RSA NetWitness Platform

Event Source Log Configuration Guide

McAfee ePolicy Orchestrator

Last Modified: Tuesday, August 6, 2019

Event Source Product Information:

Vendor: McAfee
Event Source: ePolicy Orchestrator
Versions: 3.5, 3.6.0, 3.6.1, 4.0, 4.5, 4.6, 5.x

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: epolicy
Collection Method: ODBC
Event Source Class.Subclass: Security.Antivirus

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

For table reference, see Reference Tables below.

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 **epolicy**.

Configure a DSN

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**.

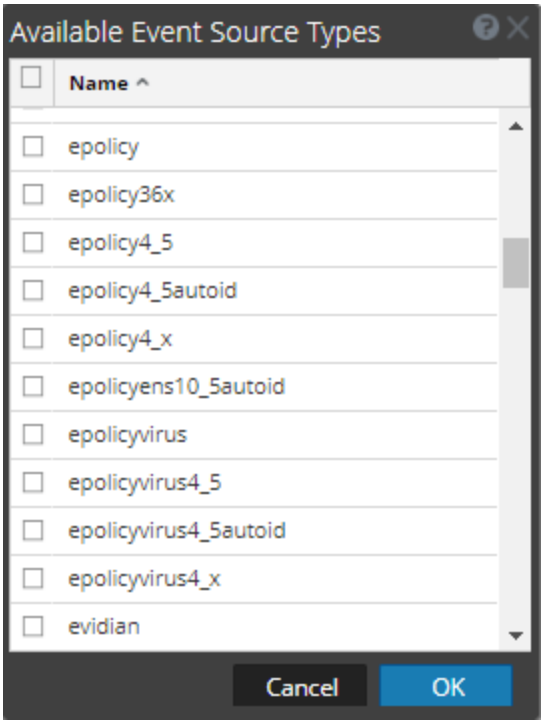
Field	Description
DSN Template	Choose the **MSSQL_Server_Windows_Template** from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the database used by McAfee ePolicy Orchestrator
PortNumber	Specify the Port Number. The default port number is **1433**
HostName	Specify the hostname or IP Address of McAfee ePolicy Orchestrator
Driver	Depending on your NetWitness Log Collector version: • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so

Add the Event Source Type

Add the ODBC Event Source Type:

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/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**.

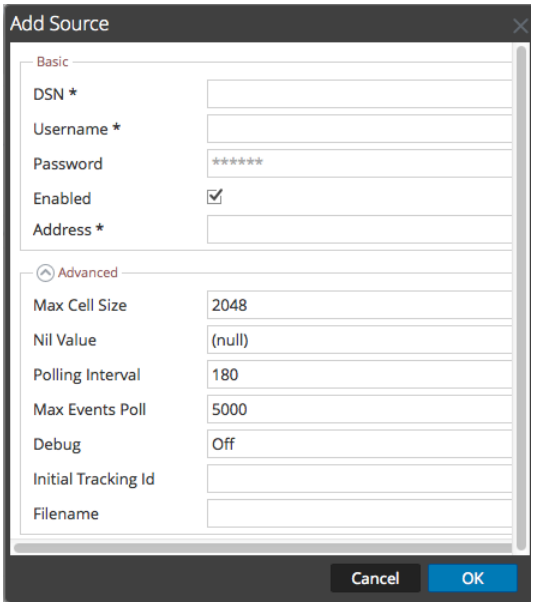
   For collecting ePolicy system logs:

   - For version 3.5, select **ePolicy**.
   - For versions 3.6.0 or 3.6.1, select **ePolicy36x**.
   - For version 4.0, select **ePolicy4_x**.
   - For version 4.5 and newer, select **ePolicy4_5**.
   - (Optional) If you want to use AutoID as the tracking column, select **ePolicy4_5Autoid**

   For collecting ePolicy virus logs:

   - For versions 3.5, 3.6.0, or 3.6.1, select **epolicyvirus**.
   - For version 4.0, select **epolicyvirus4_x**.
   - For version 4.5 and newer, select **epolicyvirus4_5**.
   - For version 5.9.x, select **epolicyvirus5_9_x**.
   - (Optional) If you want to use AutoID as the tracking column, select **ePolicyvirus4_5Autoid**.

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 the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Reference Tables

This event source collects data from the following tables, using the indicated typespec files.

- The **ServerEvents** table uses the **epolicy.xml** typespec file.
- The following tables use the **epolicy36x.xml** typespec file:
  - ServerEvents
  - EPOAuditEvents
  - EPOAuditEventMsgs
- The **OrionAuditLog** table uses the following typespec files:
  - epolicy4_5.xml
  - epolicy4_5autoid.xml
  - epolicy4_x.xml
- The **Events** table uses the **epolicyvirus.xml** typespec file.
- The **EPOEvents** table uses the following typespec files:

- epolicyens10_5autoid.xml
- epolicyvirus4_5.xml
- epolicyvirus4_5autoid.xml
- epolicyvirus4_x.xml

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.