

RSA NetWitness Logs

Event Source Log Configuration Guide



Tripwire Enterprise

Last Modified: Friday, November 3, 2017

Event Source Product Information:

Vendor: [Tripwire](#)

Event Source: Tripwire Enterprise

Versions: 5.4, 5.5, 7.x, 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.

Supported Platforms: Microsoft Windows and Linux

Additional Downloads: [sftpageant.conf.tripwire](#)

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: tripwire

Collection Method: File, Syslog

Note: Syslog collection only supported on version 8.x.

Event Source Class.Subclass: Network.Configuration Management

RSA NetWitness Suite supports Tripwire Enterprise running on Microsoft Windows or Linux platforms. Additionally, RSA enVision supports collection via File Collection and Syslog (versions 8.0 and later).

- To collect audit messages, RSA recommends that you set up Syslog collection.
- Configure File Collection to collect configuration-change related messages.

There are several tasks to set up Tripwire Enterprise:

- I. [Configure Tripwire](#)
- II. [Set Up File Collection](#)
- III. [Configure Syslog Collection \(version 8.x only\)](#)

Configure Tripwire

To log detailed data from Tripwire you must configure an execute action and enable the action on each rule. This action creates a copy of the XML output from a scan to be picked up and processed by the File Service in RSA NetWitness Suite.

To configure Tripwire Enterprise to work with RSA NetWitness Suite:

1. In Tripwire Enterprise, configure a new Tripwire action as follows:
 - a. Use the web interface to select **Actions > New Action > Execute Action**.
 - b. Complete the fields as follows:

Field	Value
Name	NetWitness
Description	Use to archive for RSA NetWitness
Command line (on Windows platforms)	<pre>%SystemRoot%\system32\cmd.exe /c copy "%f" "%f.nic"</pre> <p>Replace SystemRoot with the system root for your Tripwire server. For example:</p> <pre>C:\WINDOWS\system32\cmd.exe /c copy "%f" "%f.nic"</pre> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"><p>Note: If the above command does not work, enter the last part of the command only:</p><pre>copy "%f" "%f.nic"</pre></div>

Field	Value
Command line (on Linux platforms)	<code>cp "%f" "%f.nic"</code>

- c. Click **Finish**.
2. In Tripwire Enterprise, click on the Rules tab to access the Rules groups. Modify each rule to enable the RSA NetWitness Suite action you created in step **1**.
3. [Set up File Collection](#)

Set up File Collection

Perform the following steps to configure File Collection:

- Configure the Log Collector for File Collection
- Set up the SFTP Agent

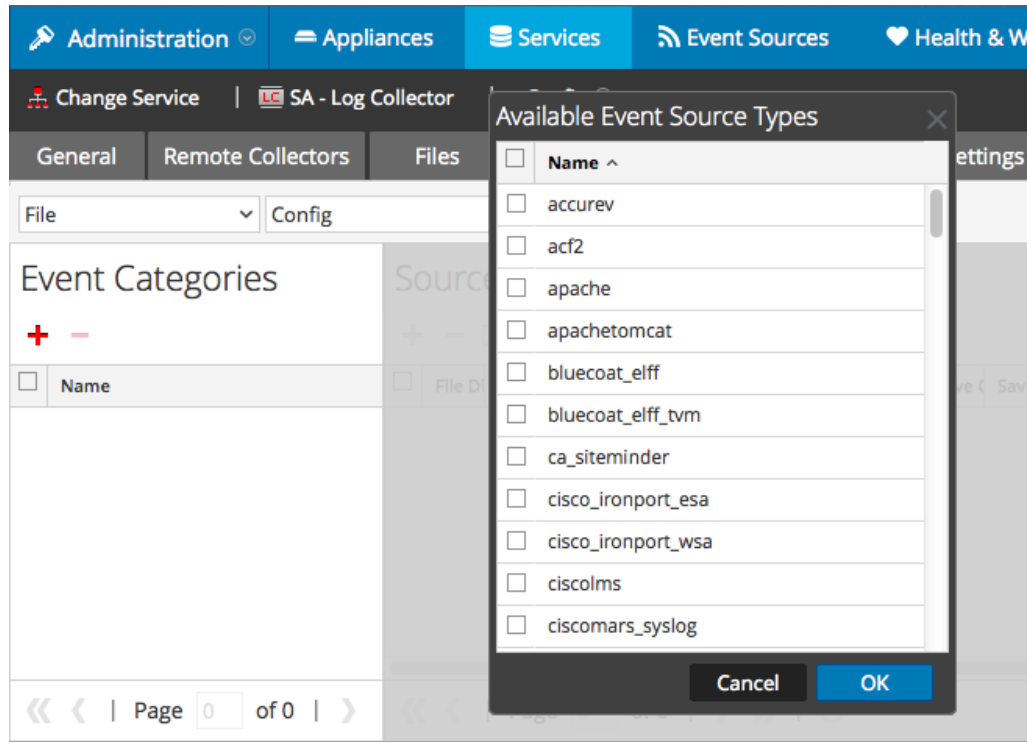
Configure the Log Collector for File Collection

Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **File/Config** from the drop-down menu.
The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

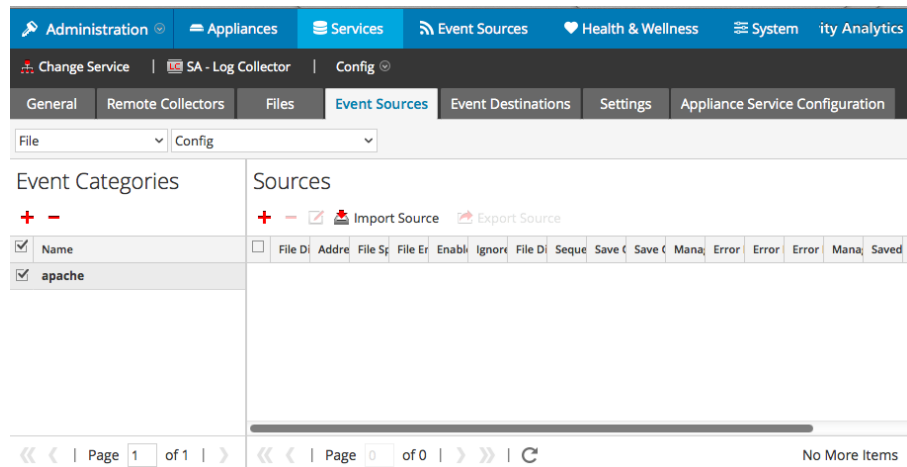


5. Select the correct type from the list, and click **OK**.

Select **tripwire** from the **Available Event Source Types** dialog.

The newly added event source type is displayed in the Event Categories panel.

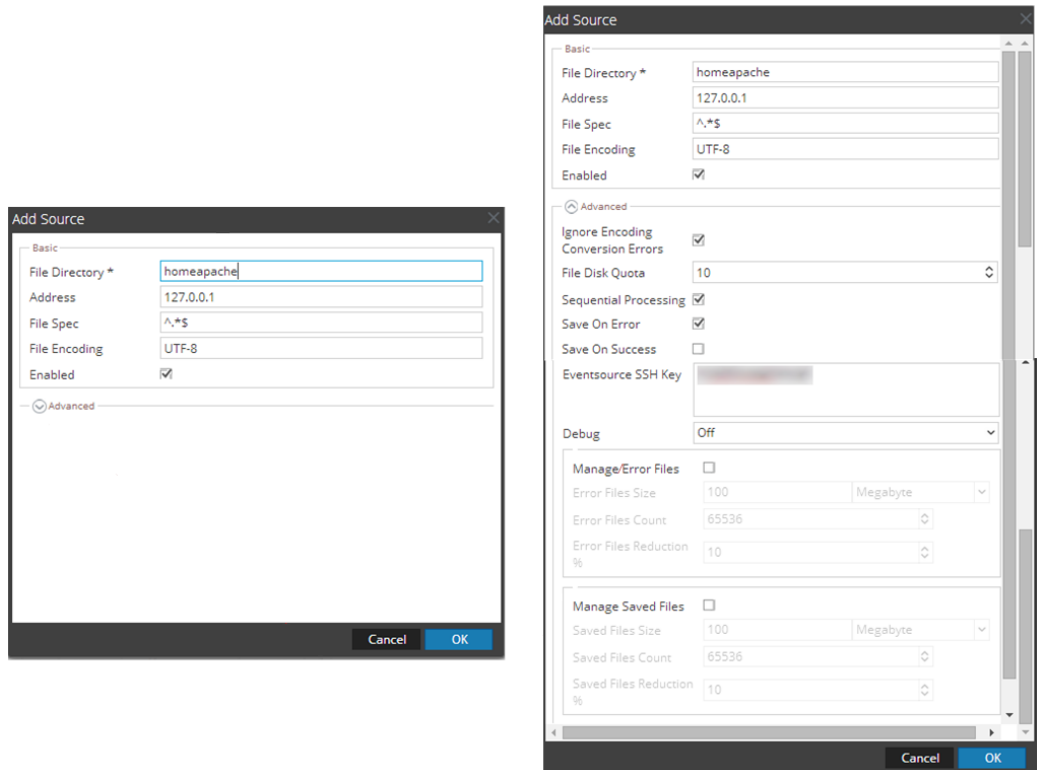
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see [Install and Update SFTP Agent](#)
- To set up the SFTP agent on Linux, see [Configure SFTP Shell Script File Transfer](#)

To set up the SFTP Agent for RSA NetWitness Suite, follow these instructions:

Configure Syslog Collection (version 8.x only)

To set up Syslog collection:

- I. Configure the Tripwire Enterprise Syslog Collection Service
- II. Ensure the Required Parser is Enabled in RSA NetWitness Suite
- III. Configure RSA NetWitness Suite for Syslog Collection

Configure the Tripwire Enterprise Syslog Collection Service

For Tripwire version 8.x, you can collect audit messages through Syslog. To collect configuration-change related messages please configure File Collection.

To configure the Syslog Collection Service:

1. In Tripwire Enterprise, click **Settings** from the top navigation bar.
2. From the left-hand menu, expand **System > Log Management**.
3. Check the **Forward TE log messages** to syslog box.
4. For **TCP Host**, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
5. For **TCP Port**, enter **514**.
6. Click **Apply**.

Ensure the Required Parser is Enabled in RSA NetWitness Suite

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 **tripwire**.



Configure RSA NetWitness Suite for Syslog Collection

If you are configuring the Remote Log Collector for syslog, select **syslog-tcp** in step 5 below. The Tripwire event source sends Syslog over TCP only.

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.

Copyright © 2017 EMC Corporation. All Rights Reserved.

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.