Zscaler and Splunk
SIEM Deployment Guide

June 2019

Version 1.0
Table of Contents

1 Document Overview ........................................................................................................... 4
  1.1 Document Audience ....................................................................................................... 4
  1.2 Software Revisions ........................................................................................................ 4
  1.3 Request for Comments ................................................................................................. 4
  1.4 Document Prerequisites ............................................................................................... 5
  1.5 Document Revision Control ......................................................................................... 6

2 Understanding Syslog.......................................................................................................... 7
  2.1 Syslog Message Structure Overview ............................................................................. 7
     2.1.1 RFC3164 ................................................................................................................ 8
     2.1.2 RFC 5424 ................................................................................................................ 9
  2.2 Syslog Message Formats ............................................................................................... 10
     2.2.1 Common Event Format (CEF) .................................................................................. 10
     2.2.2 Log Event Extended Format (LEEF) ....................................................................... 10
  2.3 Zscaler Logging Architecture Overview ...................................................................... 11
  2.4 ZSS Log Feeds .............................................................................................................. 12

3 Configuring ZIA for NSS .................................................................................................. 13
  3.1 Logging into ZIA ............................................................................................................ 13
  3.2 Configuring Nanolog Streaming Service (NSS) .......................................................... 14
     3.2.1 Nanolog Streaming Service (NSS) ........................................................................ 14
     3.2.2 Verify NSS Server State ....................................................................................... 15
     3.2.3 Add NSS Feed ....................................................................................................... 16
     3.2.4 Configure NSS Feed ............................................................................................. 17

4 Configuring Splunk for NSS/Zscaler ................................................................................. 18
  4.1 Getting Zscaler data into Splunk .................................................................................. 18
     4.1.1 Configure new Index in Splunk .............................................................................. 18
     4.1.2 Add zscaler Index in Splunk .................................................................................. 19
     4.1.3 Configure new tcp input in Splunk ......................................................................... 20
     4.1.4 Select the desired zscaler Source Type .................................................................. 21
     4.1.5 Change Default App Context and Default index ..................................................... 22
     4.1.6 Verify incoming logs ............................................................................................. 23
     4.1.7 Inspect log fields ................................................................................................... 24
     4.1.8 Extracted log fields ............................................................................................... 25

5 Requesting Zscaler Support ............................................................................................. 26
  5.1 Gather Support Information ......................................................................................... 26
     5.1.1 Obtain Company ID ............................................................................................... 26
     5.1.2 Save Company ID ................................................................................................. 27
     5.1.3 Enter Support Section ........................................................................................... 28

6 Appendix A: Zscaler Resources ....................................................................................... 29

7 Appendix B: Splunk Resources ......................................................................................... 30
# Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF</td>
<td>Common Event Format</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation <em>(RFC2890)</em></td>
</tr>
<tr>
<td>LEEF</td>
<td>Log Event Extended Format</td>
</tr>
<tr>
<td>LSS</td>
<td>Logging Streaming Service (For ZPA)</td>
</tr>
<tr>
<td>NSS</td>
<td>Nanolog Streaming Service (For ZIA)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer <em>(RFC6101)</em></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security <em>(RFC5246)</em></td>
</tr>
<tr>
<td>ZAPP</td>
<td>Zscaler End-point Client Application</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
1 Document Overview

This Deployment Guide document will provide guides examples for configuring Zscaler Internet Access and Splunk Enterprise. This guide is intended for standing up proof-on-concept topologies and demos, for evaluating interoperability, and joint integration. This guide should not be used to configure either vendor platform for production use. For production deployments, please contact Zscaler or Splunk for post-sale deployment assistance.

1.1 Document Audience

This document was designed for Network Security Engineers and Network Engineers. All examples in this guide presumes the reader has a basic comprehension of basic IP Networking and Syslog (RFC5424). For additional product and company resources, please refer to the Appendix section.

1.2 Software Revisions

This document was written using Zscaler Internet Access v5.7 and Splunk Enterprise v7.2.6.

1.3 Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact partner-doc-support@zscaler.com.
1.4 Document Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 5.7 (or newer)
- ZIA entitlement for NSS
- Working version of NSS (if not, please refer to appendix for install)
- Administrator login credentials to ZIA

Splunk

- Administrator login credentials to Splunk instance
### 1.5 Document Revision Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Change Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>June 2019</td>
<td>Initial document created by Zscaler</td>
</tr>
</tbody>
</table>
2 Understanding Syslog

Syslog has been around for a number of decades and provides a protocol used for transporting event messages between computer systems and software applications. The Syslog protocol utilizes a layered architecture, which allows the use of any number of transport protocols for transmission of Syslog messages. It also provides a message format that allows vendor-specific extensions to be provided in a structured way. Syslog is now standardized by the IETF in RFC 5424 (since 2009), but has been around since the 80's and for many years served as the de facto standard for logging without any authoritative published specification.

Syslog messages include time stamps, event messages, severity, host IP addresses, diagnostics, and more. In terms of its built-in severity level, it can communicate a range between level 0, an Emergency, level 5, a Warning, System Unstable, critical and level 6 and 7 which are Informational and Debugging.

The following sections will provide an overview of Syslog structure, Syslog message formats, and Zscaler requirements.

2.1 Syslog Message Structure Overview

As mentioned prior, Syslog has been used for many decades. Over this time, new standards have been created to define new message formats, to support new use cases. As an over simplification, a Syslog message has the following structure: A header, followed by structured-data (SD), followed by a message. In this section, we will focus on the Syslog header and Syslog message (the body of the message).
2.1.1 RFC3164

RFC3164 is considered the “original” BSD structure from 2001. An example log message is shown below:

Figure 1: Syslog message in RFC 3164 format

Syslog Header:

- `<34>`: is a priority number. It represents the facility number multiplied by 8, to which severity is added. In this case, facility=4 (Auth) and severity=2 (Critical)
- **Oct 11 22:14:15**: is the timestamp. It misses the year, the time-zone and doesn’t have sub-second information
- **mymachine**: is a host name where the message was written
- **su**: is a tag. Typically this is the process name – sometimes having a PID (e.g. su[1234];)

Syslog Message:

- **Remainder**: the message (MSG) is everything after the tag
2.1.2 RFC 5424

The “New” (2009) format (RFC 5424)

RFC5424 compliant syslog message consists of three parts - “Syslog Header”, “Structured Data” and the actual log “message”

- **Syslog Header** consists of priority, version, timestamp, hostname etc.
- **Structured Data** in key=value format. It provides a mechanism to express information in a defined, parsable and interpretable data format. (e.g. SD-ID, SD-PARAM)
- **Actual log message** follows these two fields above (Message field is free-form)

```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su -- - 'su root' failed for login vick on /dev/pts/8
```

*Figure 2: Syslog message in RFC 5424 format*

- The dashes seen above are places for PID, message ID and other structured data you may have.

```
<100>2 1982-07-10T20:30:40.001Z myserver.com su 201 32001 - BOM 'su root' failed on /dev/pts/7
```

*Figure 3: Another syslog message in RFC 5424 format*
2.2 Syslog Message Formats

Zscaler supports many Syslog formats. This includes many industry standards and the ability to create custom log strings. This document will focus on the two primary standards used by SIEM vendors.

2.2.1 Common Event Format (CEF)

CEF is an open log management standard that improves the interoperability of security-related information from different security and network devices and applications.

Base CEF format:

CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Figure 4: CEF Format

2.2.2 Log Event Extended Format (LEEF)

Log Event Extended Format (LEEF) is a customized event format for IBM QRadar. It is designed to describe (network) security events and uses encoding and transport similar to those used by CEF. However, the two formats differ in the number and types of fields.

Base LEEF format:

LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

Figure 5: LEEF Format
2.3 Zscaler Logging Architecture Overview

Zscaler has two core products: Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA). At this time, this document will focus on ZIA. Future revisions of this document will include ZPA. For more information on NSS, please refer to the Appendix section for links to NSS documentation.

When customers use Zscaler, every customer initiated transaction that traverses ZIA will generate a corresponding log entry. These logs messages are retained by Zscaler for 6 months. Customers are able to view and search these logs using the Zscaler Admin dashboard.

For customers that want to send these logs to a SIEM (on premise or in-the-cloud), Zscaler Nanolog Streaming Service (NSS) is required. As an over simplification: think of NSS as an intermediate log gateway. Log messages are sent securely from Zscaler, to NSS, and NSS then converts the Zscaler log entries to Syslog.

Note: Although Syslog usually uses UDP and destination port 514, NSS only supports TCP. By using TCP, in the event the SIEM should become unavailable, NSS will be able to detect this by the loss of the TCP connection. And in the event of a failure, NSS will queue log messages until the SIEM returns (subject to storage).
2.4 ZSS Log Feeds

ZIA logs generated by Zscaler are of two types - Web and Firewall

This is due to different fields that need to be looked into/logged with http vs. non-http traffic

Depending on the type of logs of interest, we’ll need to deploy web and/or firewall NSS

Flow of events for log messages:

- Customer deploys web or firewall NSS; either on premises or in any cloud
- Customer registers this NSS with Zscaler (Using SSL certificates obtained from Zscaler)
- Customer accesses internet while going through Zscaler (ZIA)
- Zscaler generates syslog and it is sent to Zscaler’s Nanolog service cloud
- Nanolog cloud streams these logs in compressed & encrypted format to NSS
- NSS builds a separate TCP connection to SIEM & forwards these logs to it
3 Configuring ZIA for NSS

3.1 Logging into ZIA

First, we will setup the Zscaler side of this service. The required steps for this section are:

- Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, please contact support: https://help.zscaler.com/submit-ticket.

![Login to ZIA Portal](image)
3.2 Configuring Nanolog Streaming Service (NSS)

3.2.1 Nanolog Streaming Service (NSS)

After logging into ZIA, we first need to add a NSS Server and NSS Feed. First, we will create a new NSS Server. To navigate to the Nanolog Streaming area of ZIA, please follow: Administration -> Cloud Configuration -> and then click Nanolog Streaming Service.

![Figure 8: Configure Nanolog](https://admin.zscalerthree.net/#dashboard/1)
3.2.2 Verify NSS Server State

Before proceeding to further steps, ensure that NSS State is “Healthy”

![Figure 9: Verify Nanolog State](image)
3.2.3 Add NSS Feed

![Add NSS Feed](image)

Figure 10: Add NSS Feed
3.2.4 Configure NSS Feed

SIEM IP and TCP port should be filled in as per your network setup.
Feed Output Type should be set to “Splunk CIM” from the dropdown.

Figure 11: Configure NSS Feed
4  Configuring Splunk for NSS/Zscaler

Following steps assume that you have Admin access to a working instance of Splunk

4.1  Getting Zscaler data into Splunk

4.1.1  Configure new Index in Splunk

*After logging into Splunk, navigate to Settings -> Indexes -> New Index*

Figure 12: Add new Index to Splunk
4.1.2 Add zscaler Index in Splunk

Type “zscaler” without quotes (case sensitive) and hit save

Figure 13: Configure Zscaler Index
### 4.1.3 Configure new tcp input in Splunk

**After logging into Splunk, navigate to Settings -> Data Inputs -> TCP (Add new)**

This brings you to following screen. After configuring SIEM port, click next.

![Configure New Data Input](image)

- **File & Directories**: Upload a file, index a local file, or monitor an entire directory.
- **HTTP Event Collector**: Configure tokens that clients can use to send data over HTTP or HTTPS.
- **TCP/UDP**: Configure the Splunk platform to listen on a network port.
- **Scripts**: Get data from any API, service, or database with a script.
- **Aperture**
- **App Imports Disabler**: Disables app imports.
- **App Permissions Manager**: Ensures permissions policy.
- **AutoFocus Export**
- **Configuration Checker**: Runs configuration checks.

---

#### Configure instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog).

**Port**: [TCP | UDP]

- **In Zscaler portal, NSIS should be configured to stream logs to this SIEM port**
- **Example**: 514

**Source name override**: optional
- **Example**: hostport

**Only accept connection from**: optional
- **Example**: 10.1.2.3, hostport.splunk.com, *-splunk.com

---

#### FAQ

- How should I configure the Splunk platform for syslog traffic?
- What's the difference between receiving data over TCP versus UDP?
- Can I collect syslog data from Windows systems?
- What is a source type?
4.1.4 Select the desired zscaler Source Type

Type ‘zscaler’ to display all possible zscaler sourcetypes. Please select the option based on the kind of Zscaler logs being sent to Splunk.

Figure 15: Add Zscaler Source Type
### 4.1.5 Change Default App Context and Default index

On the same page as before:

Select “Zscaler Splunk App” as the App context
 select “zscaler” as the index from the drop down menu

(This is because Zscaler’s Splunk App by default expects data to be written at index titled zscaler). Click Review and then Submit.
4.1.6 Verify incoming logs

Click “Start Searching” to verify that logs are flowing from Zscaler into Splunk
4.1.7 **Inspect log fields**

You should see incoming logs from Zscaler.

![Inspect Incoming Logs](image-url)
4.1.8 Extracted log fields

Figure 19: Log fields from NSS Feed
5 Requesting Zscaler Support

5.1 Gather Support Information

5.1.1 Obtain Company ID

The navigation is: Administration -> Settings -> and then click Company profile

Figure 20: Navigate to Company profile
5.1.2 Save Company ID

![Company Profile](image)

**Company Profile**

**GENERAL INFORMATION**

**Company ID**

zscalerthree.net-1008708

**Name**

Fusion-Labs - Test Account

**Domains**

- [Domain](#)

**Address Line 1**

- [Address](#)

**Address Line 2**

- [Address](#)

*Figure 21: Company ID*
5.1.3 **Enter Support Section**

Now that we have our company ID, we are ready to open a support ticket. The navigation is: “?” and then click **Submit a Ticket**.

![Submit a ticket to Zscaler TAC](image.png)

**Figure 22: Submit a ticket to Zscaler TAC**
6 Appendix A: Zscaler Resources

Installing NSS:

NSS Deployment Guide
https://help.zscaler.com/zia/documentation-knowledgebase/analytics/nss/nss-deployment

NSS Troubleshooting Guide
https://help.zscaler.com/zia/troubleshooting-nss

General:

Zscaler: Getting Started
https://help.zscaler.com/zia/getting-started

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/
7 Appendix B: Splunk Resources

Zscaler Splunk App:  
https://splunkbase.splunk.com/app/3866

Zscaler Splunk Technical AddOn:  
https://splunkbase.splunk.com/app/3865

Contact Splunk Technical Support:  