RSA NetWitness Platform

Event Source Log Configuration Guide

RSA Malware Analysis

Last Modified: Monday, July 9, 2018

Event Source Product Information:

Vendor: RSA
Event Source: Malware Analysis (previously NetWitness Spectrum)
Version: 1.0.5.0

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: netwitnessspectrum, cef
Collection Method: Syslog
Event Source Class.Subclass: Security.Antivirus

To configure the RSA Malware Analysis event source, you must:

I. Configure Syslog Output on RSA Malware Analysis

II. Configure NetWitness Platform for Syslog Collection

Configure Syslog Output on RSA Malware Analysis

To configure RSA Malware Analysis:

1. Log on to the RSA NetWitness Spectrum management console with administrative credentials.
2. From the navigation pane on the top left, click System.
3. Click **Auditing > Syslog**.
4. In the **Syslog Auditing** section, complete the fields as follows:

Field	Action
Server Name	Enter the IP address of the RSA NetWitness Platform Log Decoder or Remote Log Collector.
Server Port	Type **514**.
Facility	From the drop-down list, select **SYSLOG**.
Encoding	Type **UTF-8**.
Format	From the drop-down list, select **CEF**.
Max Length	Enter the desired maximum length of the syslog messages.

5. Ensure that **Include the local timestamp in syslog messages** and **Include the local hostname in syslog messages are selected**.
6. Click **Save Changes**.
7. To enable your settings, on the top right corner of the **Syslog Auditing** section, click **Enable**.

Configure NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

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 **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 **netwitnessspectrum** or **cef**.

Configure Syslog Collection

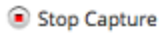
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 **Administration** > **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 **Administration** > **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.

Trademarks

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