RSA NetWitness Logs

Event Source Log Configuration Guide

Snare for Linux

Last Modified: Friday, April 14, 2017

Event Source Product Information:

Vendor: Intersect Alliance
Event Source: Snare
Versions: Snare Agent for Linux 1.5.1
Platforms:

- Redhat Enterprise Linux 4.0 U3
- Redhat Enterprise 5
- Fedora Core 5
- Fedora Core 6

RSA Product Information:

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

To configure the Snare Agent for Linux event source, you must:

I. Configure Syslog Output on Snare Agent for Linux

II. Configure NetWitness Suite for Syslog Collection

Configure Syslog Output on Snare Agent for Linux

The Intersect Alliance Snare Agent for Linux provides an audit subsystem for the Linux operating system. It can be used as a standalone auditing tool for Linux, or can send data to the Snare Server for analysis and storage.

The Snare Agent work with the following Linux versions:

- Redhat Enterprise Linux 4.0 U3
- Redhat Enterprise 5
- Fedora Core 5
- Fedora Core 6

The RSA NetWitness Suite supports the following configurations:

- Default Configuration
- Sarbanes/Oxley Configuration
- Payment Card Industry Configuration
- NISPOM Configuration

When you install Snare on the Linux host, you must choose one of these configurations.

To configure the Snare Agent for Linux:

1. Log on to the web user interface for Snare.
2. From the left navigation menu, select **File Watch Configuration** to set the files or folders for which to collect log data.

   Use the **Watch file or folder** control to include files or folders, and the **Ignore** control to exclude any files that would otherwise be included.
3. From the left navigation menu, select **Objectives Configuration** to configure the collection of events.

   > **Note:** RSA supports the following events: open,link,symlink, rename, execve, mount, umount, swapon, swapoff, login_auth, login_start, logout, socketcall. If you configure other events, there is a high chance that you will receive unknown messages in the NetWitness Suite.

4. From the left navigation menu, select **General Configuration**.
5. Enter the following values for **Destination Server Address and Port**:
   - **Server**: Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   - **Port**: Syslog – Port 514
6. Select appropriate values for **Syslog destination (if enabled)**.

   Use any of the local syslog facilities (Local0 - Local7), and set the appropriate log level to capture (Emergency, Alert, Critical, Error, Warning, Notice, Information, or Debug).

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 **linux_snare**.

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 ▶ 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.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.