RSA NetWitness Logs

Event Source Log Configuration Guide

RSA

Apcon IntellaPatch

Last Modified: Thursday, May 04, 2017

Event Source Product Information:

Vendor: Apcon
Event Source: IntellaPatch Series 3000 Network Monitoring Switch
Versions: 4.34.2

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: apconintellapatch
Collection Method: Syslog
Event Source Class.Subclass: Network.Switch

To configure the Apcon IntellaPatch event source, you must:

 I. Configure Syslog Output on Apcon IntellaPatch

 II. Configure Security Analytics for Syslog Collection

Configure Apcon IntellaPatch

To configure Syslog Output on Apcon IntellaPatch:

1. From the IntellaPatch Web UI dashboard, select **Command Center** > **Global settings** > **Services**.

2. Select the **Service Properties** tab.

3. Check the **Enable Remote Syslog** button and fill in the following fields:

Field	Action
Send Events to this IP	Enter the IP address of your RSA NetWitness Suite Log Decoder or RSA Security Analytics Remote Log Collector.
Facility/Severity	Choose the appropriate facility and severity level.

4. Click **Save** to save your changes.

Configure RSA NetWitness Suite

Perform the following steps in Security Analytics:

- 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 Suite 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 **apconintellapatch**.

Configure RSA NetWitness Suite for 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