RSA NetWitness Logs

Event Source Log Configuration Guide

ZScaler NSS

Last Modified: Monday, July 24, 2017

Event Source Product Information:

Vendor: ZScaler
Event Source: NSS
Versions: 4.1M

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: zscalernss
Collection Method: Syslog
Event Source Class.Subclass: Host.Web Logs

Configure ZScaler NSS

To configure Syslog collection for the ZScaler NSS you must:

I. Configure RSA NetWitness Suite for Syslog Collection

II. Configure Syslog Output on ZScaler NSS

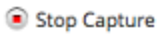
Configure RSA NetWitness Suite for Syslog Collection

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 

, click the icon to start capturing Syslog.
   - If you see 

, 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.

Configure Syslog Output on ZScaler NSS

Configure at least one feed that defines the logs that the ZScaler NSS sends to the RSA NetWitness Suite appliance and another feed that sends alerts. When you select **NSS Alerts** as the Log Type, select at which levels alerts will be sent: Warning and/or Critical. Multiple alert levels can be selected.

To configure ZScaler NSS to send logs to the RSA NetWitness Suite appliance:

1. Log in to the ZScaler Service with administrator credentials.
2. Click **Administration** > **Alerts & Notifications** > **Configure Nanalog Streaming Service**. Then click **Edit**.
3. Click **Add NSS Feed** and complete the following information:
   a. **Feed Name** - Enter or edit the name of the feed. Each feed is a connection between NSS and your RSA NetWitness Suite appliance.
   b. **NSS Name** - Choose an NSS from the list.
   c. **Status** - Choose **Enabled** to activate the feed or **Disabled** to deactivate it.
   d. **SIEM IP and TCP Port** - Enter the IP address and port of the RSA NetWitness Suite Log Decoder or Remote Log Collector to which the logs are streamed.
   e. **Log Type** - Specify which logs will be streamed by this NSS. Choose either **Web Log** or **NSS Alerts**. If you choose Web Log, complete the fields below. If you choose NSS Alerts, select the alert levels.
   f. **Feed Output Type** - The output is a comma-separated list by default. Choose **Custom**.
   g. **Feed Output Format** - These are the fields that will be displayed in the output.

Chose **Custom** as the Field Output Type, change the delimiter as well. See **NSS Output Format** for information about the available fields and their syntax.

h. **User Obfuscation** - You can enable user obfuscation. When you do, it displays a random string instead of the user names. If this is enabled, the 'login' field in Feed Format Output automatically changes to 'ologin' field which outputs the obfuscated login name. Choose **Disable** to display the user names.

i. **Timezone of the date and time in log output** - By default, this is set to the organization's time zone. The time zone you set applies to the time field in the output file. The time zone automatically adjusts to changes in daylight savings in the specific time zone. The configured time zone can be output to the logs as a separate field. The list of timezones is derived from the IANA Time Zone database. Direct GMT offsets can also be specified.

j. **Duplicate Logs** - To ensure that no logs are skipped during any down time, specify the number of minutes that NSS will send duplicate logs. (For more information, see NSS Resiliency.)

k. **Select which logs are sent to the SIEM…** - Optionally, you can define filters to limit which logs are sent to the SIEM.

4. Click **Done** to exit the **Add NSS Feed** page.

5. Click **Save**, and then click **Activate Now**.

NSS Output Format - Feed Output Format

Feed Output Format must be set to the following:

```
<134>1 ZSCALERNSS: time=%s{time}^^timezone=%s{tz}^^action=%s
{action}
^^reason=%s{reason}^^hostname=%s{host}^^protocol=%s
{proto}^^serverip=%s{sip}
^^url=%s{url}^^urlcategory=%s{urlcat}^^urlclass=%s
{urlclass}^^dlpdictionaries=%s{dlpdict}
^^dlpengine=%s{dlpeng}^^filetype=%s{filetype}^^threatcategory=%s
{malwarecat}
^^threatclass=%s{malwareclass}^^pagerisk=%d
{riskscore}^^threatname=%s{threatname}
```

```
^^clientpublicIP=%s{cintip}^^ClientIP=%s{cip}^^location=%s
{location}
^^refererURL=%s{referer}^^useragent=%s{ua}^^department=%s
{dept}^^user=%s{login}
^^event_id=%d{recordid}^^clienttranstime=%d
{ctime}^^requestmethod=%s{reqmethod}
^^requestsize=%d{reqsize}^^requestversion=%s{reqversion}^^status=%s
{respcode}
^^responsesize=%d{respsize}^^responseversion=%s
{respversion}^^transactionsize=%d{totalsize} \n
```


Trademarks