RSA NetWitness Logs

Event Source Log Configuration Guide

RSA Identity Governance and Lifecycle

Last Modified: Friday, May 12, 2017

Event Source Product Information:

Vendor: RSA, The Security Division of EMC
Event Source: Identity Governance and Lifecycle
Versions: 6.5.1, 6.9

RSA Product Information:

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

To configure RSA Identity Governance and Lifecycle to work with RSA NetWitness Suite, you must complete these tasks:

I. Configure RSA Identity Governance and Lifecycle for ODBC Collection

II. Configure NetWitness Suite for ODBC Collection

Configure RSA Identity Governance and Lifecycle

To configure RSA Identity Governance and Lifecycle:

1. Log on to the RSA Identity Governance and Lifecycle Command Line Interface with **root** credentials.
2. Enable **Port 1555** to establish ODBC connection with RSA NetWitness Suite.

Configure NetWitness Suite for ODBC Collection

To configure RSA NetWitness Suite for ODBC collection, perform the following tasks in RSA NetWitness Suite:

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 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 **rsaaveksa**.

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**.

   ```
   SID=AVDB

   PortNumber=1555

   HostName=<Specify the IP Address of RSA Identity
   Governance and Lifecycle>
   ```

   For the **Driver**, select one of the following values, 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`

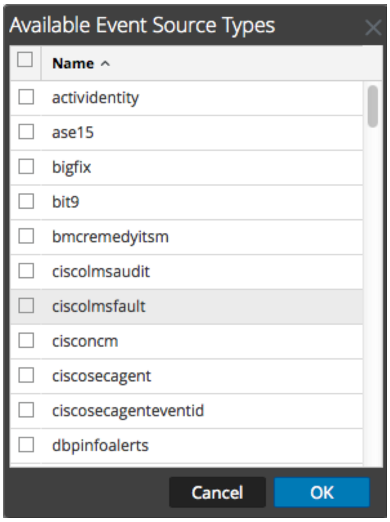
Add the ODBC Event Source Type

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.



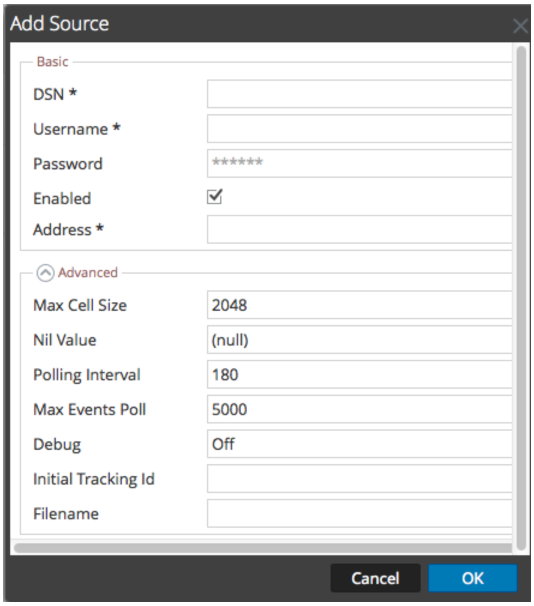
□	Name ^
□	actividentity
□	ase15
□	bigfix
□	bit9
□	bmcremedyitsm
□	ciscolmsaudit
□	ciscolmsfault
□	cisconcm
□	ciscosecagent
□	ciscosecagenteventid
□	dbpinfoalerts

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

   Select one of the following from the **Available Event Source Types** dialog:

   - For version 6.5.1, choose **rsaaveksa**
   - For version 6.9 and later, choose **rsaaveksa69**

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.



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	

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 NetWitness Suite Log Collection Guide.

Trademarks