

Z Scaler Integrations

Introduction

This integration is for Zscaler Internet Access logs. It can be used to receive logs sent by NSS log server on respective TCP ports.

The log message is expected to be in JSON format. The data is mapped to ECS fields where applicable and the remaining fields are written under `zscaler_zia.<data-stream-name>.*`.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Compatibility

This package has been tested against Zscaler Internet Access version 6.1

Requirements

Steps for setting up NSS Feeds

1. Enable the integration with the TCP input.
2. Configure the Zscaler NSS Server and NSS Feeds to send logs to the Elastic Agent that is running this integration. See Add NSS Server and Add NSS Feeds. Use the IP address hostname of the Elastic Agent as the 'NSS Feed SIEM IP Address/FQDN', and use the listening port of the Elastic Agent as the 'SIEM TCP Port' on the Add NSS Feed configuration screen. To configure Zscaler NSS Server and NSS Feeds follow the following steps.
 - In the ZIA Admin Portal, add an NSS Server.
 - Log in to the ZIA Admin Portal using your admin account. If you're unable to log in, contact Support.
 - Add an NSS server. Refer to Adding NSS Servers to set up an Add NSS Server for Web and/or Firewall.
 - Verify that the state of the NSS Server is healthy.

- In the ZIA Admin Portal, go to Administration > Nanolog Streaming Service > NSS Servers.
- In the State column, confirm that the state of the NSS server is healthy.

Graphical user interface, textDescription automatically generated

- In the ZIA Admin Portal, add an NSS Feed.
- Refer to [Add NSS Feeds](#) and select the type of feed you want to configure. The following fields require specific inputs:
- **SIEM IP Address:** Enter the IP address of the [Elastic agent](#) you'll be assigning the Zscaler integration to.
- **SIEM TCP Port:** Enter the port number, depending on the logs associated with the NSS Feed. You will need to create an NSS Feed for each log type.
 - Alerts: 9010
 - DNS: 9011
 - Firewall: 9012
 - Tunnel: 9013
 - Web: 9014
- **Feed Output Type:** Select Custom in Feed output type and paste the appropriate response format in Feed output format as follows:

Graphical user interface, applicationDescription automatically generated

Steps for setting up Cloud NSS Feeds

1. Enable the integration with the HTTP Endpoint input.
2. Configure the Zscaler Cloud NSS Feeds to send logs to the Elastic Agent that is running this integration. Provide API URL to send logs to the Elastic Agent. To configure Zscaler Cloud NSS Feeds follow the following steps.
 - In the ZIA Admin Portal, add a Cloud NSS Feed.
 - Log in to the ZIA Admin Portal using your admin account.
 - Add a Cloud NSS Feed. See to [Add Cloud NSS Feed](#).
 - In the ZIA Admin Portal, go to Administration > Nanolog Streaming Service > Cloud NSS Feeds.

- Give Feed Name, change status to Enabled.
- Select NSS Type.
- Change SIEM Type to other.
- Add an API URL.
- Default ports:
 - DNS: 9556
 - Firewall: 9557
 - Tunnel: 9558
 - Web: 9559
- Select JSON as feed output type.
- Add same custom header along with its value on both the side for additional security.

Graphical user interface, text, application, emailDescription automatically generated

3. Repeat step 2 for each log type.

Please make sure to use the given response formats for NSS and Cloud NSS Feeds.

Note: Please make sure to use latest version of given response formats.

Zscaler Integration?Procedures

Please provide the following information to CyTech:

Collect Zscaler Internet Access logs via TCP input

1. Listen Address - The bind address to listen for TCP connections.
2. Types:
 - TCP Listen Port for Zscaler Internet Access Alerts
 - TCP Listen Port for Zscaler Internet Access DNS logs
 - TCP Listen Port for Zscaler Internet Access Firewall Logs
 - TCP Listen Port for Zscaler Internet Access Tunnel Logs
 - TCP Listen Port for Zscaler Internet Access Web Logs

Collect Zscaler Internet Access logs via HTTP Endpoint

1. Listen Address - The bind address to listen for http endpoint connections.

2. Types:

- TCP Listen Port for Zscaler Internet Access DNS logs
- TCP Listen Port for Zscaler Internet Access Firewall Logs
- TCP Listen Port for Zscaler Internet Access Tunnel Logs
- TCP Listen Port for Zscaler Internet Access Web Logs

Revision #2

Created 23 April 2024 15:04:27

Updated 19 June 2024 06:54:01