Darktrace Zscaler ZIA & ZPA Integration Guide

Threat Visualizer v5.1

Last update: August 4, 2021

Darktrace and Zscaler ZIA

The Darktrace Zscaler ZIA integration ingests weblogs from a ZIA device to simulate connection data. Web events produced by the Zscaler logging will be associated with a device of the same hostname. If a device of that hostname does not already exist, Darktrace will create a new device. Connection events created from Zscaler logs will be available to core Darktrace analysis and accessible in Advanced Search.

Devices which have ZIA simulated connectivity associated will be automatically tagged with the ZIA tag.

Requirements

- A Darktrace Appliance running v4.1 or above and optionally a Darktrace vSensor or hardware probe configured to receive logs.
- A Zscaler ZIA instance with Collect Device Owner Information and Collect Machine Hostname Information enabled.
- A configured Nanolog Streaming Service (Zscaler NSS subscription required) setup with a local NSS server able to contact a Darktrace Master or Probe (Hardware or Virtualized) over the required port (1514).
- Access to the Zscaler administration portal to configure NSS feeds.

Considerations

- Packet data is not available for connections constructed from Zscaler ZIA logs.
- Connections are only created for protocols included in the ZIA logs and are limited by the data provided within the log.

  Due to the lack of source port information in ZIA logs, simulated connections are assigned to port 18000.

Deploying the ZIA Integration

Darktrace Configuration

1. Access the Darktrace master intended to receive the Zscaler logs. Within the Threat Visualizer, navigate to the **System Config** page in the main menu under **Admin**.

   Select **Modules** from the left-hand menu.

2. Locate the **Telemetry** subsection, select **"Zscaler ZIA"** from the available options.

   A new dialog will open. Ensure the module is **enabled**.

3. Click the **"Details"** button to display the log output format. Record this securely as it is required for configuration later.

4. Returning to the **Modules** page, locate the **Telemetry** subsection. Click the ⚙ **Config** button. A new dialog will open.

5. Select the appliance or probe that logs are being sent to. In the field **Log Input Allowed IPs**, enter the IP address of the Zscaler device sending the logs.

   Save the changes.

Zscaler Configuration

1. Access the ZIA console as a user with permission to configure NSS feeds.

2. Navigate to **Administration** > **Nanolog Stream Service** and select NSS feeds from the available table. Click "**+ Add NSS Feed**"

3. Provide a descriptive name for the feed and ensure it is **Enabled**.

4. Select the NSS Server located locally to the master appliance or vSensor. Enter the IP of the master appliance or vSensor/hardware probe intended to receive the logs.

5. Set the **Destination Type** and enter the **TCP Port** as **1514**.

6. Ensure the **SIEM Rate** is unlimited and the **Log Type** is set to **Web Log**.

7. Set **Feed Output Type** to "Custom" and paste the output format retrieved from the Darktrace Threat Visualizer config page into the **Feed Output Format** field.

8. Save the changes.

ZIA logs should now be received by the master or probe and begin to populate connection and hostname data within the Threat Visualizer.

Darktrace and Zscaler ZPA

In Zscaler Private Access environments, remote users initiate connections to internal resources through a ZPA App Connector located locally in an organizations private network. Darktrace observes connectivity from the ZPA App Connector to these internal resources, but is unable to resolve these connections back to a specific end user or IP address.

The Darktrace Zscaler ZPA integration ingests “User Activity” logs produced by ZPA, allowing connectivity patterns seen in network traffic to be matched back to originating remote users. Devices which have connectivity mapped through ZPA ingestion will be automatically tagged with the ZPA tag.

Requirements

- A Darktrace Appliance running v4.1 or above and optionally a Darktrace vSensor or hardware probe configured to receive logs.
- A ZPA environment with a configured Log Streaming Service setup, and an App Connector able to contact a Darktrace Master or Probe (Hardware or Virtualized) over the required port.

  Darktrace master instances and probes accept UDP and TCP log input on port 1514 plain text and TLS encrypted TCP on port 6514. The appropriate port and transfer protocol will depend on the configuration of your ZScaler environment and the output supported by the vendor.
- Access to the Zscaler administration portal to configure LSS feeds.

Considerations

• Zscaler does not guarantee log data will be transmitted if connectivity is lost between ZPA and the local App Connectors. When connectivity is restored, up to 15 minutes of lost log data may be re-transmitted, but this is also not guaranteed.

Deploying the ZPA Integration

Darktrace Configuration

1. Access the Darktrace master intended to receive the Zscaler logs. Within the Threat Visualizer, navigate to the **System Config** page in the main menu under **Admin**.

   Select **Modules** from the left-hand menu.

2. Locate the **Telemetry** subsection, select **"Zscaler ZPA"** from the available options.

   A new dialog will open. Ensure the module is **enabled**.

3. Click the **"Details"** button to display the log output format. Record this securely as it is required for configuration later.

4. Returning to the **Modules** page, locate the **Telemetry** subsection. Click the ⚙ **Config** button. A new dialog will open.

5. Select the appliance or probe that logs are being sent to. In the field **Log Input Allowed IPs**, enter the IP address of the Zscaler device sending the logs.

   Save the changes.

Zscaler Configuration

1. Access the Zscaler console as a user with permission to configure LSS feeds.

2. Navigate to **Administration** > **Log Receivers** and select **Log Receivers** from the available table. Click "**+ Add Log Receiver**"

3. In the **Log Receiver** tab, provide a descriptive name and description for the log feed.

4. Enter the IP of the master appliance or vSensor/hardware probe intended to receive the logs.

5. Enter the **TCP Port** and select whether TLS encryption is desired.

   Darktrace master instances and probes accept UDP and TCP log input on port 1514 plain text and TLS encrypted TCP on port 6514. The appropriate port and transfer protocol will depend on the configuration of your ZScaler environment and the output formats supported by the vendor.

6. Select the **Application Connector group** located locally to the master appliance or vSensor that is able to send logs.

7. Click **Next** to progress to the **Log Stream** tab. Here, set the **Log Type** to **User Activity**.

8. Set the **Log Template** to **JSON**, then paste the output format retrieved from the Darktrace Threat Visualizer config page into the **Log Stream Content** field.

9. Optionally restrict the logs sent to Darktrace in the **Policy** section, then click **Next** to proceed.

10. In the **Review** tab, confirm the settings and **Save** the new receiver.

ZPA logs should now be received by the master or probe and begin to populate within the Threat Visualizer.

US:+1 415 229 9100 UK:+44 (0) 1223 394 100 LATAM:+55 11 4949 7696 APAC:+65 6804 5010 info@darktrace.com darktrace.com