

NetWitness[®] Platform XDR

Zscaler NSS Event Source Log Configuration Guide

ZScaler NSS

IMPORTANT: NetWitness recommends you to use [ZScaler ZIA](#) parser to collect Web Logs. Zscaler NSS will be discontinued and NetWitness deprecates the Zscaler NSS.

Event Source Product Information:

Vendor: [ZScaler](#)

Event Source: NSS

Versions: 4.1M

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.0 and later

Event Source Log Parser: zscalernss

Collection Method: Syslog

Event Source Class.Subclass: Host.Web Logs

Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2022

Contents

Configure ZScaler NSS	5
Configure NetWitness Platform XDR for Syslog Collection	5
Configure Syslog Output on ZScaler NSS	7
NSS Output Format - Feed Output Format	8
Getting Help with NetWitness Platform XDR	9
Self-Help Resources	9
Contact NetWitness Support	9
Feedback on Product Documentation	10

Configure ZScaler NSS

To configure Syslog collection for the ZScaler NSS you must:





- I. Configure NetWitness Platform XDR for Syslog Collection
- II. Configure Syslog Output on ZScaler NSS

Configure NetWitness Platform XDR 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.

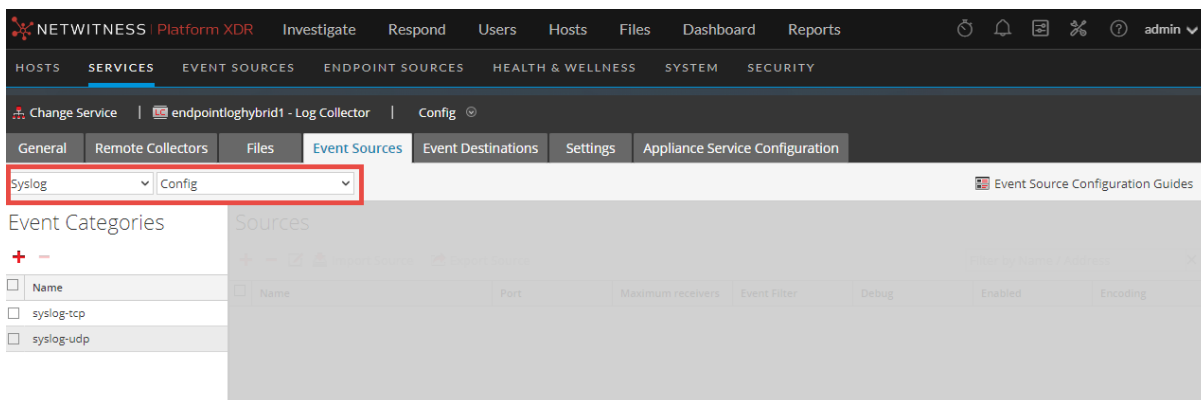
You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure Log Decoder for Syslog Collection

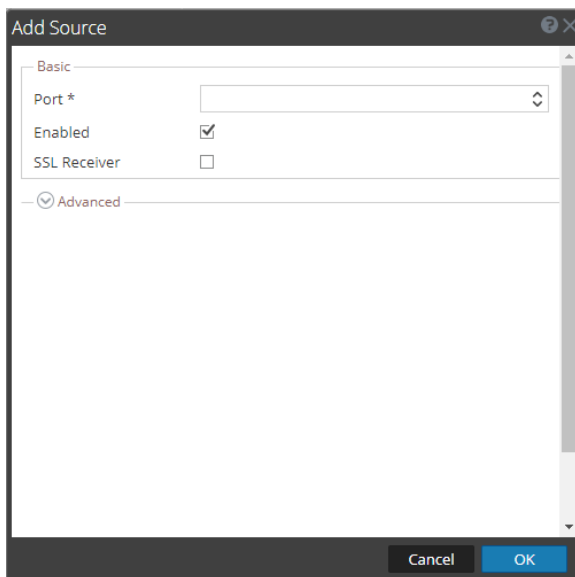
1. In the NetWitness Platform XDR menu, select  (Admin) > **Services**.
2. In the **Services** grid, choose a Log Decoder and from the **Actions** () menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:
 - If you see  **Start Capture**, click the icon to start capturing Syslog.
 - If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure Remote Log Collector for Syslog Collection

1. In the NetWitness Platform XDR menu, go to  (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 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. You can continue to add Syslog event sources to your system without a need to do any further configuration in NetWitness Platform XDR.

Configure Syslog Output on ZScaler NSS

Configure at least one feed that defines the logs that the ZScaler NSS sends to the NetWitness Platform XDR 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 Platform XDR:

1. Log in to the ZScaler Service with administrator credentials.
2. Click **Administration > Alerts & Notifications > Configure Nalog 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 NetWitness Platform XDR.
 - 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 of the NetWitness 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}
^^referrerURL=%s{referrer}^^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}^^transactionsiz=%d{totalsize} \n
```


Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click Support > Case Portal > View My Cases .
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.