RSA NetWitness Logs

Event Source Log Configuration Guide

Check Point SPLAT OS

Last Modified: Tuesday, May 09, 2017

Event Source Product Information:

Vendor: Check Point
Event Source: SPLAT OS

> **Note:** This event source is supported by the Red Hat Linux XML, and is discovered by the RSA NetWitness Suite Log Decoder as Linux.

Versions: R75, 77.10

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: rhlinux
Collection Method: Syslog
Event Source Class.Subclass: Host.Unix

Configure Check Point SPLAT OS

To configure Syslog collection for the Check Point SPLAT OS you must:

I. Configure RSA NetWitness Suite for Syslog Collection

II. Configure Syslog Output on Check Point SPLAT OS

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.

Configure Syslog Output on Check Point SPLAT OS

To configure Syslog output on Check Point SPLAT OS:

1. Open the command prompt and enter the following:

   ```
   syslog_servers add IP address of your server
   ```

   where *IP address of your server* is the IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.

2. Ensure that the syslog servers have been added by typing the following line:

   ```
   syslog_servers show
   ```

Trademarks