vault and Database Firewall

Last Modified: Monday, August 2, 2021

Event Source Product Information:

Vendor: Oracle
Event Source: Oracle Audit Vault
Versions: 10.3, 12.x, 20.3

RSA Product Information:

Supported On: NetWitness Platform 11.0 and later
Event Source Log Parser: oracleav
Collection Method: ODBC
Event Source Class.Subclass: Storage.Database

Configure Oracle Audit Vault for ODBC Collection

To configure Oracle Audit Vault for ODBC collection, perform the following tasks in RSA NetWitness Platform:

   I. Ensure the required parser is enabled

  II. Configure a DSN

 III. Add the Event Source Type

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 from RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **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 **oracleav**.

Configure a DSN

Configure a DSN (Data Source Name):

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/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:** 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. (Use this

name when you set up the ODBC event source type.)

8. Fill in the parameters and click **Save**.

| Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN.
Parameters section	
Database	Specify the database used by Oracle Audit Vault.
PortNumber	Specify the Port Number. The default port number is **1521**.
HostName	Specify the hostname or IP Address of Oracle Audit Vault.
Driver	Depending on your NetWitness Log Collector version: • 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

Add the ODBC Event Source Type

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

- For Oracle Audit Vault version 10.3, select **oracleauditvault**

- For Oracle Audit Vault version 12.x or 20.3, select **oracleauditvault_12x**

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.
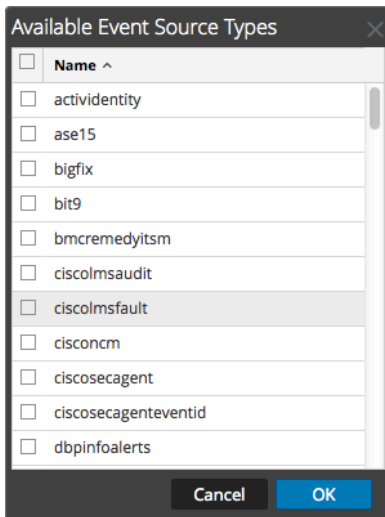
6. Choose the log collector configuration type for your event source type and click **OK**.

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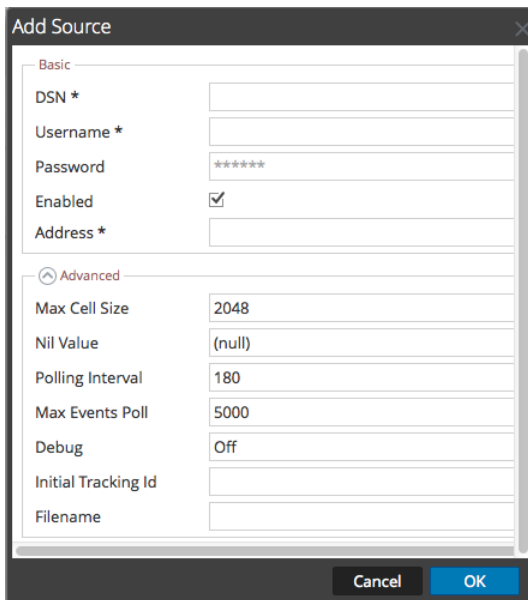
10. Enter the DSN you configured during the **Configure a DSN** procedure.

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

© 2021 RSA Security LLC or its affiliates. All Rights Reserved.

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.

Configure Oracle Audit Vault for ODBC Collection