RSA NetWitness Logs

Event Source Log Configuration Guide

Oracle Database Vault

Last Modified: Thursday, June 29, 2017

Event Source Product Information:

Vendor: Oracle
Event Source: Database Vault
Versions: 10*g*R2

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: oracledv
Collection Method: ODBC
Event Source Class.Subclass: Security.Access Control

Configure the Oracle Database Vault

To configure the Oracle Database Vault:

1. Log on to the Oracle Database Vault web console with your Database Vault owner credentials.
2. On the Administration tab, click **Realms**.
3. In the **Audit Options** section, ensure that **Audit on Failure** is enabled for all database names.
4. On the Administrator tab, click **Rule Sets**.
5. In the **Audit Options** section, ensure that **Audit on Failure** is enabled for all rule set names.
6. On the **Administrator** tab, click **Factors**.
7. Ensure that Audit Options are set to **Always** for all factor names.

Note: For information on configuring rules and policies, see the Oracle Database Vault Administrator guide.

Configure NetWitness Suite for ODBC Collection

To configure ODBC collection in RSA NetWitness Suite, 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 Suite 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 **oracledv**.

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: If you need to add a DSN template, see Configure DSNs in the NetWitness User Guide.

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 Vault
Edition Name	Enter the name of the Oracle edition
Driver	If you choose one of the native templates, you can accept the default value, **/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 Database Vault server.

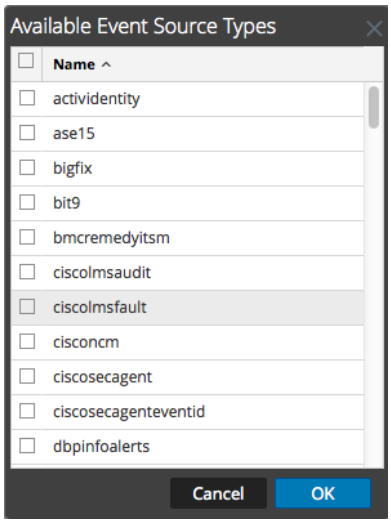
Add the Event Source Type

In step 6 below, select **oracledv** from the **Available Event Source Types** dialog.

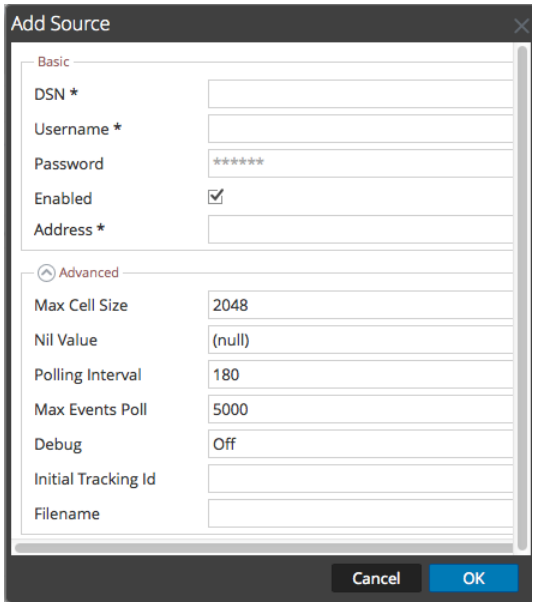
Add the ODBC Event Source Type:

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.

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**.

Trademarks