RSA NetWitness Logs

Event Source Log Configuration Guide

RSA Web Threat Detection

Last Modified: Friday, April 14, 2017

Event Source Product Information:

Vendor: RSA
Event Source: Web Threat Detection (formerly Silver Tail System Forensics and Mitigator)
Versions: Forensics 1.x, 2.x, 3.x; Mitigator 1.x, 2.x 3.x; and Web Threat Detection 4.6, 5.0, 5.0.2

RSA Product Information:

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

To configure Syslog collection for the RSA Web Threat Detection you must:

I. Configure NetWitness Suite for Syslog Collection

II. Configure Syslog Output on RSA Web Threat Detection:

- For RSA Web Threat Detection
- For Silvertail Forensics

Configure 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 RSA Web Threat Detection

Based on your version, perform one of the following tasks:

- Configure RSA Web Threat Detection
- Configure Silvertail Forensics

Configure RSA Web Threat Detection

To configure the RSA Web Threat Detection to send syslog messages to RSA NetWitness Suite:

1. Open RSA SilverCat.
2. Select the **Action Server** item, once on the page click **Edit** and enter the following information under **syslog**:
   a. Enter the name as '**rsa**'.

   > **Note:** The name entered must correspond to the Action field in the Forensics and Mitigator rule in the RSA Web Threat Detection Administration tool.

   b. Facility: *local0*

   c. Priority: *INFO*

   > **Note:** This again is your preference, but the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector recommends *INFO* as the priority.

   d. Format: RSA|Web Threat Detection|%(priority)s|ForensicsMitigator|RuleAction=%(rule.action)s RuleName=%(rule.name)s RuleDate=%(rule.date)s user=%(username)s request=%(pagename)s %(attribute.name)s=%(attribute.value)s
3. Save the settings.
4. Click **Home**.
5. Click **Review Changes and Push**.
6. Ensure the changes are to your standards, then click **Push**.

7. Log in into the RSA Web Threat Detection via SSH using *root* credentials.
8. Edit the **rsyslog.conf** and enter the following command:

   `local0.*` [type 6 tab spaces to enter IP in line with text then type:] `@<applianceIP>`

   where `<applianceIP>` is the address of the RSA NetWitness Suite Log Decoder or Remote Log Collector.
9. Save the changes and restart the rsyslog services.

Configure Silvertail Forensics

To configure the Silver Tail Action Server to send CEF formatted syslog messages to RSA NetWitness Suite:

1. Open Silver Cat.
2. Enter the following information in the **Action Server** > **Syslog** setting:
   a. Facility: *local0*

      > **Note:** This can be changed to reflect your preference. The RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector supports *local0* through *local7* as options.

   b. Priority: Notice

      > **Note:** This again is your preference, but the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector recommends *Notice* as the priority.

   c. Format: CEF:0|Silver Tail Systems|Forensics|*version number*|100|Rule %(rule.name)s fired|10|src=%(ip)s duser=%(username)s request=%(pagename)s

      > **Note:** *version number* should be changed to reflect the current device version number which can be 1.x, 2.x, or 3.x.

3. Save the settings.

Trademarks