RSA NetWitness Platform

Event Source Log Configuration Guide

EMC Avamar

Last Modified: Tuesday, August 6, 2019

Event Source Product Information:

Vendor: EMC
Event Source: Avamar
Versions: 4.1, 6.0, and 7.0

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: emcavamar
Collection Method: Syslog, ODBC
Event Source Class.Subclass: Storage.Storage

Configure EMC Avamar

Note: RSA supports collection of system events through syslog or the ODBC service and audit events through the ODBC Service.

To configure EMC Avamar, you must complete these tasks:

I. Configure Collection of System Events: configure Syslog or ODBC

Note: System events can be collected through Syslog method or ODBC service. You must choose one or the other.

II. Configure Collection of Audit Events: configure ODBC

Configure Collection of System Events via Syslog

To configure the EMC Avamar event source, you must:

I. Configure Syslog Output on EMC Avamar

II. In RSA NetWitness Platform, ensure the required parser is enabled

III. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on EMC Avamar

To configure EMC Avamar for syslog collection:

1. Log on to the Avamar Administrator.
2. Click **Tools** > **Manage Profiles** > **New**.
3. In the **Profile Name** field, type **enVision**.
4. Ensure that **Syslog Notification** is selected, and click **Next**.
5. Select all event codes that your environment requires.

   Note: The RSA NetWitness Platform Log Decoder or Remote Log Collector supports all event codes.
6. Click **Finish**.
7. Select the **enVision** profile that you created, and click **Edit**.
8. Click the **Syslog Notification** tab, and ensure the fields are completed as follows.

Field	Action
Address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Ensure that the value is 514

9. Ensure that **Include extended event data** is selected.
10. Click **OK**.

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.

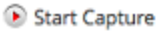
Note: The required parser is **emcavamar**.

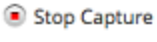
Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see 

, click the icon to start capturing Syslog.
   - If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Configure NetWitness Platform for ODBC Collection

You should configure ODBC collection in the following cases:

- To collect Audit events from EMC Avamar, and
- To collect System events from EMC Avamar ***only if you did not configure EMC Avamar to collect System events using Syslog collection***.

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

> **Note:** The event source type for system events is **emcavamar_syslog**, and the event source type for audit events is **emcavamar_audit**.

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 from 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 **emcavamar**.

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 one of the PostgreSQL drivers (Unix or Windows) from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Enter **mcdb**
PortNumber	Enter **5555**
HostName	Specify the hostname or IP Address for the EMC Avamar event source

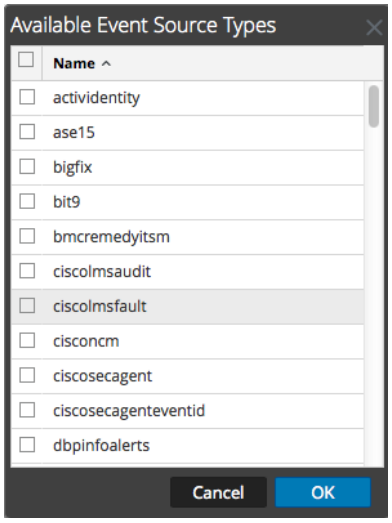
Add the Event Source Type

If you are collecting both system and audit events using ODBC, you need to perform this procedure twice: once to select the EMC Avamar Syslog event source type and once to select the ODBC 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.

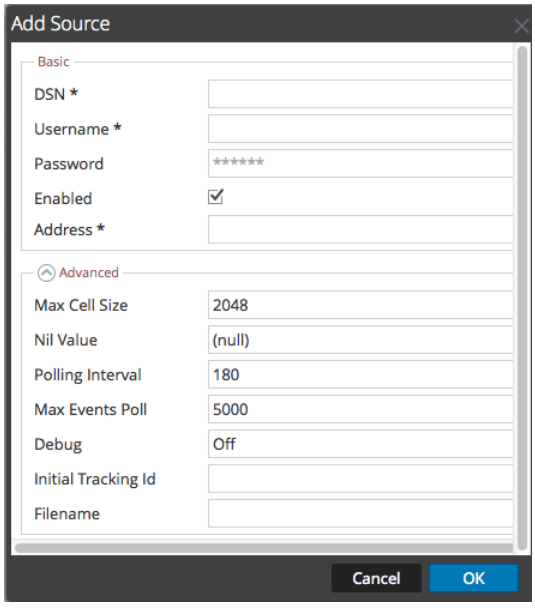
   The Event Categories panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



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

    - If you are configuring ODBC for system events, select **emcavamar_syslog** from the **Available Event Source Types** dialog.
    - If you are configuring ODBC for audit events, select **emcavamar_audit** 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 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 **v_audits** table uses the **emcavamar_audit.xml** typespec file.
- The **v_events** table uses the **emcavamar_syslog.xml** typespec file.

Trademarks

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