

RSA NetWitness Platform

Event Source Log Configuration Guide



Solarwinds IPAM

Last Modified: Friday, July 20, 2018

Event Source Product Information:

Vendor: [Solarwinds](#)

Event Source: Solarwinds IP Address Manager

Versions: 4.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: solarwindsipam

Collection Method: Syslog

Event Source Class.Subclass: Network.Configuration Management

To configure the Solarwinds IPAM event source, you must:

- I. Configure Syslog Output on Solarwinds IPAM
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Solarwinds IPAM

Solarwinds can be configured to forward alerts to a Syslog server. The content of each alert contains information about why that alert is generated.

The following procedure describes how to configure Syslog output on Solarwinds.

To configure Solarwinds:

1. Log on to the Solarwinds console.
2. When editing or adding an alert, click **Add Action** in the **Trigger or Reset Action** section of the Alert wizard.
3. Select the **Send a SysLog Message** option, then click **Configure Action**.
4. Under Send a SysLog message settings:
 - a. Enter the Hostname or IP Address of the Netwitness Log Decoder in the field provided.
 - b. Select a Severity and a Facility from the drop down lists.
5. Enter the Message of your alert trigger in the field provided.
6. Schedule the action by selecting **Time of Day > Use special Time of Day** schedule for this action. This schedule only applies to the alert action you are editing.

Note: Use this to prevent an action from occurring during specific time windows
7. In **Execution Settings**, select the frequency for each triggered alert.
8. Click **Add Action**.

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 **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 **solarwindsipam**.



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.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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