RSA NetWitness Platform

Event Source Log Configuration Guide

Sophos UTM

Last Modified: Wednesday, October 10, 2018

Event Source Product Information:

Vendor: Sophos
Event Source: UTM
Version: 9.x, 17.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: astarosg
Collection Method: Syslog
Event Source Class.Subclass: Security.Firewall

To configure the Sophos UTM event source, you must:

I. Configure Syslog Output on YOUR EVENT SOURCE

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Sophos UTM

Configure Sophos UTM to output Syslog messages to the correct location.

1. Log on to the Sophos UTM web interface, using administrator credentials.
2. Click **Logging & Reporting > Log Settings**.
3. Click the **Remote Syslog Server** tab.
4. To enable the remote syslog server, select **Enable**.
5. To add RSA NetWitness Platform as the syslog server, follow these steps:
   a. From the **Remote Syslog Server** settings, click the add icon next to the **Host** drop-down menu.
   b. From the **Add Syslog Server** window, complete the fields as follows:

Field	Value
Name	Enter a name to represent your NetWitness platform.
Server	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Enter **514**.

   c. Click **Save**.

6. To select logs to send to the remote syslog server, follow these steps:
   a. From the **Remote syslog log selection** area, select the logs that you want to sent to RSA NetWitness.

> **Note:** RSA supports the following logs for collection: DNS Proxy, Firewall, Web Application Firewall, and Web Filtering.

   b. Click **Apply**.

Configure RSA 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 **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 **astarosg**.

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 ▶ Start Capture , click the icon to start capturing Syslog.
- If you see ■ Stop Capture , 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.