RSA NetWitness Logs

Event Source Log Configuration Guide

CentOS

Last Modified: Monday, January 16, 2017

Event Source Product Information:

Vendor: CentOS
Event Source: CentOS
Version: 6.0

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

To configure the CentOS event source, you must:

I. Configure Syslog Output on CentOS

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on CentOS

To configure CentOS:

1. On the Linux appliance, open the **/etc/rsyslog.conf** file in a text editor with **root** privileges.
2. To configure the event source to log all messages of debug level and higher to the syslog server, add the following line:

   `*.* @xxx.xxx.xxx.xxx:514`

   where xxx.xxx.xxx.xxx is the address for the IP address of the RSA NetWitness Log Decoder or Remote Log Collector, and **514** is the default port number.
3. Save the file, and close the text editor.
4. To restart the syslog service, depending on your version of Linux, run the following command:

   ```
   service rsyslog restart
   ```

Configure NetWitness Suite

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 **rhlinux**.

Configure Syslog Collection

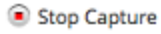
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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