RSA NetWitness Platform

Event Source Log Configuration Guide

Symantec ATP (Advanced Threat Protection)

Last Modified: Thursday, August 29, 2019

Event Source Product Information:

Vendor: Symantec
Event Source: Advanced Threat Protection
Versions: 3.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.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: cef
Collection Method: Syslog
Event Source Class.Subclass: Security.Antivirus

To configure the Symantec ATP event source, you must:

I. Configure Syslog Output on Symantec ATP

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Symantec ATP

The following description is from the Symantec website:

> *Symantec Advanced Threat Protection (ATP) sends syslog communications over UDP. If you set up an all-in-one device, you only need to configure default syslog server connections. If you installed a management platform with one or more network scanners, you can apply the default syslog server connection settings to each appliance, or you can configure custom settings for individual appliances.*

To configure syslog for Symantec ATP perform the following steps:

> **Note:** This procedure is reproduced from the Configuring connections to syslog servers topic on the Symantec website.

1. Do either of the following:

To configure the syslog server connection for the default appliance	Do the following: A. In ATP Manager, click **Settings > Appliances**. B. Click **Edit Default Appliance**.
To configure a custom syslog server connection for a single device	Do the following: A. In ATP Manager, click **Settings > Appliances**, and double-click on the device in the **Appliances** list. B. In the **Syslog** section, uncheck **Use default**, if it is checked.

2. Click **+Add Syslog Server**.
3. In the **Add Syslog Server** dialog box, in the **Host** field, type the IP address of the syslog server.
4. In the **Protocol** field, select the appropriate protocol.
5. In the **Port** field, type the port on the syslog server that accepts syslog messages.

Syslog usually uses port 514.

6. Click **Save**.

Refer to the manufacturer's instructions if you need assistance.

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 **cef**.

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 **ADMIN** > **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 **ADMIN** > **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

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.