Vectra ZPA Integration Guide

Jan 20, 2021

zscaler™

About ZPA and Vectra's Existing Support of ZIA

The Zscaler Private Access (ZPA) service enables organizations to provide access to internal applications and services while ensuring the security of their networks. Unlike VPNs, which require users to connect to your network to access your enterprise applications, ZPA allows you to give users policy-based secure access only to the internal apps they need to get their work done. With ZPA, application access does not require network access. ZPA decouples applications from the physical network so you can provide seamless connectivity to private internal applications and assets whether they are in the cloud, the data center, or both. It also adjusts dynamically to network changes, so you can move your resources without impacting user access.

Vectra's support of ZPA is a key component of Vectra's ZTNA (Zero Trust Network Access) strategy. For additional guidance related to Vectra and ZTNA, here are some articles on Vectra's public website:

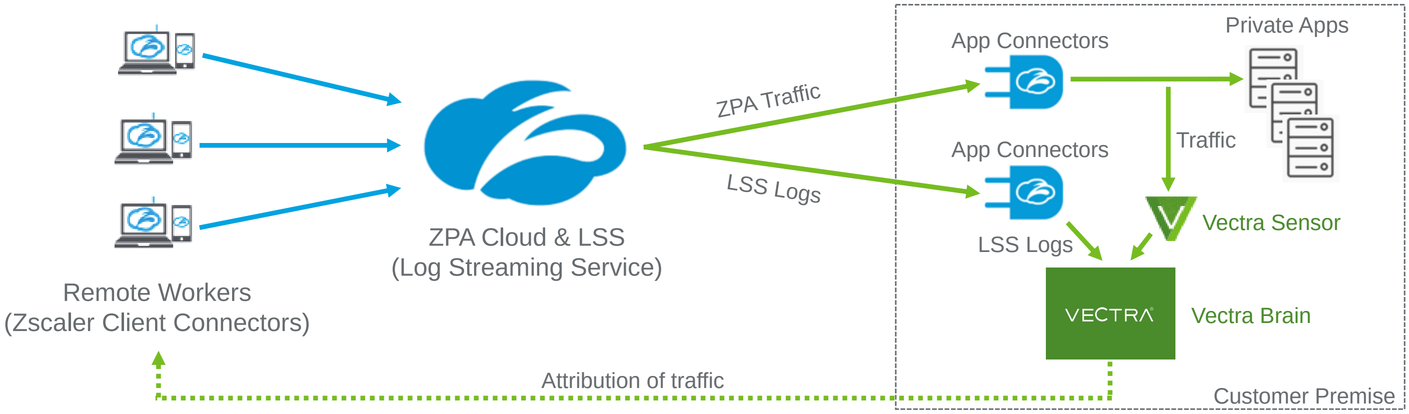
- Why NDR is a Required Component of NIST Zero Trust Architecture
- Why the NIST Zero Trust Architecture No Longer Requires Decryption

While ZPA is for connecting users to an enterprise's internal applications, Zscaler Internet Access (ZIA) is for connecting users to public applications on the internet. ZIA is already supported by Vectra. Vectra is proxy aware and treats all traffic to ZIA as in to out. Vectra has a support article that provides configuration advice to help avoid spurious Detections related to ZIA proxies.

Document Purpose and Use

This integration guide provides an overview of Vectra Cognito integration for customers who have deployed Zscaler Private Access (ZPA). It includes the instructions necessary to onboard the ZPA logs into Cognito.

Solution – Key Components



As shown in the conceptual design above, Vectra attribution to behaviors undertaken by remote workers are the byproduct of observations of traffic via Vectra Sensors and ZPA logs generated by the Log Streaming Service (LSS). These logs are sourced preferably from a dedicated App Connector group used only for LSS, contain data related to the activities brokered through your App Connectors that are used for ZPA traffic, and when forwarded to the Cognito Brain, form the basis of this integration. The Cognito Brain serves as an Enterprise Log Receiver in ZPA parlance.

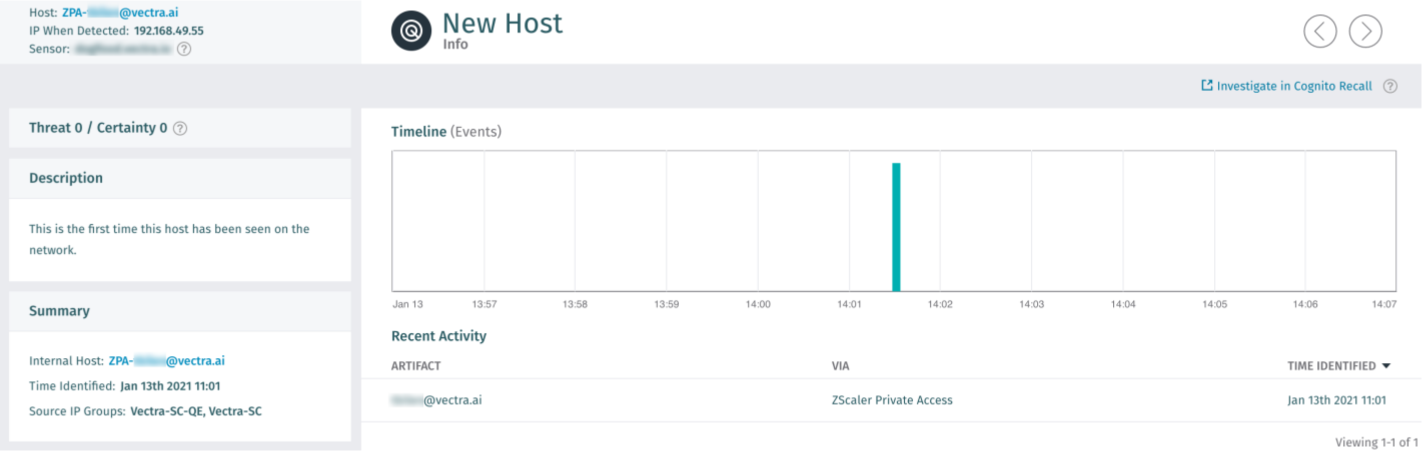
Architecture and Performance Guidance

- Vectra recommends a dedicated App Connector group for log forwarding
  - This will separate data plane (ZPA network) and log forwarding traffic from each other and prevent any potential service degradation that could affect access to ZPA apps within a customer environment
  - Using an App Connector Group will also distribute LSS load and provide for some redundancy
  - **Note this is not a requirement but it is highly recommended**
- Vectra can process approximately 3000 LSS log events per second in a Brain
- **Vectra requires TCP transport over port 4639 in JSON format without encryption**
- If a customer is using an intermediary host, such as a SIEM or Central Log Management server, to collect the LSS logs and then forward them to the Vectra Brain, Vectra requires the logs to be in the same format as if there were no intermediary.
- Network traffic in between the App Connectors and the customer's private apps is required to be captured with Vectra Sensors
  - Please work with your SE and/or installation team to help ensure the proper traffic is captured
- It is recommended to position the App Connectors that are used to broker LSS traffic to the Vectra Brain in the same network location or subnet that the Vectra Brain is located in
  - This will help to reduce latency
  - This will possibly eliminate the need to open up firewall rules to allow the App Connector to speak to the Vectra Brain
  - This will also help to alleviate any concerns with the App Connector to Brain traffic being in the clear

Attribution of Traffic to ZPA Users

Vectra Cognito Sensors (virtual or physical) capture network traffic as normal in customer environments. The Sensors will then forward the metadata to the Cognito Brain for analysis. The Brain will attribute traffic that is observed coming from the App Connectors used for private app access into Host containers that are attributed to the ZPA user based on the ZPA LSS log information received.

Below is an example of a New Host Detection on one of Vectra's internal servers. The username and Sensor name have been blurred out, but you can see the naming convention for ZPA hosts should be ZPA-username@domain.tld. All Vectra Detections will function normally.



Host: ZPA-[redacted]@vectra.ai
IP When Detected: 192.168.49.55
Sensor: [redacted]

Threat 0 / Certainty 0

Description

This is the first time this host has been seen on the network.

Summary

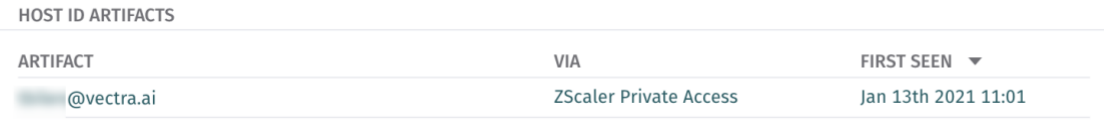
Internal Host: ZPA-[redacted]@vectra.ai
Time Identified: Jan 13th 2021 11:01
Source IP Groups: Vectra-SC-QE, Vectra-SC

Recent Activity

ARTIFACT	VIA	TIME IDENTIFIED ▼
[redacted]@vectra.ai	ZScaler Private Access	Jan 13th 2021 11:01

Viewing 1-1 of 1

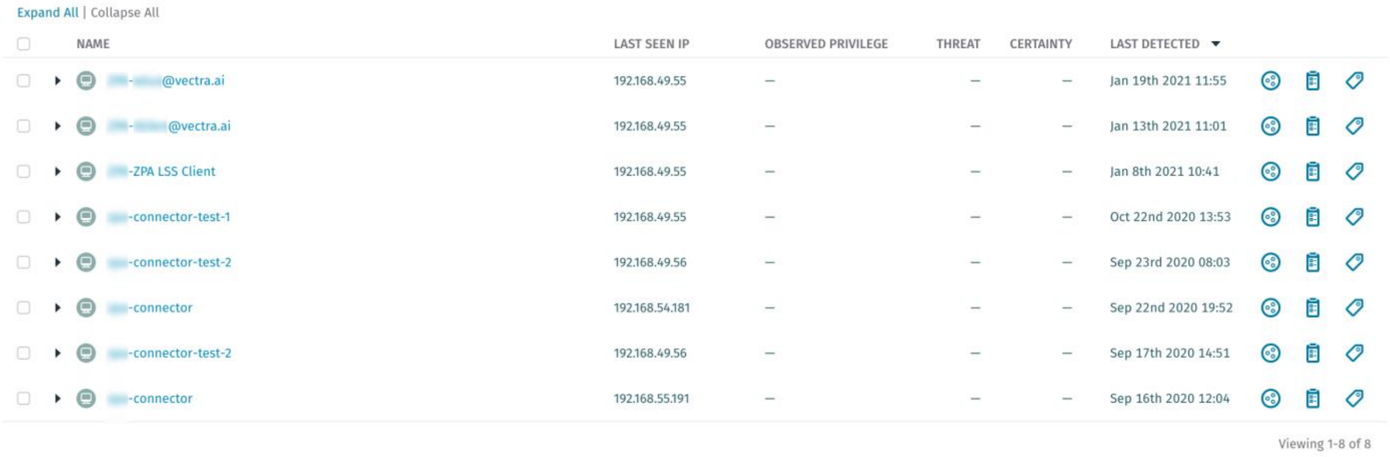
Drilling into the ZPA-Host in the “Details section” you can see the Host ID Artifacts including “First Seen” attribute:



HOST ID ARTIFACTS

ARTIFACT	VIA	FIRST SEEN ▼
[redacted]@vectra.ai	ZScaler Private Access	Jan 13th 2021 11:01

Doing a simple search on the Hosts page for “zpa” with a status of “all” will show identified ZPA hosts with or without an active Threat/Certainty score:



Expand All | Collapse All

□	NAME	LAST SEEN IP	OBSERVED PRIVILEGE	THREAT	CERTAINTY	LAST DETECTED ▼
□	[redacted]-[redacted]@vectra.ai	192.168.49.55	–	–	–	Jan 19th 2021 11:55
□	[redacted]-[redacted]@vectra.ai	192.168.49.55	–	–	–	Jan 13th 2021 11:01
□	[redacted]-ZPA LSS Client	192.168.49.55	–	–	–	Jan 8th 2021 10:41
□	[redacted]-connector-test-1	192.168.49.55	–	–	–	Oct 22nd 2020 13:53
□	[redacted]-connector-test-2	192.168.49.56	–	–	–	Sep 23rd 2020 08:03
□	[redacted]-connector	192.168.54.181	–	–	–	Sep 22nd 2020 19:52
□	[redacted]-connector-test-2	192.168.49.56	–	–	–	Sep 17th 2020 14:51
□	[redacted]-connector	192.168.55.191	–	–	–	Sep 16th 2020 12:04

Viewing 1-8 of 8

Log Format Example

“User Activity” is the ZPA LSS log that Vectra requires for the integration. The full user activity log contains many more pieces of information than shown below. The below represents the data that Vectra requires for the integration. The additional fields can be filtered out at the source if desired. Vectra Cognito Detect will ignore the additional data if it is present in the log stream. There is no Vectra requirement to pre-filter the log at the source.

```
{
"IPProtocol": 6,
"TimestampConnectionStart": "2020-09-22T19:45:13.201Z",
"ConnectionStatus": "active",
"TimestampConnectionEnd": "",
"LogTimestamp": "Wed Sep 23 00:00:14 2020",
"Username": "user@domain.tld",
"ServerIP": "192.168.55.136",
"ServerPort": 22,
"ConnectorIP": "192.168.49.55",
"ConnectorPort": 40692,
"SessionID": "af7EqwAggd74neI+1PGP",
}
```

ZPA LSS Configuration Instructions

Prerequisites

- Administrative access to the ZPA Administrative Console

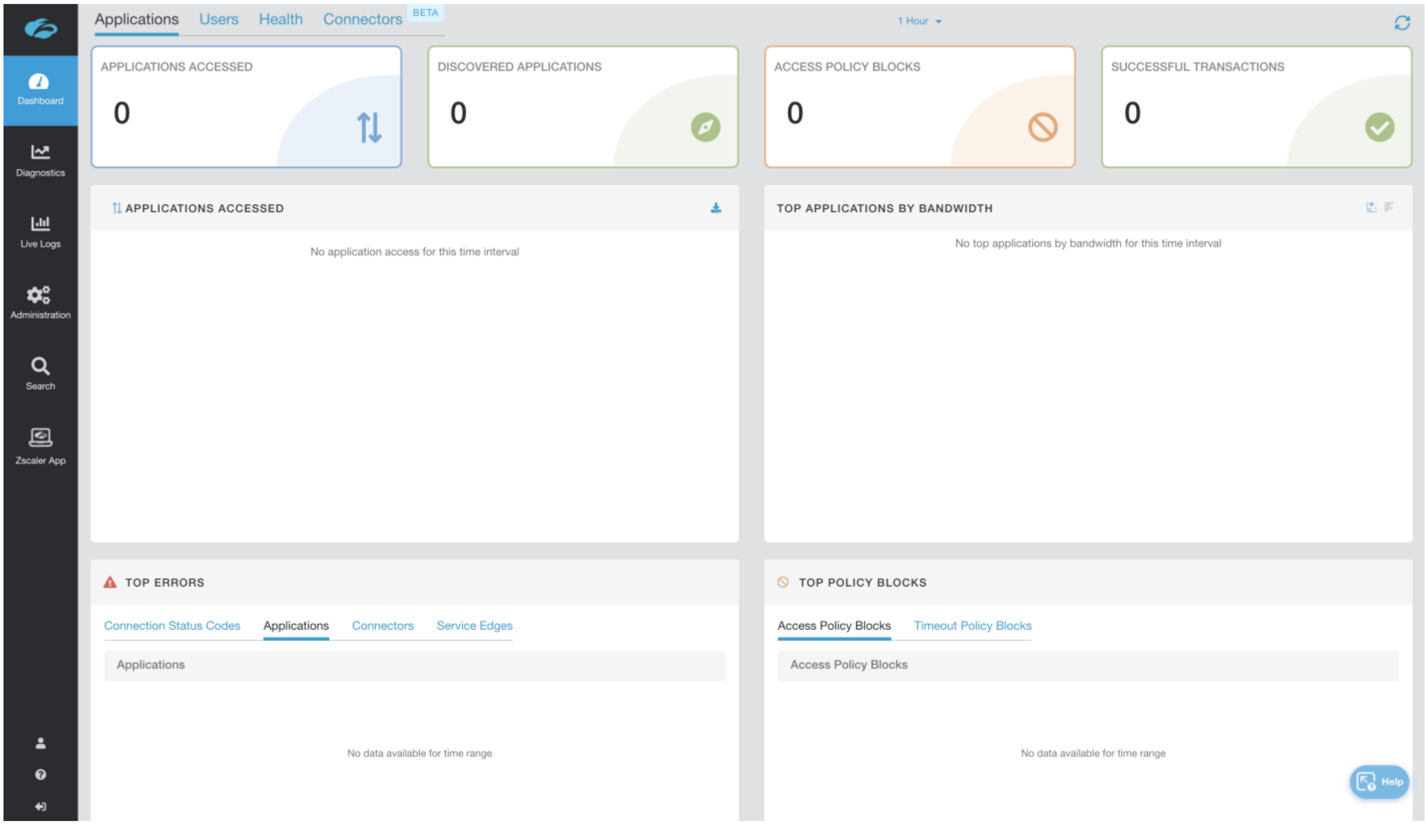
Supporting Material

Official Zscaler ZPA support documentation may be useful to reference while making these configurations:

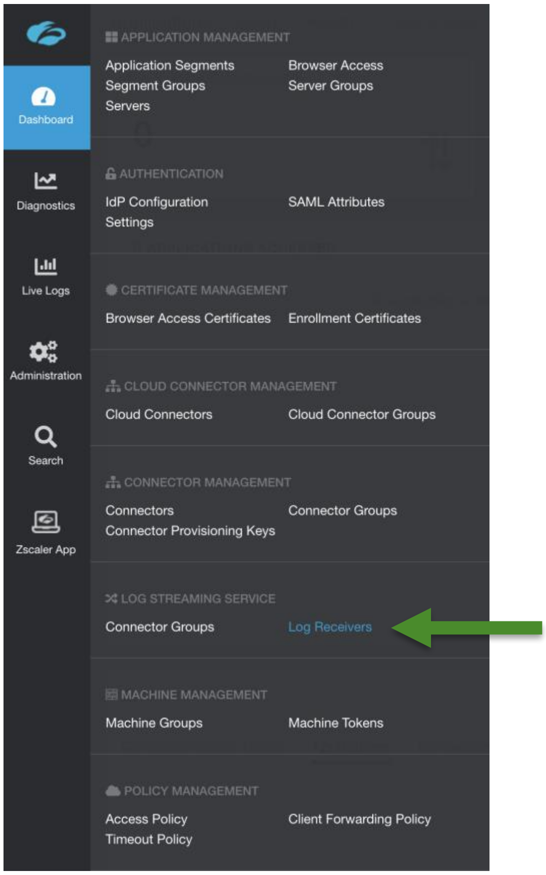
- https://help.zscaler.com/zpa/log-streaming-service

Configuration Instructions (Zscaler LSS)

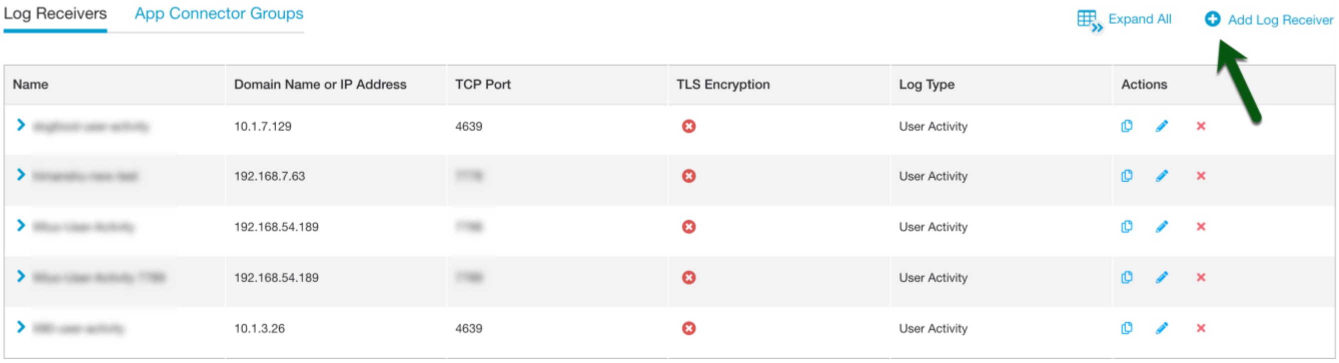
1. Log in to the Zscaler management portal



2. Go to **Administration > Log Receivers**



3. Click **Add Log Receiver** - The **Add Log Receiver** window appears



Name	Domain Name or IP Address	TCP Port	TLS Encryption	Log Type	Actions
› [redacted]	10.1.7.129	4639	⊗	User Activity	⧉ ✎ ×
› [redacted]	192.168.7.63	[redacted]	⊗	User Activity	⧉ ✎ ×
› [redacted]	192.168.54.189	[redacted]	⊗	User Activity	⧉ ✎ ×
› [redacted]	192.168.54.189	[redacted]	⊗	User Activity	⧉ ✎ ×
› [redacted]	10.1.3.26	4639	⊗	User Activity	⧉ ✎ ×

4. In the **Add Log Receiver** window, configure the following tabs:

   a. Log Receiver

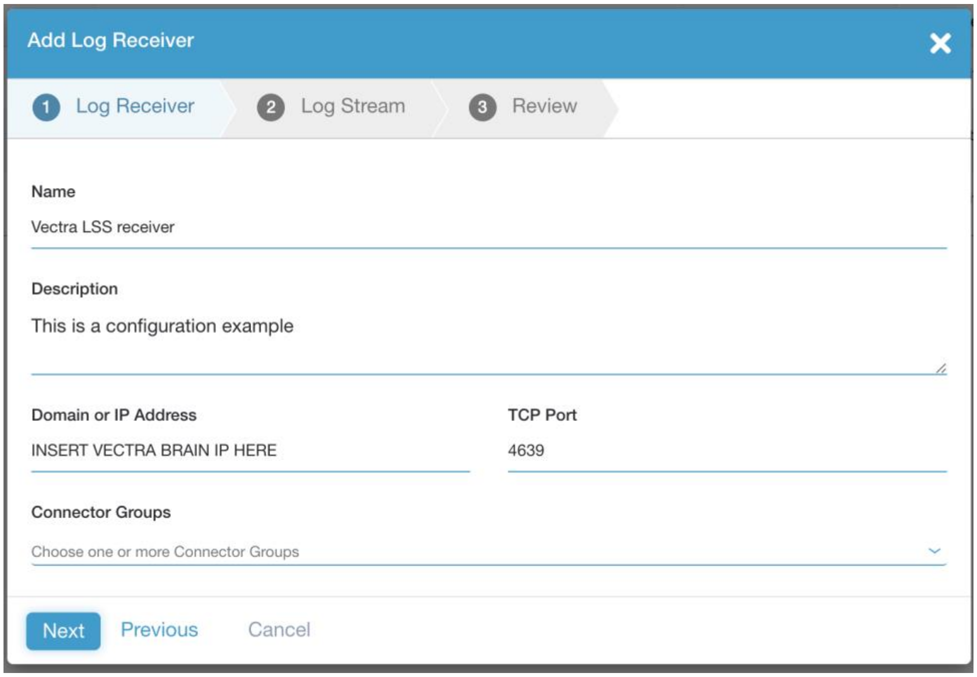
      i. Name - Provide a name for this receiver. For Example: “Vectra LSS Receiver”

      ii. Domain/IP - Provide the management IP address or hostname of the Cognito Brain

      iii. TCP Port - 4639 **Note: This port is not configurable today**

      iv. Ensure the TLS Encryption is “Disabled”

      v. Connector Groups - Select a connector group to act as the log forwarder that can reach the Brain’s IP or hostname



Name
Vectra LSS receiver

Description
This is a configuration example

Domain or IP Address
INSERT VECTRA BRAIN IP HERE

TCP Port
4639

Connector Groups
Choose one or more Connector Groups

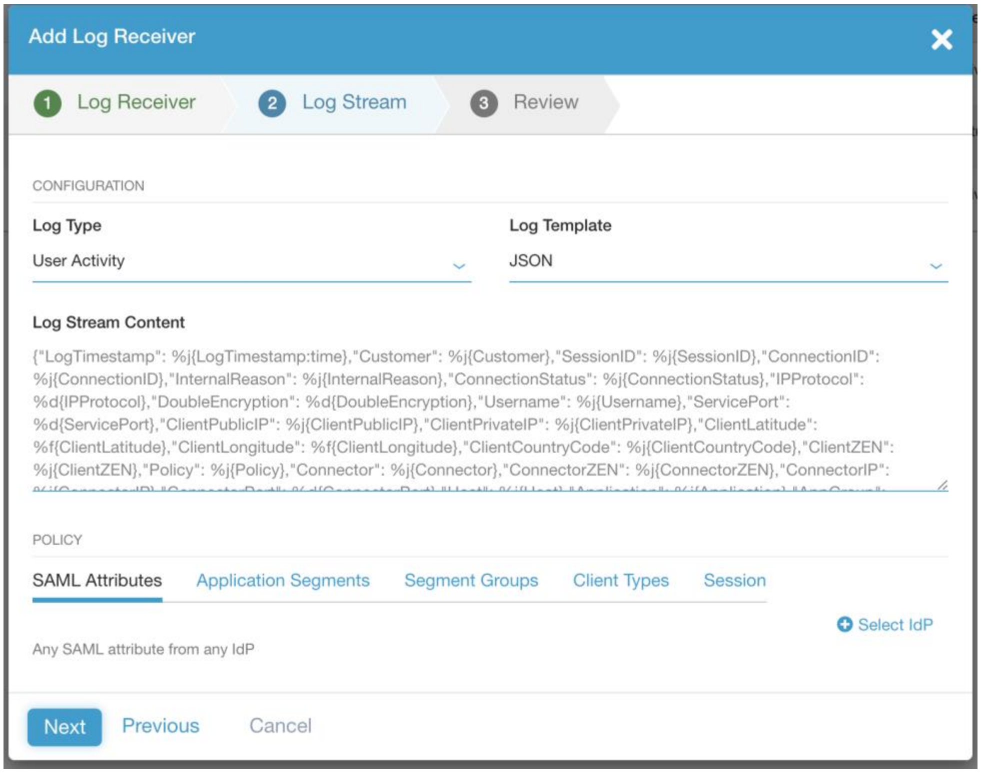
   a. Log Stream - For additional information regarding limiting fields sent see this link. Essentially you can just modify the Log Stream Content section to remove fields that you do not want forwarded to Cognito Detect while leaving the required fields listed earlier in this document. You do not need to do this step. It is optional as Cognito Detect will ignore the extra fields.

      vi. Log Type - Select “User Activity”

      vii. Log Template - Select “JSON”

      viii. Log Stream Content - Leave as Default or modify as required per the above guidance

      ix. Policy - Leave as default unless you would like to add any specific restrictions on the logs



CONFIGURATION

Log Type: User Activity

Log Template: JSON

Log Stream Content

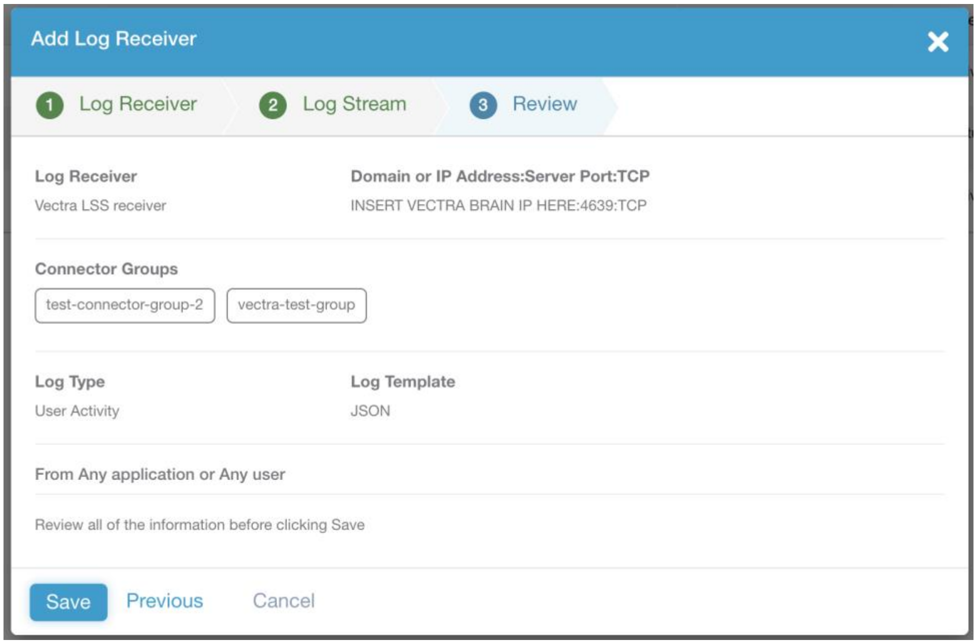
```
{"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"SessionID": %j{SessionID},"ConnectionID":
%j{ConnectionID},"InternalReason": %j{InternalReason},"ConnectionStatus": %j{ConnectionStatus},"IPProtocol":
%d{IPProtocol},"DoubleEncryption": %d{DoubleEncryption},"Username": %j{Username},"ServicePort":
%d{ServicePort},"ClientPublicIP": %j{ClientPublicIP},"ClientPrivateIP": %j{ClientPrivateIP},"ClientLatitude":
%f{ClientLatitude},"ClientLongitude": %f{ClientLongitude},"ClientCountryCode": %j{ClientCountryCode},"ClientZEN":
%j{ClientZEN},"Policy": %j{Policy},"Connector": %j{Connector},"ConnectorZEN": %j{ConnectorZEN},"ConnectorIP":
```

POLICY

Any SAML attribute from any IdP

b. Review

x. Click next, and if all looks good click **Save**



Log Receiver: Vectra LSS receiver

Domain or IP Address:Server Port:TCP: INSERT VECTRA BRAIN IP HERE:4639:TCP

Connector Groups: test-connector-group-2, vectra-test-group

Log Type: User Activity

Log Template: JSON

From Any application or Any user

Review all of the information before clicking Save

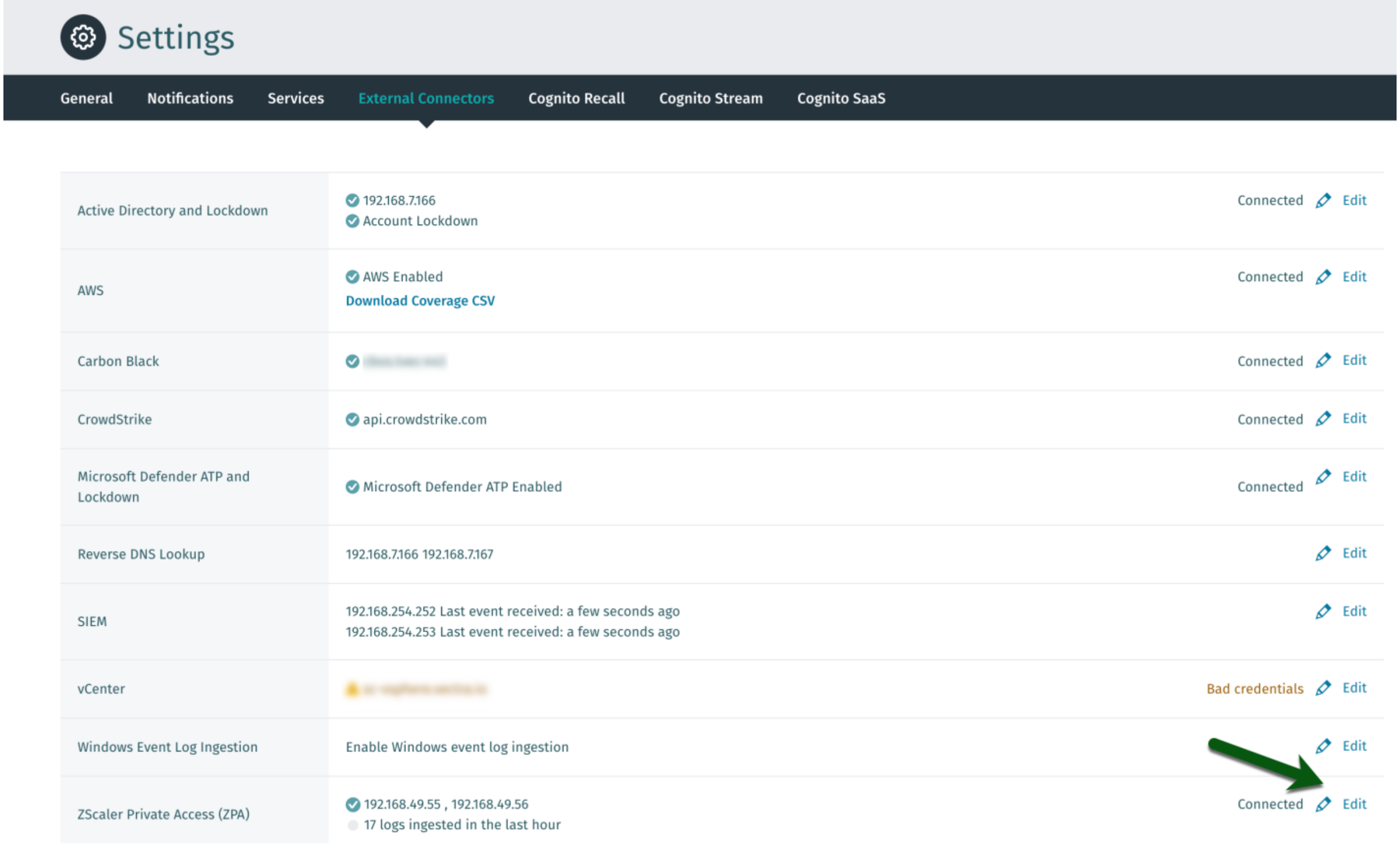
Vectra ZPA Integration Configuration Instructions

Prerequisites

- Detect Brain account with Role permissions including “View” and “Edit” for “Settings - Zscaler Private Access”

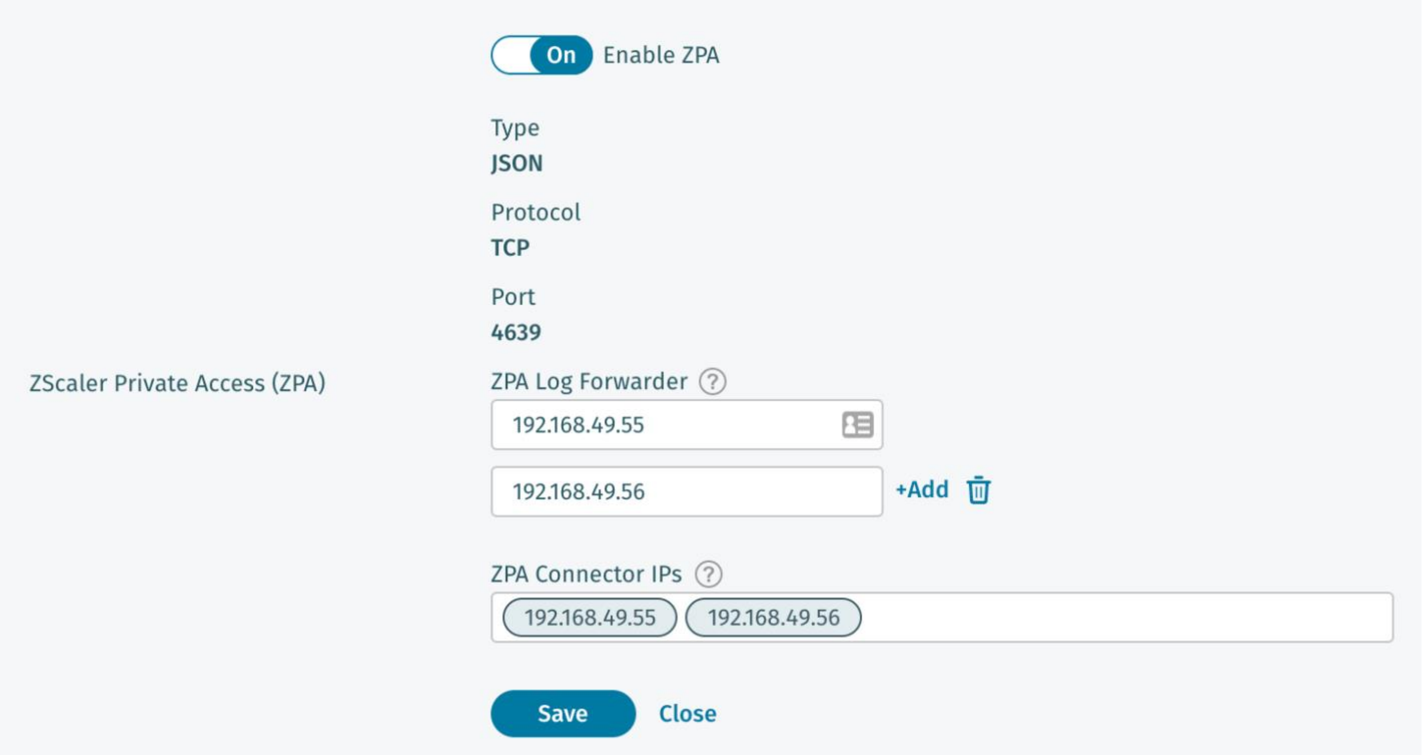
Configuration Instructions (Vectra Cognito Brain)

1. After logging in to the Cognito Detect, navigate to **Settings > External Connectors > Zscaler Private Access (ZPA)** and click the “Edit” or pencil icon.



Active Directory and Lockdown	✓ 192.168.7.166 ✓ Account Lockdown	Connected	Edit
AWS	✓ AWS Enabled Download Coverage CSV	Connected	Edit
Carbon Black	✓ [redacted]	Connected	Edit
CrowdStrike	✓ api.crowdstrike.com	Connected	Edit
Microsoft Defender ATP and Lockdown	✓ Microsoft Defender ATP Enabled	Connected	Edit
Reverse DNS Lookup	192.168.7.166 192.168.7.167		Edit
SIEM	192.168.254.252 Last event received: a few seconds ago 192.168.254.253 Last event received: a few seconds ago		Edit
vCenter	[redacted]	Bad credentials	Edit
Windows Event Log Ingestion	Enable Windows event log ingestion		Edit
ZScaler Private Access (ZPA)	✓ 192.168.49.55 , 192.168.49.56 17 logs ingested in the last hour	Connected	Edit

2. Configure the Cognito Detect ZPA settings as directed below. An example screenshot follows.
   a. Ensure the feature is enabled at the top
   b. Enter the IPs that your Brain will be receiving LSS logs from the in “ZPA Log Forwarder “area. These will be the IPs of the App Connectors that you have selected in the ZPA admin console. Use the “+Add” button to add additional Log Forwarder IPs as required.
   c. Enter the IPs of the App Connectors that you use for ZPA traffic in your environment in the “ZPA Connector IPs” area.
   d. Click **Save** when done



ZScaler Private Access (ZPA)

On Enable ZPA

Type
JSON

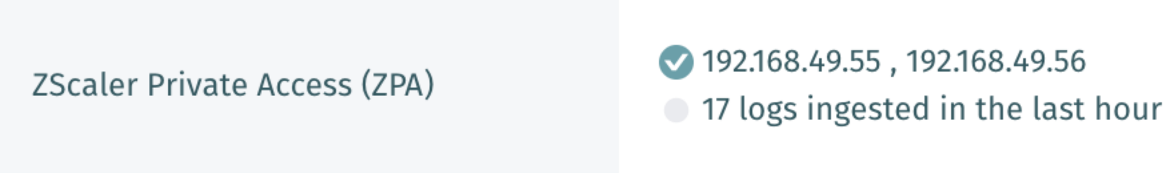
Protocol
TCP

Port
4639

ZPA Log Forwarder
192.168.49.55
192.168.49.56

ZPA Connector IPs
192.168.49.55 192.168.49.56

3. Once you have saved you will return to the **External Connectors** screen where you can see the status of the ZPA integration. An example screenshot is below. Please note the following:
   a. Log counts shown are an average, so it is possible to see non whole numbers
   b. It can take up to 10 min for numbers to change as this data is polled
   c. A Green checkmark means that logs are coming in, in the proper format
   d. Some reasons why the integration may fail include
      i. Log format is incorrect - Not JSON, intermediary has altered them in some way, etc
      ii. Inability of the App Connector used for LSS to reach the Brain which may be firewall related
      iii. Not sending all the required logs as specified earlier in the document
      iv. Sending more logs than the Brain can process, resulting in some logs being dropped



ZScaler Private Access (ZPA)

✓ 192.168.49.55 , 192.168.49.56
○ 17 logs ingested in the last hour