ZSCALER AND AZURE SENTINEL DEPLOYMENT GUIDE
## Contents

**Terms and Acronyms**  
4

**About This Document**  
5

- **Zscaler Overview**  
5
  - Zscaler Resources  
5
- **Azure Sentinel Overview**  
6
  - Azure Sentinel Resources  
6
- **Audience**  
6
- **Software Versions**  
6
- **Request for Comments**  
6

**Document Prerequisites**  
7

- **Syslog Overview**  
7
- **Syslog Message Structure Overview**  
7
- **RFC3164**  
7
- **RFC 5424**  
8

**Syslog Message Formats**  
8

- **Common Event Format (CEF)**  
8
- **Log Event Extended Format (LEEF)**  
9

**Zscaler Logging Architecture Overview**  
10

- **Nanolog Stream Service (NSS)**  
10
- **ZIA Log Feeds**  
11

**Configuring ZIA for NSS**  
12

- **Logging into ZIA**  
12
- **Configuring Nanolog Streaming Service (NSS)**  
12
  - Nanolog Streaming Service (NSS)  
13
  - Verify NSS Server State  
15
- **Add NSS Feed**  
15
- **Configure NSS Feed**  
16
Edit NSS Feed (Web) 16
Edit NSS Feed (Firewall) 17
Edit NSS Feed (DNS) 17
Activate your changes 18

Configuring Sentinel for Zscaler 19

Log into Azure Portal 19
Deploy the Data-Connector Host VM 20
Create Virtual Machine 21
Bind this VM to a Resource Group 22

Allowing Inbound Ports 23
Add Inbound Security Rule for syslog 25
Add Inbound Security Rule for SSH 26

Create and Configure Sentinel Instance 27
Create Log Analytics Workspace 27
Name, Add, and Link a Resource Group to Workspace 28
Add Workspace to Azure Sentinel 29

Configure Data Collection 30
Search for Zscaler Connector 31
Configure Syslog Agent 32
Pick a Zscaler Workbook 35
Explore Zscaler Workbook 35

Appendix A: Requesting Zscaler Support 36
Gather Support Information 36
Save Company ID 36
Enter Support Section 37
# 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>
About This Document

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Flagship offerings, Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can’t match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, view www.zscaler.com or follow Zscaler on Twitter @zscaler.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZPA Help Portal</td>
<td>Help articles for ZPA</td>
</tr>
<tr>
<td>NSS Deployment Guide</td>
<td>Help article for NSS deployment.</td>
</tr>
<tr>
<td>NSS Troubleshooting Guide</td>
<td>Help article for NSS troubleshooting.</td>
</tr>
<tr>
<td>Deploy NSS on Azure</td>
<td>Help article on deploying NSS on Azure.</td>
</tr>
<tr>
<td>Web Logs</td>
<td>Help article on Zscaler web logs.</td>
</tr>
<tr>
<td>Firewall Logs</td>
<td>Help article on Zscaler firewall logs.</td>
</tr>
<tr>
<td>DNS Logs</td>
<td>Help article on Zscaler DNS logs.</td>
</tr>
<tr>
<td>Tunnel Logs</td>
<td>Help article on Zscaler tunnel logs.</td>
</tr>
<tr>
<td>Sentinel Deployment</td>
<td>Walkthrough on configuring Zscaler with Azure Sentinel.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
Azure Sentinel Overview

Microsoft Azure, part of Microsoft.com (NASDAQ: MSFT) and commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. Azure Active Directory (Azure AD) is Microsoft’s cloud-based identity and access management service. Azure AD is an integral part of the Azure solution that provides:

- Authentication
- Conditional access
- Device Management
- Domain Services
- Identity Governance
- Identity Protection
- Privileged Identity Management

For more information on Azure, view azure.microsoft.com or follow them on Twitter @microsoft.

Azure Sentinel Resources

The following table contains links to Azure support resources.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling Private Preview of the Zscaler Data Connector</td>
<td>Help article on enabling private preview in Azure Sentinel.</td>
</tr>
<tr>
<td>Azure Sentinel Documentation</td>
<td>Article with use cases to get started using Microsoft Sentinel.</td>
</tr>
<tr>
<td>Azure support</td>
<td>Support portal for Azure problems and help.</td>
</tr>
<tr>
<td>Sentinel Query Language Reference</td>
<td>Kusto query overview.</td>
</tr>
</tbody>
</table>

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to the Zscaler Resources and Azure Active Directory (AAD) Identity Resources.

Software Versions

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

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Please contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- For Zscaler Employees: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.
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

Syslog Overview
This section explains Syslog. If you are already familiar with Syslog, skip to the section Zscaler Logging Architecture Overview.

Syslog Message Structure Overview
Syslog has been used for many decades, but over time new standards were created to define new message formats and support new use cases. Briefly, a Syslog message has the following structure (in order): a header, structured data (SD), a message. In this section, we focus on the Syslog header and Syslog message (the body of the message).

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 sum of the facility number multiplied by eight and severity. In this case, facility=4 (Auth) and severity=2 (Critical).
  - **Oct 11 22:14:15**: is the timestamp. It doesn't include the year, time-zone, and 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
RFC 5424

The new (2009) format (RFC 5424) of syslog is three parts - “Syslog Header”, “Structured Data”, and the actual log “message”.

- **Syslog Header.** Consists of priority, version, timestamp, hostname etc.
- **Structured Data.** This is 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.** This follows the two fields above (the Message field is free-form).

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

*Figure 2. Syslog message in RFC 5424 format*

- The dashes places for the PID, message ID, and other structured data.

```
<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*

### Syslog Message Formats

Zscaler supports many Syslog formats, includes many industry standards, and can incorporate custom log strings. This document focuses on the two primary standards used by SIEM vendors.

**Common Event Format (CEF)**

Common Event Format (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
```
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 like 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
```
Zscaler Logging Architecture Overview

Zscaler has two core products: Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA). Currently, 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 generates a corresponding log message. These logs messages are retained by Zscaler for six months (or longer through a paid-for service). Customers can view and search these logs using the Zscaler Admin dashboard.

Nanolog Stream Service (NSS)

Log messages are stored within Nanolog. When an organization deploys NSS for various log feeds, 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.

![Nanolog Stream Service (NSS) overview](image)

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 security information and event management (SIEM), and then streams the logs to your SIEM over a raw TCP connection.

Zscaler NSS is required for customers that want to send these logs to a SIEM (on premise or in-the-cloud). Think of NSS as an intermediate log gateway. NSS uses a virtual machine (VM) to stream traffic logs in real time from ZIA.

Although Syslog usually uses UDP and destination port 514, NSS only supports TCP. By using TCP NSS can detect if the SIEM becomes unavailable this by the loss of the TCP connection. In the event of a failure, NSS queues log messages until the SIEM returns (subject to storage).
ZIA Log Feeds

An NSS feed specifies the data from the logs that the NSS sends 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 eight 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>Zscaler 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>
Configuring ZIA for NSS

The following sections describe how to configure ZIA to work with NSS.

Logging into ZIA

First, setup the Zscaler side of this service. Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, please contact support.

![ZIA Admin Portal](image)

Figure 5. ZIA Admin Portal

Configuring Nanolog Streaming Service (NSS)

Log messages sent between Zscaler NSS and Azure data connector are not encrypted.

It’s strongly recommended that you spin up your NSS in same VNET as Azure data connector VM so that plaintext log messages traffic doesn’t leave your VNET.

If you are deploying NSS in a different network, you should use an external mechanism (e.g., IPSec tunnel) to encrypt plain text communication between NSS and Azure connector VM.
**Nanolog Streaming Service (NSS)**

After logging into ZIA, you need to add an **NSS server** and **NSS feed**. To navigate to the **Nanolog Streaming** section of ZIA, please follow: **Administration > Cloud Configuration > Nanolog Streaming Service**.

Follow instructions in the [NSS Deployment Guide help](https://admin.zcalerthree.net/#dashboard/1) (based on your deployment type) to set up web and firewall NSS.

![Figure 6. Navigate to NSS](https://admin.zcalerthree.net/#dashboard/1)
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 one hour to finish.

**Zscaler NSS Azure Resource Manager (ARM) Template** can be accessed at the [Zscaler GitHub repository](https://github.com/zscaler).

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

Connect to the NSS VM using SSH and execute following commands as root user. Change the IPs as needed to fit your environment.

```
[n@NSS /usr/home/zsroot]# nss configure
Detected an Azure VM!!
nameserver:168.63.129.16 (Options <c:change, d:delete, n:no change>) [n]
Do you wish to add a new nameserver? <n:no y:yes> [n]:
snet_dev (Service interface IP address with netmask) [192.168.100.4/24]: 192.168.100.5/24
snet_dflt_gw (Service interface default gateway IP address) [192.168.100.1]: 192.168.100.1
Successfully Applied Changes
[n@NSS /usr/home/zsroot]#
[n@NSS /usr/home/zsroot]# nss update-now
Connecting to server...
Connecting to update server 104.129.193.117.
Installed build version: 209302
Latest available build version: 209302
Build file is up-to-date

Checking if installation required...
Service is up-to-date.
[n@NSS /usr/home/zsroot]# nss restart
Detected an Azure VM!!
NSS service stopped
NSS service running with pid 3000
[n@NSS /usr/home/zsroot]# nss enable-autostart
Detected an Azure VM!!
Auto-start of NSS enabled
```
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 Zscaler Resources. If everything is as expected, you can move to the next section.

![Figure 7. Verify NSS server state](image)

Add NSS Feed

An NSS feed specifies what data from the logs that the NSS sends 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 8. Add NSS feed](image)
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 [Edit NSS Feed (Web)](#) for the details.

When configuring the log feed to Sentinel, add `"\" to the Feed Escape Character section.

Edit NSS Feed (Web)

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

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

©2022 Zscaler, Inc. All rights reserved. 16
**Edit NSS Feed (Firewall)**

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

```
%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} destinationTranslatedAddress=%s{sdip} deviceTranslatedPort=%d{ssport} 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=aggregated cs5=%s{threatcat} cs5Label=threatcat cs6=%s{threatname} cs6Label=threatname cn1=%d{durationms} cn1Label=durationms cn2=%d{numsessions} cn2Label=numsessions cs5Label=ipCat destinationTranslatedPort=%d{sdport} destinationTranslatedAddress=%s{sdip} sourceTranslatedPort=%d{ssport} sourceTranslatedAddress=%s{ssip} src=%s{csip} spt=%d{csport} dst=%s{cdip} dpt=%d{cdport} deviceTranslatedAddress=%s{ssip} destinationTranslatedAddress=%s{sdip} deviceTranslatedPort=%d{ssport} 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=aggregated cs5=%s{threatcat} cs5Label=threatcat cs6=%s{threatname} cs6Label=threatname cn1=%d{durationms} cn1Label=durationms cn2=%d{numsessions} cn2Label=numsessions cs5Label=ipCat cs5=%s{ipcat} destCountry=%s{destcountry} avgduration=%d{avgduration}\
```

**Edit NSS Feed (DNS)**

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

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-fw
CEF:0|Zscaler|NSSDNSlog|5.7|%s{action}|%s{rulelabel}|3| suser=%s{login} cs1=%s{dept} cs1Label=department cs2=%s{reqaction} cs2Label=reqaction cs3=%s{resaction} cs3Label=resaction cs4=%s{reqtype} cs4Label=dns_reqtype cs5=%s{req} cs5Label=dns_req cs6=%s{res} cs6Label=dns_resp cn1=%d{durationms} cn1Label=durationms cn1Label=durationms flexString1=%s{reqrulelabel} flexString1Label=reqrulelabel flexString2=%s{resrulelabel} flexString2Label=resrulelabel cat=%s{domcat} src=%s{cip} dst=%s{sip} dpt=%d{sport} spriv=%s{location} suid=%s{deviceowner} dvchost=%s{devicehostname}\
```

Activate your changes

The last step on the Zscaler side is to “activate” the configuration. All prior configurations to this point are candidate configurations. Once active, these changes become active in production.

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

![Activate your change](image)
Configuring Sentinel for Zscaler

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

Log into Azure Portal

Normally you would navigate to the Azure Login Portal and login using your account. To enable Private Preview of the Zscaler Data-Connector, visit the redirect to the Azure portal.

![Microsoft Azure Login Page](image)

Figure 11. Log into Azure Portal
Deploy the Data-Connector Host VM

The first step in Azure is deploying a Linux VM. This Linux VM is the Zscaler data-connector and runs Microsoft's Operations Management Suite (OMS) agent. The OMS agent is the software component that sends log messages to Azure Sentinel. There are more software components on this VM that enable this data pipeline, but you don’t need to worry about them as they are automatically configured by Azure.

After navigating to the Home screen click on Virtual Machine.

Figure 12. This VM is a Syslog server and run Azure's data connector
Create Virtual Machine

Your **Virtual machines** screen may have additional information displayed if you have existing virtual machines. Navigate to **Create Virtual Machine**.

Figure 13. Create virtual machine
Bind this VM to a Resource Group

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

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

Figure 14. Initiate VM deployment

Fill in the pertinent details, click **Review + create**, and follow subsequent prompt to finish VM creation. Once the deployment is complete, proceed to the next step.
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 and the OMS. By default, these ports are not permitted in Azure and we must manually allow inbound connections to tcp/22 and tcp/514. This access should be locked down to only permitted 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 15. Network Security Groups

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

Figure 16. Network Security Groups, continued
Next, select the **Inbound Security Rules** option. This allows you 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 or management station

Please review to the following sections to see how to exactly configure each rule separately.
Add Inbound Security Rule for syslog

You should 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.

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.

Figure 18. Add inbound security rule for NSS
Add Inbound Security Rule for SSH

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

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.

Figure 19. Add inbound security rule for SSH
Create and Configure Sentinel Instance

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

![Navigate to Azure Sentinel](image)

Create Log Analytics Workspace

First, 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.

![Create new workspace](image)
Name, Add, and Link a Resource Group to Workspace

This document presumes the following steps are performed in a new, non-production environment. In this guide, we reuse the resource group created in Bind this VM to a Resource Group. If you are configuring this in an existing and production environment, your steps might 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]

*Figure 22. Name, add, and link resource group to workspace*
Add Workspace to Azure Sentinel

Next, click Add Azure Sentinel. You need to wait until the deployment finishes before moving to next section. This should take a few minutes.

Figure 23. Add workspace to Azure Sentinel
Configure Data Collection

You need to configure data collection. To do so, navigate to **News & guides > Collect data**.

**Azure Sentinel**

*A cloud-native SIEM to help you focus on what matters most*

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

1. **Collect data**
   - Collect data at cloud scale across the enterprise, both on-premises and in multiple clouds

2. **Create security alerts**
   - Focus on what’s important using analytics to create alerts

*Figure 24. Configure Zscaler data connector*
Search for Zscaler Connector

In the search box, type in “Zscaler”. Next select the Zscaler connector, and then click Open connector page.

![Zscaler connector search results](image)

*Figure 25. Search for Zscaler connector*
Configure Syslog Agent

Clicking **Open connector page** displays following screen. Instructions on this page consists of:

1. Selecting a Linux machine (in any cloud or on prem) that acts as a proxy between your security solution and Sentinel. We use VM setup previously.

2. Installing Azure monitoring agent (CEF connector) on this Linux box

![](image)

**Figure 26. Steps to configure logging pipeline**
3. Log into the VM setup using SSH and run the command highlighted below from CLI.

![Log into the VM setup 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.

2. 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.

3. 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.

![Command to configure logging agent](image)

```bash
sudo wget https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataCollector
```

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 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:

   ![Validate collector agent installation](image)
You should see output “Installation completed” and the netstat output should show that the syslog server and Azure collector agent (Ruby scripts) are running.

If you run into issues, run the following command.

<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 and apply the CEF collector:</td>
<td></td>
</tr>
<tr>
<td><code>sudo wget https://raw.githubusercontent.com/Azure/Azure-Sentinel/main/DataCen...</code></td>
<td></td>
</tr>
<tr>
<td>2. Forward Common Event Format (CEF) logs to Syslog agent</td>
<td></td>
</tr>
<tr>
<td>Set Zscaler probot 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:</td>
<td></td>
</tr>
<tr>
<td><code>sudo wget https://raw.githubusercontent.com/Azure/Azure-Sentinel/main/DataCen...</code></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 29. Troubleshoot collector agent installation*
Pick a Zscaler Workbook

1. Navigate to Dashboard > Azure Sentinel Workspaces > Workbooks and search for “zscaler”.
2. Select the workbook that you are interested in and click View template.
3. You can also save the workbook to a geographic location and revisit it later.

Explore Zscaler Workbook

Workbooks are responsive and you can click around to drill down based on different criterions.

You can filter by selecting options towards top of the page or by clicking on individual entries.
Appendix A: Requesting Zscaler Support

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

Gather Support Information

To contact Zscaler support, select Administration > Settings > Company profile.

![Figure 32. Collecting details to open support case with Zscaler TAC](image)

Save Company ID

Copy your Company ID.

![Figure 33. Company ID](image)
Enter Support Section

With your company ID information, you can open a support ticket. Navigate to Dashboard > Support > Submit a Ticket.

![Support Section Diagram](image)

Figure 34. Submit a ticket