RSA NetWitness Logs

Event Source Log Configuration Guide

Pulse Connect Secure

Last Modified: Friday, November 3, 2017

Event Source Product Information:

Vendor: Pulse Secure
Event Source: Pulse Connect Secure (formerly Juniper Networks SSL VPN)
Versions: 5.4, 5.5, 6.0, 6.2 R2, 6.5 R2, 7.0 R2, 7.1 R5, 7.2 R1, 8.0, 8.0 R7.1, 8.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 Suite 10.0 and later
Event Source Log Parser: junipervpn
Collection Method: Syslog
Event Source Class.Subclass: Security.VPN

To configure Pulse Connect Secure to work with RSA NetWitness Suite, perform the following procedures:

- Configure Pulse Connect Secure
- Configure NetWitness Suite for Syslog Collection

Configure Pulse Connect Secure

To configure Pulse Connect Secure:

1. Access the Administrative interface at **https://*devicename* or IP/admin**.
2. Configure logging on the Pulse Connect Secure Appliance.

   This is configured on the **System > Log/Monitoring > Events**, **User Access**, and **Admin Access** tabs.

   Filter and format the events log (which contains system events), the user access log (which contains end-user requests and modifications), and the administrator access log (which contains administrator modifications).

   a. In the Web console, choose **System > Log/Monitoring**.

   b. Select the **Events**, **User Access**, or **Admin Access** tab, and then choose **Settings**.

   c. Under **Select Events to Log**, select each type of event that you want to capture in the local log file.

   > **Note:** If you disable **Statistics** in the **Events** table, the IVE does not write statistics to the log file, but continues to display them in the **System > Log/Monitoring > Statistics** tab.

   d. (Optional) Under **Syslog Servers**, enter information about the syslog servers where you want to store your log files.

      i. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

      ii. (Central Manager only) Choose one of the following filters to apply to the log file:

      - Standard (default)
      - WELF

      > **Note:** If you choose the WELF filter, do not edit the default tag, **id=firewall**.

      iii. Click **Add**.

iv. Repeat for multiple servers if desired, using different formats and filters for different servers and facilities.

e. Click **Save Changes**.

Configure NetWitness Suite for Syslog Collection

Perform the following steps in RSA NetWitness Suite:

- 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 **junipervpn**.

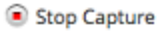
Configure Syslog Collection

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 

, 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.

Trademarks