RSA NetWitness Platform

Event Source Log Configuration Guide

Microsoft Windows via RSA NetWitness Endpoint

Last Modified: Friday, January 7, 2022

Event Source Product Information:

Vendor: Microsoft
Event Source: Microsoft Windows
Versions:

- Windows 7, 8, 8.1, 10
- Windows Servers 2008, 2012, 2016, 2019

RSA Product Information:

Supported On: NetWitness Suite 11.1 and later
Event Source Log Parser: windows
Collection Method: Syslog (via NetWitness Endpoint Agent)
Event Source Class.Subclass: Windows.Hosts

This document contains the following sections:

I. Configure the NetWitness Endpoint Agent

II. Configure RSA NetWitness Platform for Syslog Collection

III. List of Tags and Meta for the Netwitness Endpoint Agent

Configure the NetWitness Endpoint Agent

The RSA NetWitness Endpoint product is an endpoint threat detection solution that exposes malware and other threats, highlights suspicious activity for investigation, and instantly determines the scope of a compromise to help security teams stop advanced threats faster.

An Endpoint Agent can be deployed on hosts with Windows, Mac, or Linux operating system. Hosts can be laptops, workstations, servers, tablets, routers, or any system, physical or virtual, where a supported operating system is installed.

To collect log messages from Microsoft Windows using the NetWitness Endpoint Agent, you must generate and deploy agent onto your Windows machine.

1. Generate an Agent Packager. For more details, see **Generate an Agent Packager** topic in the *NetWitness Endpoint Agent Installation Guide*.
2. Deploy the agent. For more details, see **Deploying and Verify Agents** topic in the *NetWitness Endpoint Agent Installation Guide*.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- 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 Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Admin** > **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 **windows**.

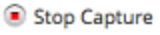
Configure Syslog Collection

Note: Syslog collection must be configured only for the first time when you set up an event source which uses Syslog to send its output to NetWitness.

For Syslog, configure either the Log Decoder or the Remote Log Collector. You do not need to configure both.

Log Decoder Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the **Services** grid, choose 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.

Remote Log Collector Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, go to **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 will appear.
5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Choose the **New Type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog will appear.
7. Enter **514** for the port, and choose **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

After 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.

List of Tags and Meta for the Netwitness Endpoint Agent

RSA maintains a mapping spreadsheet that details how information is parsed from Windows into RSA NetWitness. This blog post is available on RSA Link here: Microsoft Windows Logs via RSA NetWitness Endpoint Agent.

November 2020

Trademarks