RSA NetWitness Platform

Event Source Log Configuration Guide

Palo Alto Panorama Management Server

Last Modified: Friday, August 24, 2018

Event Source Product Information:

Vendor: Palo Alto
Event Source: Panorama Management Server
Versions: 4.1.0, 5.1.4, 7.1, 8.x

RSA Product Information:

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

To configure the Palo Alto Panorama Management Server event source, you must:

I. Configure Syslog Output on Palo Alto Panorama Management Server

II. Forward Logs to Panorama

III. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Palo Alto Panorama Management Server

To configure Palo Alto Panorama Management Server:

> **Note:** This configuration allows you to transfer only system and configuration logs of Palo Alto Panorama Management Server to RSA NetWitness Platform.

1. Log on to the Palo Alto Panorama Management Server with administrative credentials.
2. To add RSA NetWitness Platform to Palo Alto Panorama Management Server, follow these steps:
   a. Click the **Panorama** tab.
   b. From the navigation menu, click **Server Profiles** > **Syslog**.
   c. Click **Add**.
   d. In the **Name** field, enter a name for the syslog server.
   e. Click **Add**.
   f. In the **Name** field, enter a name for your RSA NetWitness Platform.
   g. In the **Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   h. Ensure that the port is set to **514** and that the facility value is set to **LOG_USER**.
   i. Click **OK**.
   j. In the top right menu bar, click **Save**.
3. To configure Palo Alto Panorama Management Server to send system logs to the RSA NetWitness Platform, follow these steps:
   a. Click the **Panorama** tab.
   b. From the navigation menu, click **Log Settings** > **System**.
   c. From the **Syslog** drop-down list of each category of messages that you want to forward to the RSA NetWitness Platform, select the name of the RSA NetWitness Platform that you specified in step 2.

d. Click **OK**.

e. Click **Apply**.

f. Click **Save**.

4. To configure Palo Alto Panorama Management Server to send configuration logs to RSA NetWitness Platform, follow these steps:

   a. Click the **Panorama** tab.

   b. From the navigation menu, click **Log Settings** > **Config**.

   c. Click the configuration icon in the upper right corner, then select the name of the RSA NetWitness Platform that you specified in step 2.

   d. Click **OK**.

5. From the top menu, click **Save**.

6. From the top menu, click **Commit** to confirm all the changes.

Forward Logs to Panorama

Before you send logs from Palo Alto Panorama Management Server to RSA NetWitness Platform, you must first forward logs from your firewall event sources to Panorama. To forward logs to Palo Alto Panorama Management Server, see the Palo Alto documentation.

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 **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 **paloaltonetworks**.

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.