RSA NetWitness Logs

Event Source Log Configuration Guide

McAfee Policy Auditor

Last Modified: Friday, June 02, 2017

Event Source Product Information:

Vendor: McAfee
Event Source: Policy Auditor
Versions: 5.2, 6.01, 6.2

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: mcafeepa
Collection Method: ODBC
Event Source Class.Subclass: Network.Configuration Management

Configure McAfee Policy Auditor for ODBC Collection

To configure the McAfee Policy Auditor 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

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 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 **mcafeepa**.

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	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the hostname or IP Address of the Oracle database for McAfee Policy Auditor.
PortNumber	Specify the Port Number. The default port number is **1521**
HostName	Specify the hostname or IP Address of the McAfee Policy Auditor event source.
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

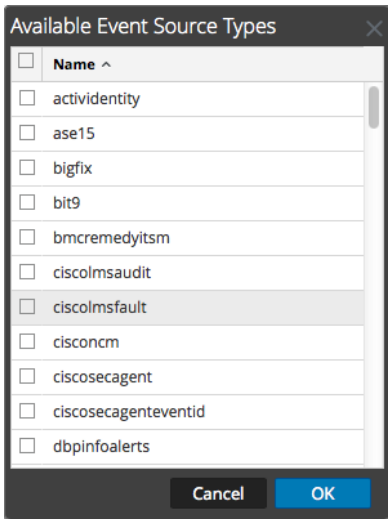
Add the ODBC Event Source Type

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.

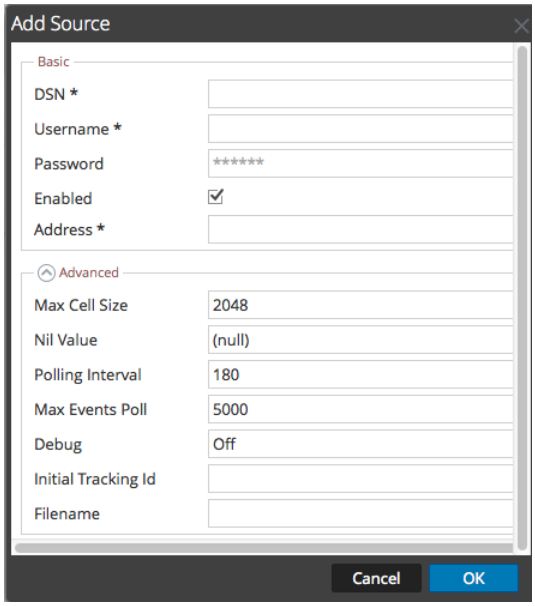


6. Choose the log collector configuration type for your event source type and click **OK**.

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

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 NetWitness Suite Log Collection 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