RSA NetWitness Platform

Event Source Log Configuration Guide

Zscaler Deception

Last Modified: Friday, October 7, 2022

Event Source Product Information:

Vendor: Zscaler
Event Source: Zscaler Deception
Versions: v4.13.10

RSA Product Information:

Supported On: NetWitness Platform 11.0 and later
Event Source Log Parser: deception
Collection Method: Syslog
Event Source Class.Subclass: IPS

Configure Zscaler Deception

To configure Syslog collection for the Zscaler Deception, you must:

- Configure Syslog Output on Zscaler Deception
- Configure NetWitness Platform for Syslog Collection

Configure Syslog Output on Zscaler Deception

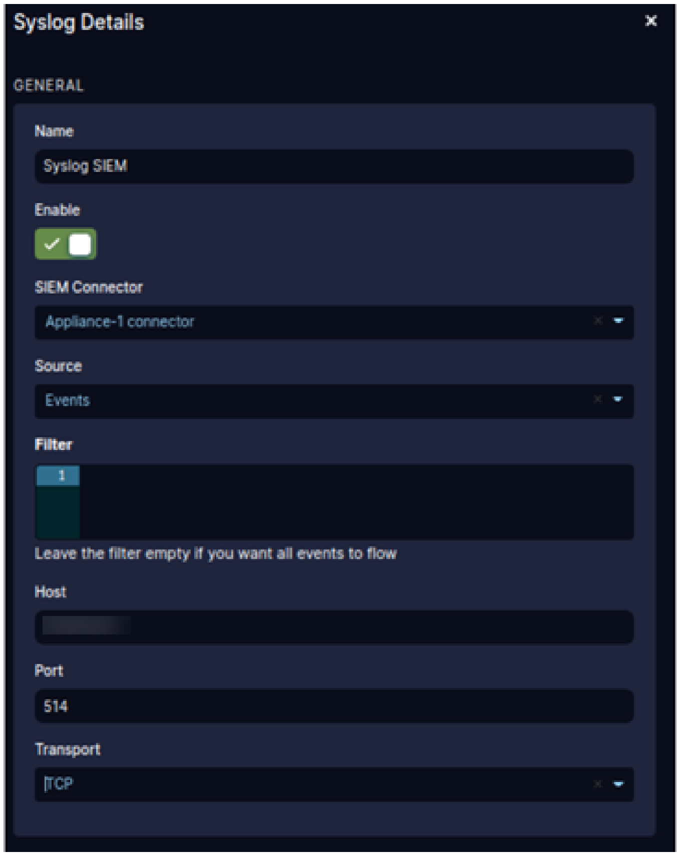
Configure a SIEM connector to forward logs to a Syslog server. Do the following:

1. Log in to Zscaler Deception Admin Portal.
2. Go to **Orchestrate** > **SIEM** > **Integrations**.
3. Click the **Add Integration** button and select **Syslog** from the drop-down.
4. In the **Syslog Details** view,
   - Enter the name of the integration in the **Name** field.

     For Example: **Syslog Event Integration**.
   - Enable the rule with the toggle button.
   - Select one of following SIEM connectors from the drop-down:
     - **Deception Connector**: If you select this, the Zscaler Deception Admin Portal will send logs to the Syslog server.
     - **Appliance Connector**: If you select this, the selected Appliance will send logs to the Syslog server.
   - Select the **Source** from the drop-down list. Do one of the following:
     - **Event logs**: Select this option if you want to send event logs to the Syslog server.
     - **Audit logs**: Select this option, if you want to send audit logs to the Syslog server.
   - In the **Filters** field, specify a filter query to send filtered event logs to the Syslog server.

     > **Note:** If you want to send all the events, leave the **Filters** field blank.
   - Enter the Server IP address for the Syslog server in the **Host** field.
   - Enter the port that the Syslog server listens to in the **Port** field.
   - In the **Transport** field, select one of the following:
     - **TCP**

- **UDP**



Syslog Details

GENERAL

Name: Syslog SIEM

Enable: ✓

SIEM Connector: Appliance-1 connector

Source: Events

Filter:

Leave the filter empty if you want all events to flow

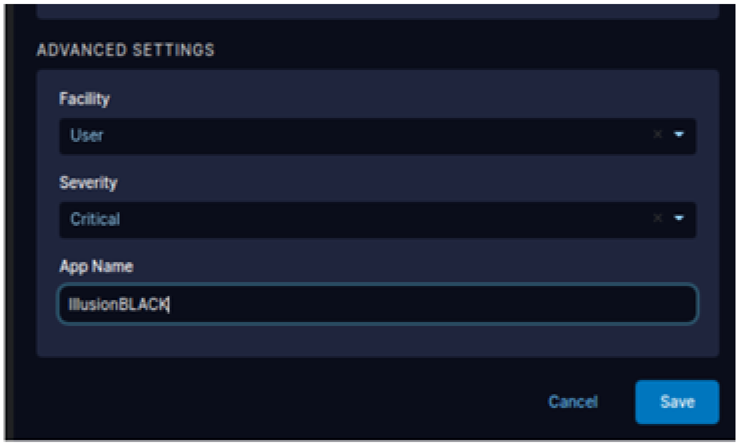
Host: [redacted]

Port: 514

Transport: TCP

5. In the **ADVANCED SETTINGS** view,
   - Select the following:
     - **Facility**: Each message is labeled with a facility code, indicating the software type generating the message.
     - **Severity**: Each message is labeled with a severity, indicating the severity of the tool generating the message.
   - Enter the following:

- **App Name**: This is just a log identifier and it can be set to any relevant text.



ADVANCED SETTINGS

Facility: User

Severity: Critical

App Name: IllusionBLACK

Configure NetWitness Platform for Syslog Collection

Ensure that the parser for your event source is available:

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 **deception**.

Note: Syslog collection must be configured only for the first time when you set up an event source which uses Syslog to send its output to NetWitness.

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

Log Decoder Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, select **Administration** > **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.

Remote Log Collector Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, go to **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 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. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

November 2020

Trademarks

RSA Conference Logo, 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.