

RSA NetWitness Logs

Event Source Log Configuration Guide



Lancope StealthWatch

Last Modified: Wednesday, May 03, 2017

Event Source Product Information:

Vendor: [Lancope](#)

Event Source: Lancope StealthWatch

Versions: 5.5, 5.6, 5.9, 5.10, 6.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: stealthwatch

Collection Method: Syslog

Event Source Class.Subclass: Security.IDS

StealthWatch Overview

The StealthWatch system by Lancope enables organizations to quickly resolve problems by providing actionable insight into network, security, and data center operations. StealthWatch delivers total network visibility from a single, integrated platform across both physical and virtual environments.

Configure StealthWatch

You can configure Lancope StealthWatch version 5.x through the event source itself or through the StealthWatch Management Console. For version 6.0, you must use the StealthWatch Management Console.

Configure StealthWatch From the Event Source Itself

You can configure version 5.x by using a web UI from the event source itself.

To configure the Lancope StealthWatch event source:

1. Log on to the StealthWatch web UI with administrative credentials.
2. Go to **Administration > Data Management > System Logging**.
3. In the Logging Configuration section, set the following values:
 - **Log Remotely:** Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
 - **Log locally:** Select the checkbox.
 - **Send messages securely:** Deselect the checkbox.
 - **Enable zero padded IP addresses in syslog:** Select the checkbox.
4. Click **Apply**.

Configure StealthWatch Using the Management Console

You can configure version 5.x or 6.0 by using the StealthWatch Management Console.

To configure the Lancope StealthWatch device using the StealthWatch Management Console:

1. Log on to the StealthWatch Management Console, with administrative credentials.
2. In the Menu bar, select **Configuration > Response Management. > Syslog Formats.**
 - a. Click **Add.**
 - b. In the **Name** field, enter a name .
 - c. In the MSG Part section, select the following variables in the order that they are listed below. Separate each variable with a comma, except for the last two variables where you use a space instead:

```
{start_active_time},{alarm_type_id},{alarm_type_name},"  
{details}",{source_ip},{source_zone_name},{target_ip},{target_  
zone_name},{port},{protocol},{device_ip},{end_active_time},  
{exporter_ip},{alarm_category_name},{alarm_severity_name},  
{alarm_severity_id},{source_url} {target_url}
```
 - d. Click **OK.**
3. Select **Actions.**
 - a. Click **Add.**
 - b. Select **Syslog Message**, and click **Add.**
 - c. In the **Name** field, enter a name.
 - d. Ensure that **Enabled** is selected.
 - e. Set the destination IP address by entering the IP address of the RSA NetWitness Log Decoder or Remote Log Collector for the server and port = **514.**
 - f. In the **Format** drop-down list, select the format that you created in Step 2a.
 - g. Click **OK.**
4. Select **Rules** and click **Add.**
 - a. Select **Host Alarm**, and click **OK.**
 - b. Select **Rule.**
 - c. In the **Name** field, enter a name.
 - d. Select **Actions.**

- e. Under the **Execute the following action when the Alarm becomes active** section, click **Add**.
 - f. Select the action that you created in Step 3, and click **OK**.
 - g. Under the **Execute the following action when the Alarm becomes inactive** section, click **Add**.
 - h. Select the action that you created in Step 3, and click **OK**.
 - i. Click **Ok**.
5. Click **Add**.
 - a. Select **StealthWatch Appliance System Alarm** and click **OK**.
 - b. Select **Rule**.
 - c. In the **Name** field, enter a name.
 - d. Select **Actions**.
 - e. Under the **Execute the following action when the Alarm becomes active** section, click **Add**.
 - f. Select the action that you created in Step 3, and click **OK**.
 - g. Under the **Execute the following action when the Alarm becomes inactive** section, click **Add**.
 - h. Select the action that you created in Step 3, and click **OK**.
 - i. Click **Ok**.
6. Click **Add**.
 - a. Select **Exporter or Interface Alarm** and click **OK**.
 - b. Select **Rule**.
 - c. In the **Name** field, enter a name.
 - d. Select **Actions**.
 - e. Under the **Execute the following action when the Alarm becomes active** section, click **Add**.
 - f. Select the action that you created in Step 3, and click **OK**.
 - g. Under the **Execute the following action when the Alarm becomes inactive** section, click **Add**.

- h. Select the action that you created in Step 3, and click **OK**.
 - i. Click **Ok**.
 - 7. Click **Add**.
 - a. Select **StealthWatch Management Console System Alarm**, and click **OK**.
 - b. Select **Rule**.
 - c. In the **Name** field, enter a name.
 - d. Select **Actions**.
 - e. Under the **Execute the following action when the Alarm becomes active** section, click **Add**.
 - f. Select the action that you created in Step 3, and click **OK**.
 - g. Under the **Execute the following action when the Alarm becomes inactive** section, click **Add**.
 - h. Select the action that you created in Step 3, and click **OK**.
 - i. Click **Ok**.
 - 8. Click **Close**.

Configure RSA 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 **stealthwatch**.



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 © 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.