# Table of Contents

1 Document Overview ........................................................................................................... 5  
1.1 Document Audience ....................................................................................................... 5  
1.2 Software Revisions ......................................................................................................... 5  
1.3 Request for Comments ................................................................................................... 5  
1.4 Document Prerequisites ................................................................................................. 6  
1.5 Document Revision Control ............................................................................................ 7  
1.6 Syslog Overview ............................................................................................................. 8  
  1.6.1 Syslog Message Structure Overview ........................................................................... 8  
  1.6.2 RFC3164 ....................................................................................................................... 8  
  1.6.3 RFC 5424 ...................................................................................................................... 9  
1.7 Syslog Message Formats ............................................................................................... 10  
  1.7.1 Common Event Format (CEF) ..................................................................................... 10  
  1.7.2 Log Event Extended Format (LEEF) ........................................................................ 10  
2 Zscaler Logging Architecture Overview ...................................................................... 11  
2.1 Nanolog Stream Service (NSS) .................................................................................. 11  
2.2 ZIA 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 ............................................................................................. 16  
  3.2.3 Add NSS Feed ............................................................................................................ 17  
  3.2.4 Configure NSS Feed ................................................................................................ 18  
  3.2.5 Edit NSS Feed (Web) ............................................................................................... 19  
  3.2.6 Edit NSS Feed (Firewall) .......................................................................................... 19  
3.3 Activate your changes ................................................................................................. 20  
4 Configuring Sentinel for Zscaler ............................................................................... 21  
4.1 Log into Azure Portal ................................................................................................... 21  
4.2 Deploy the Data-Connector Host VM .......................................................................... 22  
  4.2.1 Create virtual machine .............................................................................................. 23  
  4.2.2 Bind this VM to a Resource Group .......................................................................... 24  
4.3 Allowing Inbound Ports ............................................................................................... 25  
  4.3.1 Add Inbound Security Rule for syslog ..................................................................... 27  
  4.3.2 Add Inbound Security Rule for SSH ....................................................................... 28  
4.4 Create and Configure Sentinel Instance ..................................................................... 29  
  4.4.1 Create Log Analytics Workspace ........................................................................... 30  
  4.4.2 Name, Add, and Link a Resource group to workspace ........................................... 31  
  4.4.3 Add workspace to Azure Sentinel ........................................................................... 32  
4.5 Configure Data Collection .......................................................................................... 33  
  4.5.1 Search for Zscaler Connector .................................................................................. 34  
  4.5.2 Configure Syslog Agent ......................................................................................... 35
4.5.3 Pick a Zscaler Workbook ................................................................. 39
4.5.4 Explore Zscaler Workbook ............................................................. 40

5 Requesting Zscaler Support ...................................................................... 41
  5.1 Gather Support Information ............................................................... 41
      5.1.1 Obtain Company ID ................................................................. 41
      5.1.2 Save Company ID ............................................................... 42
      5.1.3 Enter Support Section ......................................................... 43

6 Appendix A: Zscaler Resources .............................................................. 44
  6.1 Installing NSS .............................................................................. 44
  6.2 Installing NSS on Azure .............................................................. 44
  6.3 Zscaler Feed Formats ........................................................... 44
  6.4 General Zscaler Resources ......................................................... 45

7 Appendix B: Azure Sentinel Resources ................................................. 46
  7.1 General Sentinel Resources ......................................................... 46
# 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 (RFC2890)</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>NSG</td>
<td>Network Service Group (Azure)</td>
</tr>
<tr>
<td>NSS</td>
<td>Nanolog Streaming Service (For ZIA)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (RFC6101)</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security (RFC5246)</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 Azure Sentinel. 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 Microsoft 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 in this document.

1.2 Software Revisions

This document was written using Zscaler Internet Access v5.7, NSS v4.0.4, and the latest Azure Sentinel version as of January, 2020.

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

To use this document, the following prerequisites are required:

**Zscaler Internet Access (ZIA):**

- An active instance of ZIA 5.7 (or newer)
- A working deployment of NSS (If not, please refer to appendix for install instructions)
- Administrator login credentials to ZIA

**Azure Sentinel:**

- Administrator login credentials to Microsoft Azure
- Active subscription with Azure Sentinel
### 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>July 2019</td>
<td>Initial document created by Zscaler</td>
</tr>
<tr>
<td>1.11</td>
<td>January 2020</td>
<td>Revised with Azure Sentinel GA launch</td>
</tr>
</tbody>
</table>
1.6 Syslog Overview

If you are unfamiliar with Syslog, this section will help you get up-to-speed. If you are already familiar with Syslog, please skip to section “Zscaler Logging Architecture Overview”.

1.6.1 Syslog Message Structure Overview

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 oversimplification, 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).

1.6.2 RFC3164

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

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
```

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
1.6.3 RFC 5424

The “New” (2009) format (RFC 5424) of syslog 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)

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.

Figure 3: Another syslog message in RFC 5424 format
1.7 **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.

### 1.7.1 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 Message Format](image)

### 1.7.2 Log Event Extended Format (LEEF)

Log Event Extended Format (LEEF) is a customized event format created by 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 Message Format](image)
2 Zscaler Logging Architecture Overview

Zscaler has two core products: Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA). At this time, the scope of this document only addresses ZIA. Future revisions of this document will include ZPA. ZIA’s ability to send log messages outside of Zscaler’s cloud requires a product known as **Nanolog Stream Service** (NSS).

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

2.1 Nanolog Stream Service (NSS)

As shown above, log messages are stored within Nanolog. When an organization deploys NSS for various log feeds (web and mobile shown in photo), each NSS opens a secure tunnel to the Nanolog in the Zscaler cloud. The Nanolog then streams copies of the logs to each NSS in a highly compressed format to reduce bandwidth footprint; the original logs are retained on the Nanolog.

When an NSS receives the logs from the Nanolog, it unscrambles them, applies the configured filters to exclude unwanted logs, converts the filtered logs to the configured output format so they can be parsed by your SIEM, and then streams the logs to your SIEM over a raw TCP connection.
For customers that want to send these logs to a SIEM (on premise of in-the-cloud), Zscaler NSS is required. As a simplification: think of NSS as an intermediate log gateway. NSS uses a virtual machine (VM) to stream traffic logs in real time from ZIA.

**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).

### 2.2 ZIA Log Feeds

An NSS feed specifies the data from the logs that the NSS will send to the SIEM. You can filter the data, so you send only the data you need to the SIEM. You can add one or more fields for the logs and one field for alerts. You can add up to 8 NSS feeds for each NSS. Each feed can have a different list of fields, a different format, and different filters. Below are the feeds supported today.

<table>
<thead>
<tr>
<th>Zcaler Platform &amp; Product</th>
<th>Feed Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA NSS</td>
<td>Web Logs</td>
</tr>
<tr>
<td>ZIA NSS</td>
<td>Firewall Logs</td>
</tr>
<tr>
<td>ZIA NSS</td>
<td>DNS Logs</td>
</tr>
<tr>
<td>ZIA NSS</td>
<td>Alert Logs</td>
</tr>
<tr>
<td>ZIA NSS</td>
<td>Tunnel Logs</td>
</tr>
</tbody>
</table>
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.
3.2 Configuring Nanolog Streaming Service (NSS)

**CAUTION!**
Log messages sent between Zscaler NSS and Azure data connector are *not encrypted!*
Hence, it’s strongly recommended that you spin up your NSS in same VNET as Azure data connector VM. In that case, plaintext log messages traffic will not leave your VNET.
If you are deploying NSS in a different network, you should use an external mechanism (e.g. IPSEC tunnel) to encrypt plaintext communication between NSS and Azure connector VM.

### 3.2.1 Nanolog Streaming Service (NSS)

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

Follow instructions listed on link below (based on your deployment type) to set up web and/or firewall NSS.


![Figure 8: Navigate to NSS](image-url)
NOTE:

If you are deploying a new NSS in Azure:

Zscaler NSS Azure Resource Manager (ARM) Template has been developed to automate setting up an NSS in Azure. This voids the need for manually running PowerShell scripts.

Deployment can take up to 1 hour to finish.

**Zscaler NSS Azure Resource Manager (ARM) Template** can be accessed using link:

https://github.com/zscaler/nss-azure-deploy

After ARM template deployment, check the IP address using “ifconfig -a”. We will configure another IP in the same network range. NSS requires two interfaces in same subnet.

SSH to NSS as and execute following commands as root. Change the IPs as needed to fit your environment:

```
[nss]
[nss]
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nss configure</code></td>
<td>Detected an Azure VM!!</td>
</tr>
<tr>
<td></td>
<td>(nameserver:168.63.129.16 (Options &lt;c:change, d:delete, n:no change&gt;) [n])</td>
</tr>
<tr>
<td></td>
<td>Do you wish to add a new nameserver? &lt;n:no y:yes&gt; [n]:</td>
</tr>
<tr>
<td></td>
<td>(smnet_dev (Service interface IP address with netmask) [192.168.100.4/24]: 192.168.100.5/24)</td>
</tr>
<tr>
<td></td>
<td>(smnet_dflt_gw (Service interface default gateway IP address) [192.168.100.1]: 192.168.100.1)</td>
</tr>
<tr>
<td></td>
<td>Successfully Applied Changes</td>
</tr>
<tr>
<td></td>
<td>[root@NSS /usr/home/zsroot]# nss update-now</td>
</tr>
<tr>
<td></td>
<td>Connecting to server...</td>
</tr>
<tr>
<td></td>
<td>Connecting to update server 104.129.193.117.</td>
</tr>
<tr>
<td></td>
<td>Installed build version: 209302</td>
</tr>
<tr>
<td></td>
<td>Latest available build version: 209302</td>
</tr>
<tr>
<td></td>
<td>Build file is up-to-date</td>
</tr>
<tr>
<td></td>
<td>Checking if installation required...</td>
</tr>
<tr>
<td></td>
<td>Service is up-to-date.</td>
</tr>
<tr>
<td></td>
<td>[root@NSS /usr/home/zsroot]# nss restart</td>
</tr>
<tr>
<td></td>
<td>Detected an Azure VM!!</td>
</tr>
<tr>
<td></td>
<td>NSS service stopped</td>
</tr>
<tr>
<td></td>
<td>NSS service running with pid 3000</td>
</tr>
<tr>
<td></td>
<td>[root@NSS /usr/home/zsroot]# nss enable-autostart</td>
</tr>
<tr>
<td></td>
<td>Detected an Azure VM!!</td>
</tr>
<tr>
<td></td>
<td>Auto-start of NSS enabled</td>
</tr>
<tr>
<td></td>
<td>[root@NSS /usr/home/zsroot]#</td>
</tr>
</tbody>
</table>
3.2.2 Verify NSS Server State

Before proceeding to further steps, ensure that NSS State is “Healthy”. If NSS is not healthy, please refer to troubleshooting steps listed in the Appendix section. If everything is as expected, you can move to the next section.

Figure 9: Verify NSS Server State
3.2.3 Add NSS Feed

An NSS feed specifies the data from the logs that the NSS will send to the SIEM. Each feed can have a different list of fields, a different format, and different filters. You can add one or more fields for the logs and one field for alerts.

![Figure 10: Add NSS Feed](image-url)
3.2.4 Configure NSS Feed

The following fields are required:

1) SIEM IP Address: The public IPv4 address of your Azure Sentinel data connector.

2) SIEM TCP Port: Should be 514.

3) Feed Output Type: Should be set to “Custom” from the dropdown

4) In this version of Zscaler (v5.7), the feed format needs to be edited to interoperate with Sentinel. Please refer to next section of this guide for the details.

![Configure NSS Feed](image-url)
3.2.5  Edit NSS Feed (Web)

Override the prepopulated CEF feed by replacing it with following block and then click “Save”.

```plaintext
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss
CEF:0|Zscaler|NSSWeblog|5.7|%s{action}|%s{reason}|3| act=%s{action}
reason=%s{reason} app=%s{proto} dhost=%s{ehost} dst=%s{sip} src=%s{cintip}
sourceTranslatedAddress=%s{cip} in=%d{respsize} out=%d{reqsize}
request=%s{eurl} requestContext=%s{ereferer} outcome=%s{respcode}
requestClientApplication=%s{ua} requestMethod=%s{reqmethod}
suser=%s{login} spriv=%s{location} externalId=%d{recordid}
fileType=%s{filetype} destinationServiceName=%s{appname} cat=%s{urlcat}
deviceDirection=1 cn1=%d{riskscore} cn1Label=riskscore cs1=%s{dept}
cs1Label=dept cs2=%s{urlcat} cs2Label=urlcat cs3=%s{malwareclass}
cs3Label=malwareclass cs4=%s{malwarecat} cs4Label=malwarecat
cs5=%s{threatname} cs5Label=threatname cs6=md5hash cs6Label=%s{bamd5}
rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass=%s{urlclass}
devicemodel=%s{devicemodel}
```

![Figure 12: Override CEF String for Web](image)

3.2.6  Edit NSS Feed (Firewall)

Override the prepopulated CEF feed by replacing it with following block and then click “Save”.

```plaintext
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-fw
CEF:0|Zscaler|NSSFWlog|5.7|%s{action}|%s{rulelabel}|3| act=%s{action}
suser=%s{login} src=%s{csip} spt=%d{csport} dst=%s{cdip} dpt=%d{cdport}
deviceTranslatedAddress=%s{ssip} deviceTranslatedPort=%d{ssport}
destinationTranslatedAddress=%s{sdip} destinationTranslatedPort=%d{sdport}
sourceTranslatedAddress=%s{tsip} sourceTranslatedPort=%d{tsport}
proto=%s{ipproto} tunnelType=%s{ttype} dnat=%s{dnat} stateful=%s{stateful}
spriv=%s{location} reason=%s{rulelabel} in=%ld{inbytes} out=%ld{outbytes}
deviceDirection=1 cs1=%s{dept} cs1Label=dept cs2=%s{nwsvc}
cs2Label=nwService cs3=%s{nwapp} cs3Label=nwApp cs4=%s{aggregate}
cs4Label=aggregatedService cs5=%s{threatcat} cs5Label=threatcat
cs6=%s{threatname} cs6Label=threatname cn1=%d{durationms}
cn1Label=durationms cn2=%d{numsessions} cn2Label=nsessions
cs5Label=ipCat cs5=%s{ipcat} destCountry=%s{destcountry}
avgduration=%d{avgduration}
```

![Figure 13: Override CEF String for Firewall](image)
3.3 **Activate your changes**

The last and final step to configure on the Zscaler side is to “Active” what we have configured to this point. All prior configurations to this point are candidate configurations. Once active, these changes will become active in production.

Navigate to **Activation** from the sidebar, and then click the “**Activate**” button to commit your changes.

![Figure 14: Activate your changes](image)
4 Configuring Sentinel for Zscaler

Following steps assume that you have Admin access to the Sentinel portal

4.1 Log into Azure Portal

Navigate to https://portal.azure.com and login using your account.

Figure 15: Log into Azure Portal
4.2 **Deploy the Data-Connector Host VM**

The first step in Azure is to deploy a Linux VM. This Linux VM will be used as the Zscaler data-connector, which will run Microsoft’s Operations Management Suite (OMS) agent. The OMS agent is the software component that will send log messages to Azure Sentinel. There are more software components on this VM that enable this data pipeline, but you need not worry about them as they are automatically configured by Azure.

After navigating to the **Home** screen click on “**Virtual Machine**”, as shown in Figure 16.

---

**Figure 16:** This VM will work as syslog server and run Azure’s data connector
4.2.1 Create virtual machine

When you arrive to this screen, your screen may have additional information being displayed, if you have existing virtual machines. Navigate to “Create Virtual Machine”, as shown in Figure 17.

Figure 17: Create virtual machine
4.2.2 Bind this VM to a Resource Group

A “Resource Groups” (RG) is a way to group a collection of assets in logical containers for easy automatic provisioning, monitoring, access control and for more effective management of their costs. One benefit of using RGs is grouping related resources that belong to an application together, as they share a unified lifecycle from creation to usage and finally, de-provisioning.

This VM could be bound to an existing resource group or we can create a new one. In this guide, we will create a new resource group and name it at this point. In this guide, we will use Ubuntu Server 18.04 LTS.

![Figure 18: Initiate VM deployment](image)

After filling up the pertinent details, click **“Review + create”** and follow subsequent prompt to finish VM creation. Once the deployment is complete, proceed to the next step.
4.3 Allowing Inbound Ports

We need to configure the Network Security Group (NSG) to permit inbound SSH access for management, and to allow inbound tcp/514 from NSS -> the OMS. By default, these ports are not permitted in Azure and we will manually allow inbound connections to tcp/22 and tcp/514. This access should be locked down and only permitted from specific source IPs. On the Azure “Home” page, in the search bar at the top, type “Network Security Groups” and select the option shown below.

![Figure 19: Network Security Groups](image19.png)

A new security group should have been automatically created by Azure with your resource group being tied to it. Open the auto created network security group as shown below.

![Figure 20: Network Security Groups Continued](image20.png)
Next, select the “Inbound Security Rules” option. This will allow us to configure the following rules to allow inbound connections.

- Protocol and port tcp/514 from your Zscaler NSS IP
- Protocol and port tcp/22 from your trusted network / management station

Please review to the following sections to see how to exactly configure each rule separately.

![Figure 21: Inbound Security Rule](image)
4.3.1 Add Inbound Security Rule for syslog

**NOTE:** Below, for testing purposes, we are allowing any source IP to connect to this data connector VM on port 514. **Post testing, you should restrict this access to NSS source IP only**

You will need to configure these fields to match your environment. Although the destination port is 514, the destination can be configured on the ZIA side to other ports. If you set this port to something other than 514 in ZIA, the port number must match here. Once you are done, select “Add” and move on to the next section.

![Add inbound security rule](image-url)
4.3.2 Add Inbound Security Rule for SSH

**NOTE:** Below, for testing purposes, we are allowing any source IP to connect to this data connector VM on port 22. Post testing, **you should restrict this access to trusted/management source IP only**

You will need to configure these fields to match your environment. The “Source” should match your trusted network / management station from which you want to allow the SSH access.

![Add inbound security rule](image)

**Figure 23: Add Inbound Security Rule for SSH**
4.4 *Create and Configure Sentinel Instance*

Navigate back to Home screen and search for ‘sentinel’ and click the option shown below.

![Figure 24: Navigate to Azure Sentinel](image)

*Figure 24: Navigate to Azure Sentinel*
4.4.1 Create Log Analytics Workspace

We first need to create a “Workspace” for Azure Sentinel. A Log Analytics workspace is a unique environment for Azure Monitor log data. Each workspace has its own data repository and configuration, data sources, and solutions are configured to store their data in a particular workspace. Click **Add**, then **Create a new workspace**, as shown in Figure 25.

![Figure 25: Create new workspace](image-url)
### 4.4.2 Name, Add, and Link a Resource group to workspace

This document presumes the steps are being performed in a new, non-production environment. In this guide, we will reuse the resource group created in step 4.1.4. If you are configuring this in an existing and/or production environment, your steps will be slightly different. You can proceed with one of the two steps below, followed by selecting “Ok” to proceed:

1) Link an existing ‘resource group’ to the new workspace

OR

2) Create and then link an entirely new resource group to this new workspace

![Image of workspace configuration](image)

Figure 26: Name, Add, and Link Resource Group to workspace
4.4.3 **Add workspace to Azure Sentinel**

Next, click the “**Add Azure Sentinel**” button at the bottom of the page. You will need to wait until the deployment finishes before moving to next section. This should take a few minutes.

![Add workspace to Azure Sentinel](image)

*Figure 27: Add workspace to Azure Sentinel*
4.5 Configure Data Collection

The first set to enable data collection is to configure data collection. To do so, you need to navigate: **News & guides -> Collect data**, as shown in Figure 28.

![Configure Zscaler Data-Connector](image-url)

Figure 28: Configure Zscaler Data-Connector
4.5.1 Search for Zscaler Connector

In the search box, type in “Zscaler” as shown in Figure 29. Next select it, and then click “Open connector page” at the bottom right of the page.

Figure 29: Search for Zscaler Connector
4.5.2 Configure Syslog Agent

After clicking ‘Open connector page’ you will be presented with following screen. Instruction on this page consists of:

Selecting a linux machine (in any cloud or on prem) that acts as a proxy between your security solution and Sentinel. We will use VM setup in step 4.1.4 for this purpose

Installing Azure monitoring agent (CEF connector) on this linux box

Figure 30: Steps to configure logging pipeline
Log into the VM we setup in step 4.1.4 using SSH and run the command highlighted below from cli

---

**Configuration**

1. **Linux Syslog agent configuration**
   Install and configure the Linux agent to collect your Common Event Format (CEF) Syslog messages and forward them to Azure Sentinel.
   
   Notice that the data from all regions will be stored in the selected workspace.

1.1 **Select or create a Linux machine**
   Select or create a Linux machine that Azure Sentinel will use as the proxy between your security solution and Azure Sentinel. This machine can be on your on-prem environment, Azure or other clouds.

1.2 **Install the CEF collector on the Linux machine**
   Install the Microsoft Monitoring Agent on your Linux machine and configure the machine to listen on the necessary port and forward messages to your Azure Sentinel workspace. The CEF collector collects CEF messages on port 514 TCP.
   
   1. Make sure that you have Python on your machine using the following command: python --version.
   2. You must have elevated permissions (sudo) on your machine.

   Run the following command to install and apply the CEF collector:
   ```bash
   sudo wget https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/CEF/CEFicts/CEFicts.ipc
   ```

2. **Forward Common Event Format (CEF) logs to Syslog agent**
   Set Zscaler product to send Syslog messages in CEF format to your Syslog agent. Make sure you to send the logs on port 514 TCP.
   
   Go to [Zscaler Sentinel integration guide](#) to learn more.

3. **Validate connection**
   Follow the instructions to validate your connectivity:
   
   Open Log Analytics to check if the logs are received using the CommonSecurityLog schema.
   
   It may take about 20 minutes until the connection streams data to your workspace.

   If the logs are not received, run the following connectivity validation script:
You should see output “Installation completed” and netstat output should show syslog server and Azure collector agent (ruby scripts) to be running.
If you run into issues, running following command will help in troubleshooting

<table>
<thead>
<tr>
<th>Instructions</th>
<th>Next steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the Microsoft Monitoring Agent on your Linux machine and configure the machine to listen on the necessary port and forward messages to your Azure Sentinel workspace. The CEF collector collects CEF messages on port 514 TCP.</td>
<td></td>
</tr>
<tr>
<td>1. Make sure that you have Python on your machine using the following command: python --version.</td>
<td></td>
</tr>
<tr>
<td>2. You must have elevated permissions (sudo) on your machine.</td>
<td></td>
</tr>
<tr>
<td>Run the following command to install the CEF collector: sudo wget <a href="https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataCon">https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataCon</a>...</td>
<td></td>
</tr>
<tr>
<td>2. Forward Common Event Format (CEF) logs to Syslog agent</td>
<td></td>
</tr>
<tr>
<td>Set Zscaler product to send Syslog messages in CEF format to your Syslog agent. Make sure you to send the logs on port 514 TCP.</td>
<td></td>
</tr>
<tr>
<td>Go to Zscaler Sentinel integration guide to learn more.</td>
<td></td>
</tr>
<tr>
<td>3. Validate connection</td>
<td></td>
</tr>
<tr>
<td>Follow the instructions to validate your connectivity:</td>
<td></td>
</tr>
<tr>
<td>Open Log Analytics to check if the logs are received using the CommonSecurityLog schema.</td>
<td></td>
</tr>
<tr>
<td>It may take about 20 minutes until the connection streams data to your workspace.</td>
<td></td>
</tr>
<tr>
<td>If the logs are not received, run the following connectivity validation script:</td>
<td></td>
</tr>
<tr>
<td>1. Make sure that you have Python on your machine using the following command: python --version</td>
<td></td>
</tr>
<tr>
<td>2. You must have elevated permissions (sudo) on your machine</td>
<td></td>
</tr>
<tr>
<td>Run the following command to validate your connectivity. sudo wget <a href="https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataCon">https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataCon</a>...</td>
<td></td>
</tr>
<tr>
<td>4. Secure your machine</td>
<td></td>
</tr>
<tr>
<td>Make sure to configure the machine’s security according to your organization’s security policy</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 33: Troubleshoot collector agent installation**
4.5.3 Pick a Zscaler Workbook

Navigate to Dashboard -> Azure Sentinel Workspaces -> Workbooks & search for 'zscaler' Select the Workbook that you are interested in and click 'View template'
You can also ‘save’ the workbook to a geographic location and revisit it later

![Figure 34: Select Zscaler workbook](image)
4.5.4 Explore Zscaler Workbook

Workbooks are responsive & can be clicked around to drill down based on different criterions. Filtering can be done by selecting options towards top of the page or by clicking on individual entries.

Figure 35: Sample workbook visualization
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 36: Collecting details to open support case with Zscaler TAC](image)
5.1.2 Save Company ID

![Company Profile](image)

**Company Profile**

**ORGANIZATION**

**SUBSCRIPTIONS**

**GENERAL INFORMATION**

**Company ID**

```
zscalerthree.net-1008708
```

**Name**

Tushar-Labs - Test Account

**Domains**

```
www.
```

**Address Line 1**


**Address Line 2**


Figure 37: Company ID
Now that we have our company ID, we are ready to open a support ticket. The navigation is: “?” and then click **Submit a Ticket**.
6 Appendix A: Zscaler Resources

6.1 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

6.2 Installing NSS on Azure

Deploy NSS on Azure

Zscaler NSS Azure Resource Manager (ARM) Template
https://github.com/zscaler/nss-azure-deploy

6.3 Zscaler Feed Formats

Web Logs

Firewall Logs

DNS Logs

Tunnel Logs
6.4 **General Zscaler Resources**

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: Azure Sentinel Resources

7.1 General Sentinel Resources

Azure Sentinel Documentation:
https://docs.microsoft.com/en-us/azure/sentinel/

Azure support:
https://portal.azure.com/#blade/Microsoft_Azure_Support/HelpAndSupportBlade/overview

Sentinel Query Language Reference:
https://docs.microsoft.com/en-us/azure/kusto/query/