RSA NetWitness Logs

Event Source Log Configuration Guide

Arbor Networks Peakflow SP5

Last Modified: Thursday, May 04, 2017

Event Source Product Information:

Vendor: Arbor Networks
Event Source: Peakflow SP5
Versions: 5.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: arborpeakflowsp
Collection Method: Syslog
Event Source Class.Subclass: Security.IPS

Configure Arbor Networks Peakflow SP5

To configure Syslog collection for the Arbor Networks Peakflow SP5 you must:

I. Configure RSA NetWitness Suite for Syslog Collection

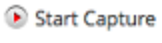
II. Configure Syslog Output on Arbor Networks Peakflow SP5

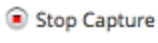
Configure RSA NetWitness Suite for Syslog Collection

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 

, 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.

Configure Syslog Output on Arbor Networks Peakflow SP5

To configure Arbor Networks Peakflow SP5:

1. Log on to the Peakflow SP 5.0 web interface as Administrator.
2. Navigate to the Notification Groups page: **Administration > Notification > Groups**
3. Do either of the following:
   - To add a new group, click **Add Notification Group**.
   - To modify an existing group, click a name link.
4. Type the group name in the **Name** box.
5. Type the description in the **Description** box.
6. Based on the format you want to send the DoS alerts, do one of the following:
   - To send DoS alerts in text format, type the email addresses in the **Text Email Addresses** box.
   - To send DoS alerts in XML format, type the email addresses in the **DoS XML Email Addresses** box.
7. Navigate to the **Remote Syslog** section, and fill in the fields as follows:
   - Type the IP address of your RSA NetWitness Suite Log Decoder or RSA Security Analytics Remote Log Collector in the **Destinations** box.

- Type the port number your NetWitness Suite platform listens to for Syslog messages in the **Destination Port** box.
- Select the facility from the **Facility** list.
- Select the syslog severity from the **Severity** list.

8. Click **Save**.
9. Click **CONFIG COMMIT** on the right side of the menu bar.
10. In the new pop-up window, you can now add an optional log message and click **Commit** to apply your changes.

Trademarks