

Slide 1 - Zscaler Private Access



Zscaler Private Access

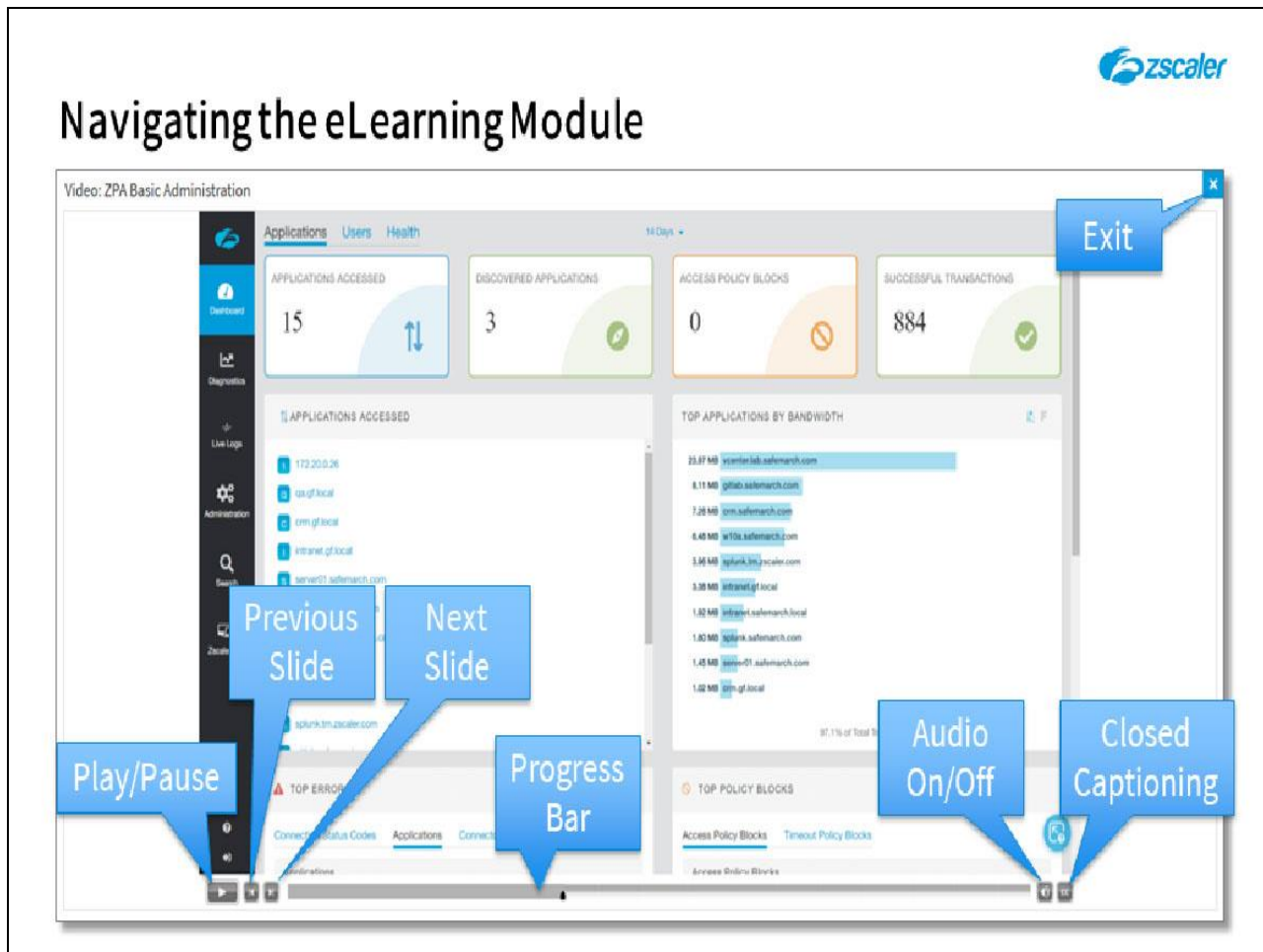
Health Monitoring and Logging Overview

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on ZPA Health monitoring and Logging.

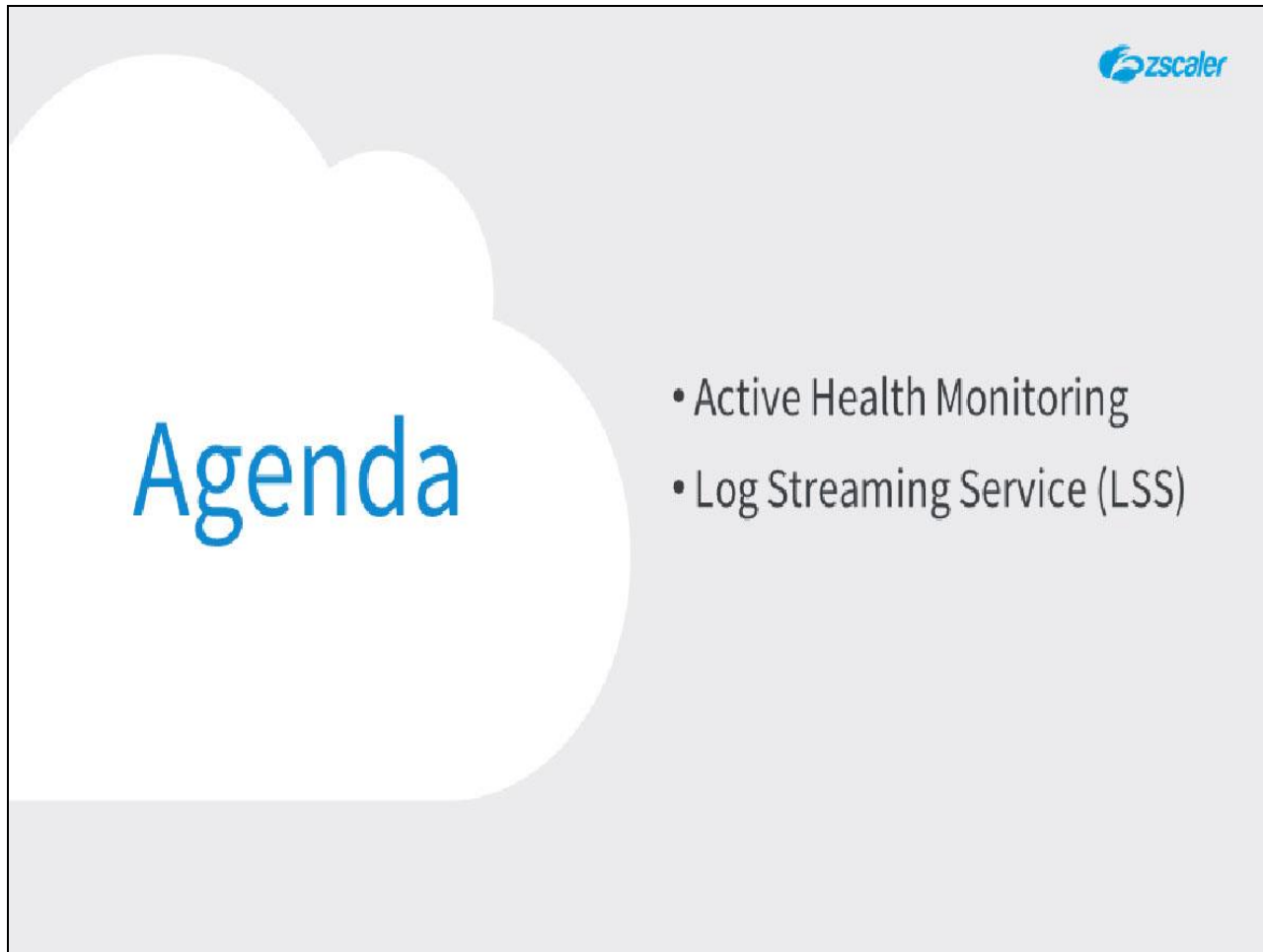
Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play** and **Pause**, **Previous** and **Next** slide. You can also **Mute** the audio or enable **Closed Captioning** which will cause a transcript of the module to be displayed on the screen. Finally, you can click the **X** button at the top to exit.

Slide 3 - Agenda



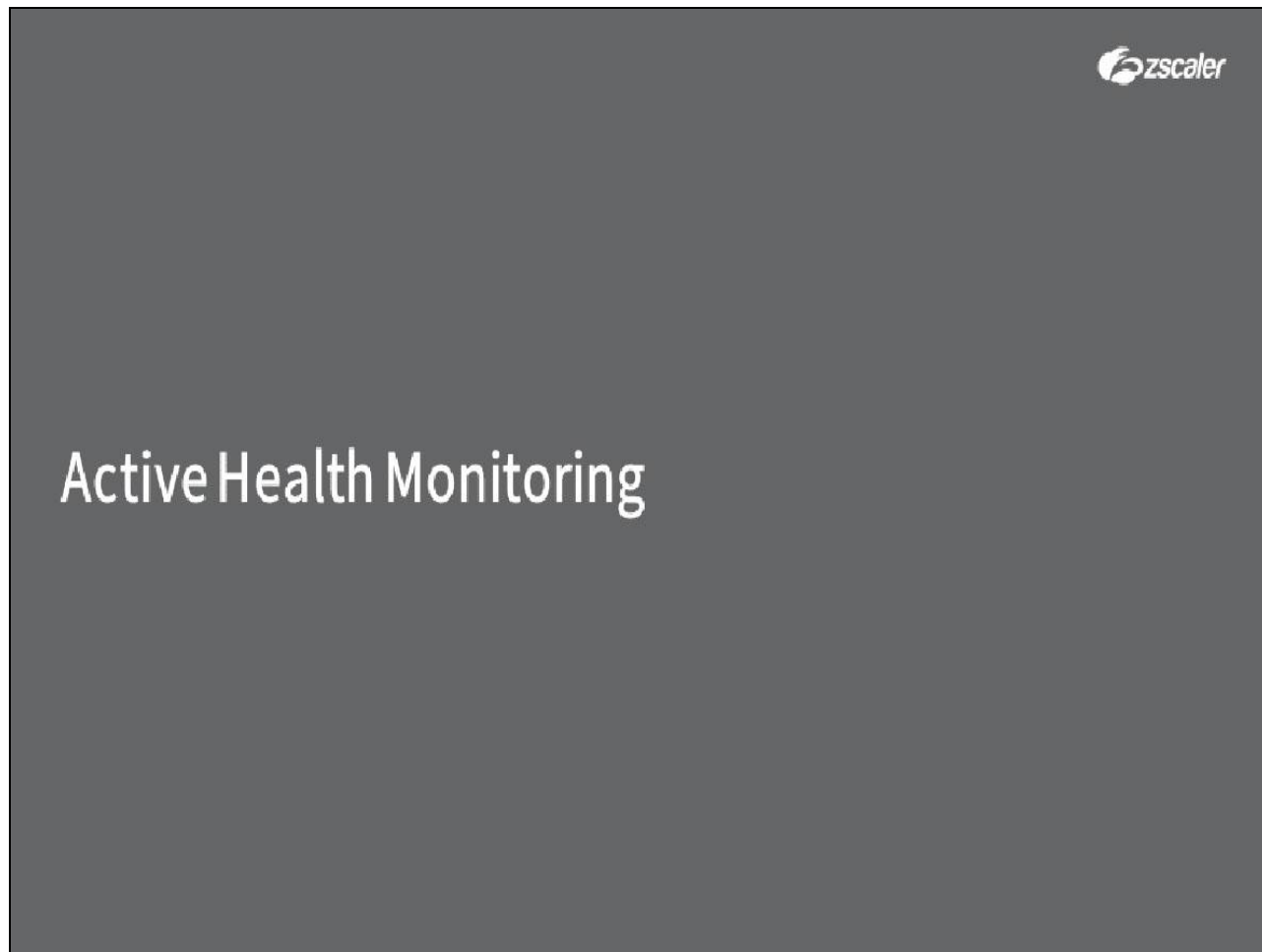
Agenda

- Active Health Monitoring
- Log Streaming Service (LSS)

Slide notes

In this module we will we will look at the active health monitoring capability of the ZPA service and at an overview of the Log Streaming Service (LSS).


Slide 4 - Active Health Monitoring



Slide notes


The first topic we will cover is ZPA active health monitoring for applications.

Slide 5 - Active Health Monitoring of Defined Applications



Active Health Monitoring of Defined Applications

- Active Health Monitoring
 - Connectors poll one application instance on one port every second
 - Randomized round robin through all defined applications and ports
 - No DoS on internal applications
 - Number of applications and ports controls how often any one application is polled



Slide notes


By default, ZPA monitors the health of applications based on user traffic to that application, so application health is only updated while users are accessing the application. If you explicitly define your applications (rather than enabling application discovery), you can enable active, or continuous, health monitoring.

This means that ZPA will continuously monitor the health of your applications to ensure that they're accessible using ZPA. If you enable **Active Health Monitoring** for an application, you can always view the health status of the application on the **Health** Dashboard.

With **Active Health Monitoring** enabled, Connectors will poll one local application instance on one port every second, and round robin through all of the defined applications and ports, although the polling is randomized. This is to ensure that we do not effectively perform a DoS attack on the customer's internal applications. This also means that the interval with which we poll an application/port combination depends on the number of applications defined, and the number of ports defined for each.


For discovered applications, ZPA only performs health monitoring while users are accessing the application, and for a 30 Minute interval afterwards.

Slide 6 - Active Health Monitoring of Defined Applications




Active Health Monitoring of Defined Applications

- Active Health Monitoring
 - Connectors poll one application instance on one port every second
 - Randomized round robin through all defined applications and ports
 - No DoS on internal applications
 - Number of applications and ports controls how often any one application is polled




Slide notes

Slide 7 - Active Health Monitoring of Defined Applications



Active Health Monitoring of Defined Applications

- Active Health Monitoring
 - Connectors poll one application instance on one port every second
 - Randomized round robin through all defined applications and ports
 - No DoS on internal applications
 - Number of applications and ports controls how often any one application is polled



Microsoft Exchange

File shares

ORACLE

Accounting


NETFacilities

Slide notes

Slide 8 - Active Health Monitoring of Defined Applications


Active Health Monitoring of Defined Applications

- Active Health Monitoring
 - Connectors poll one application instance on one port every second
 - Randomized round robin through all defined applications and ports
 - No DoS on internal applications
 - Number of applications and ports controls how often any one application is polled




Slide notes

Slide 9 - Active Health Monitoring of Defined Applications



Active Health Monitoring of Defined Applications

- Active Health Monitoring
 - Connectors poll one application instance on one port every second
 - Randomized round robin through all defined applications and ports
 - No DoS on internal applications
 - Number of applications and ports controls how often any one application is polled



Microsoft Exchange

File shares

ORACLE


Accounting

NETFacilities

80


Slide notes

Slide 10 - Active Health Monitoring of Defined Applications




Active Health Monitoring of Defined Applications

- Active Health Monitoring
 - Connectors poll one application instance on one port every second
 - Randomized round robin through all defined applications and ports
 - No DoS on internal applications
 - Number of applications and ports controls how often any one application is polled









Slide notes

Slide 11 - Active Health Monitoring of Defined Applications



Active Health Monitoring of Defined Applications

- Active Health Monitoring
 - Connectors poll one application instance on one port every second
 - Randomized round robin through all defined applications and ports
 - No DoS on internal applications
 - Number of applications and ports controls how often any one application is polled
- Active Health Monitoring is only for:
 - Defined applications with explicit domains (no wildcards, no IP addresses)
 - On a maximum of 10 ports (specific port, or a port range)



Slide notes

Note that **Active Health Monitoring** can only be enabled for defined applications with specific hostnames, so you cannot enable this for applications specified with a wildcard domain, nor for applications defined by IP address. Also, that the maximum number of ports for any one application that can be actively monitored is 10, whether configured individually, or as a port range.

Slide 12 - Health Check and Reporting Configuration

Health Check and Reporting Configuration

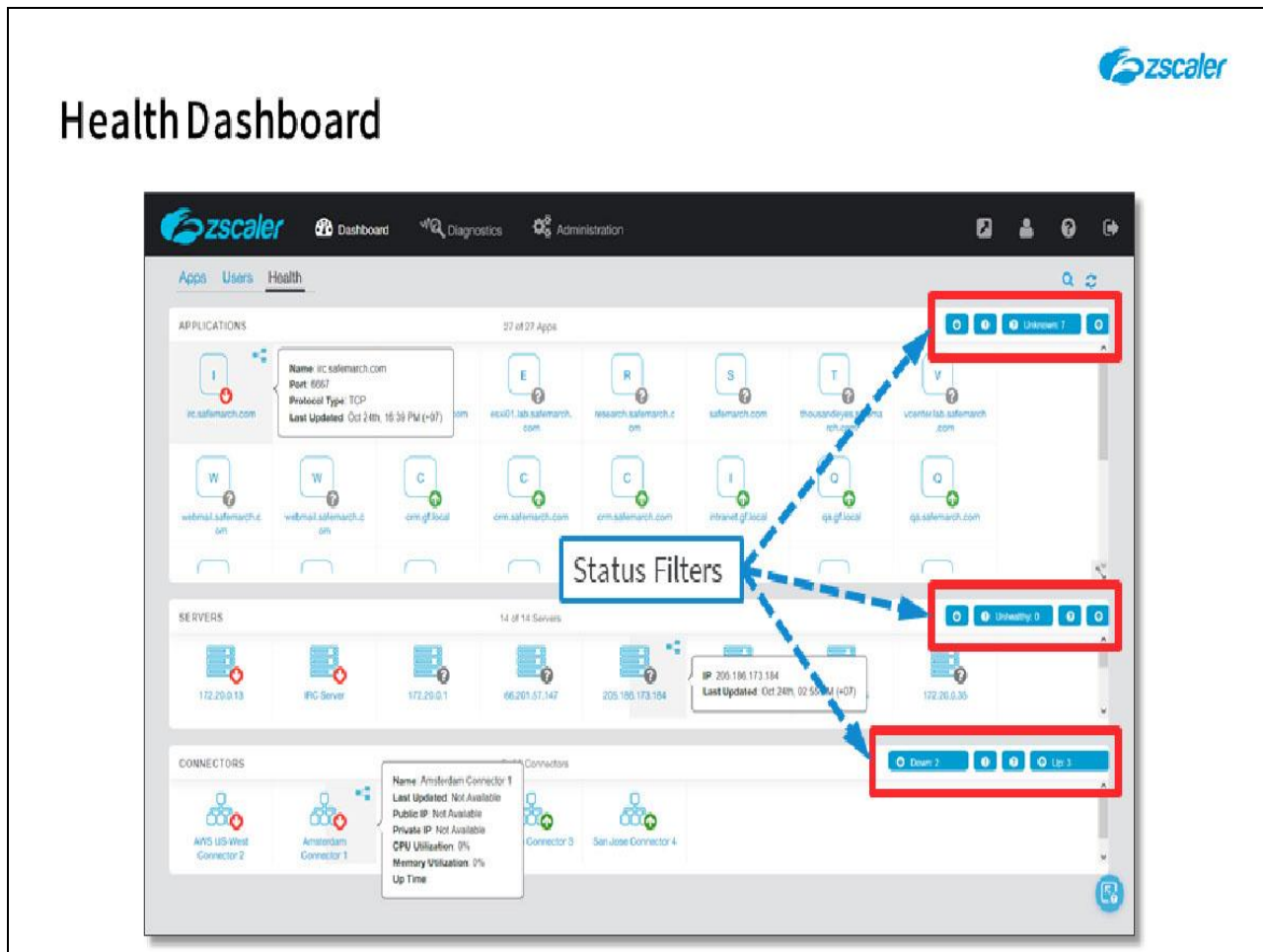
The screenshot displays the Zscaler Administration console. The left sidebar shows the navigation menu with 'Applications' selected. The main area shows the 'Edit Application' configuration for an application named 'OFS'. The 'Status' is 'Enabled'. The 'Domain or IP Address' is 'fms.training.safemarch.com'. The 'TCP Port Ranges' are '139' to '139' and '445' to '445'. The 'UDP Port Ranges' are 'From...' to 'To...'. The 'Enable Double Encryption' is 'Disabled'. The 'Bypass When' is 'Never'. The 'Server Groups' are 'x San Jose Auto-Servers'. The 'Application Group' is 'Safemarch Training Application Group'. The 'Health Reporting' dropdown is set to 'Continuous' and the 'Health Check' dropdown is set to 'Default'. Two callout boxes provide details about these settings:

- Health Reporting:** Choose whether the Connector reports the health of this application to the ZPA Central Authority continuously (Continuous) or while a user is accessing it (On Access).
- Health Check:** Enable if you want the Connector to check the health status of this application. If disabled, the Connector assumes the health status of the application is Up.

Slide notes

The **Health Check** and **Health Reporting** options are enabled in the configuration for an **Application Segment**. The **Health Check** option is a simple **Default** (meaning enabled), or **None** configuration. The **Health Reporting** option may be set to **Continuous**, or **On Access** (for reporting only while users are accessing the application).

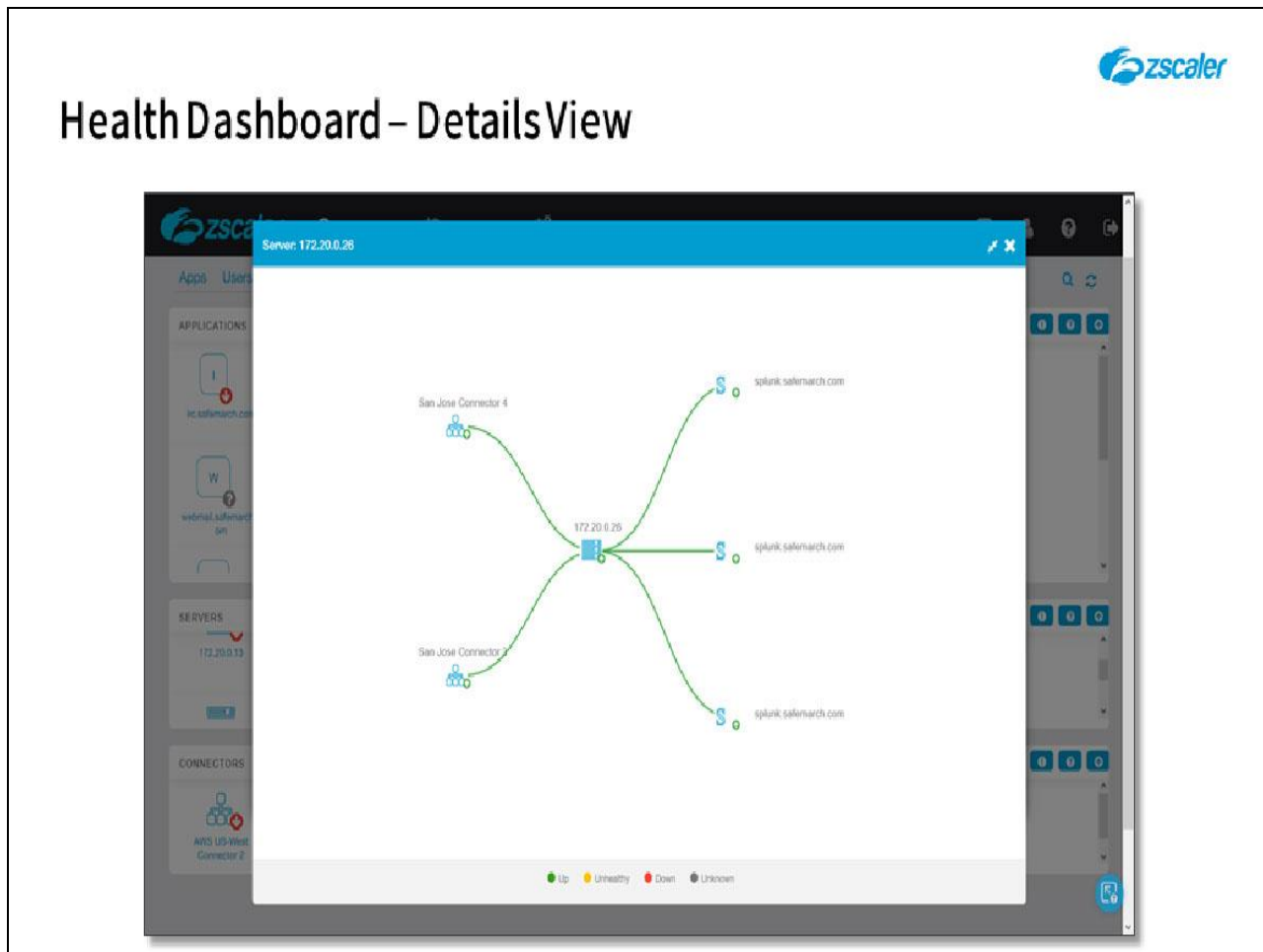
Slide 13 - Health Dashboard



Slide notes

The **Health** Dashboard provides a real-time view of the status of **APPLICATIONS**, **SERVERS**, and **CONNECTORS**. One thing to note here, is that the default view is filtered to show only those items that are **Down** or are **Unhealthy**. The status filter toggles can be used to additionally show or hide **Healthy** and **Unknown** items.

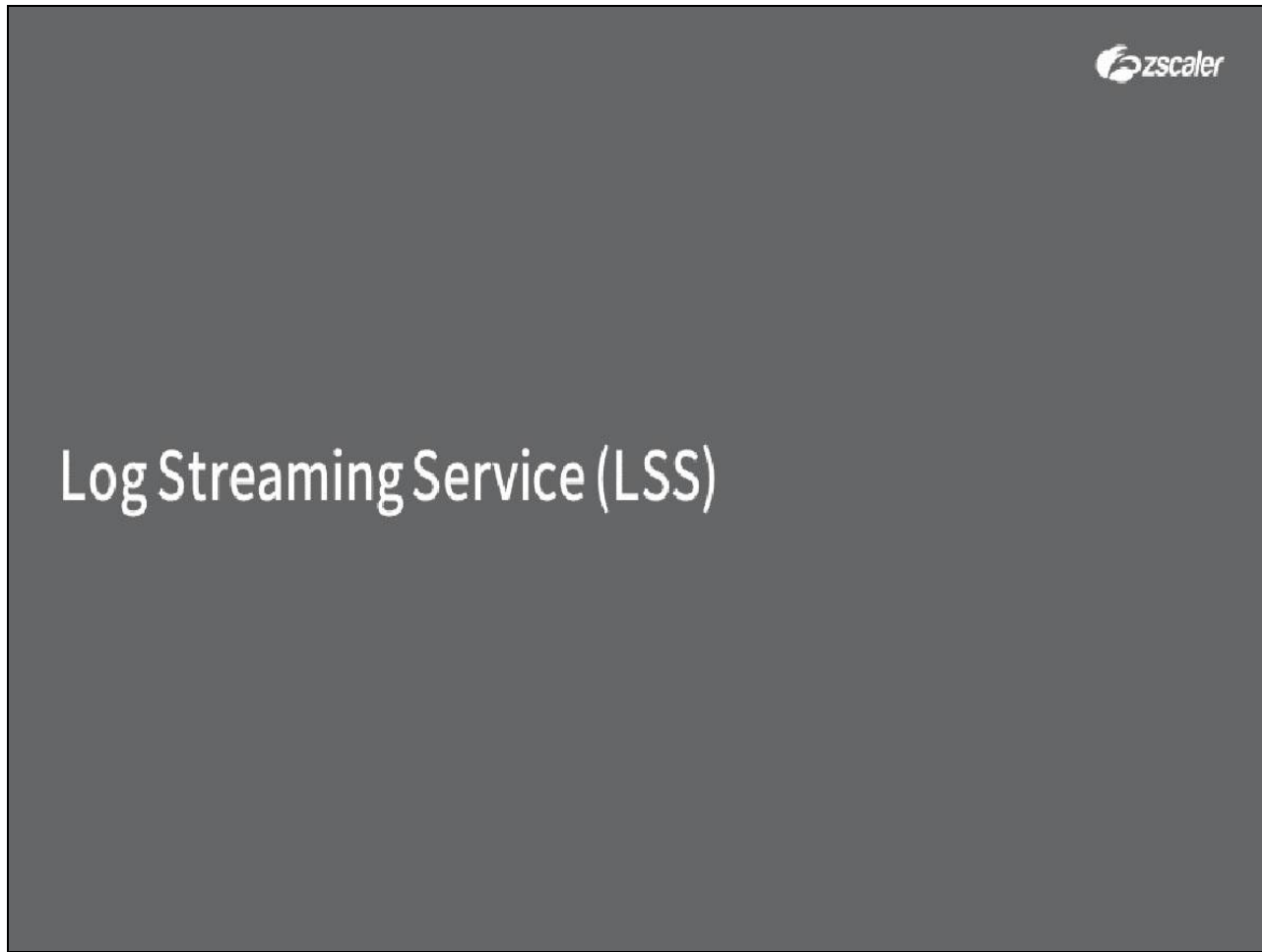
Slide 14 - Health Dashboard – Details View



Slide notes

From the **Health** Dashboard you can drill down into any object, to view a real-time status map of its connectivity.

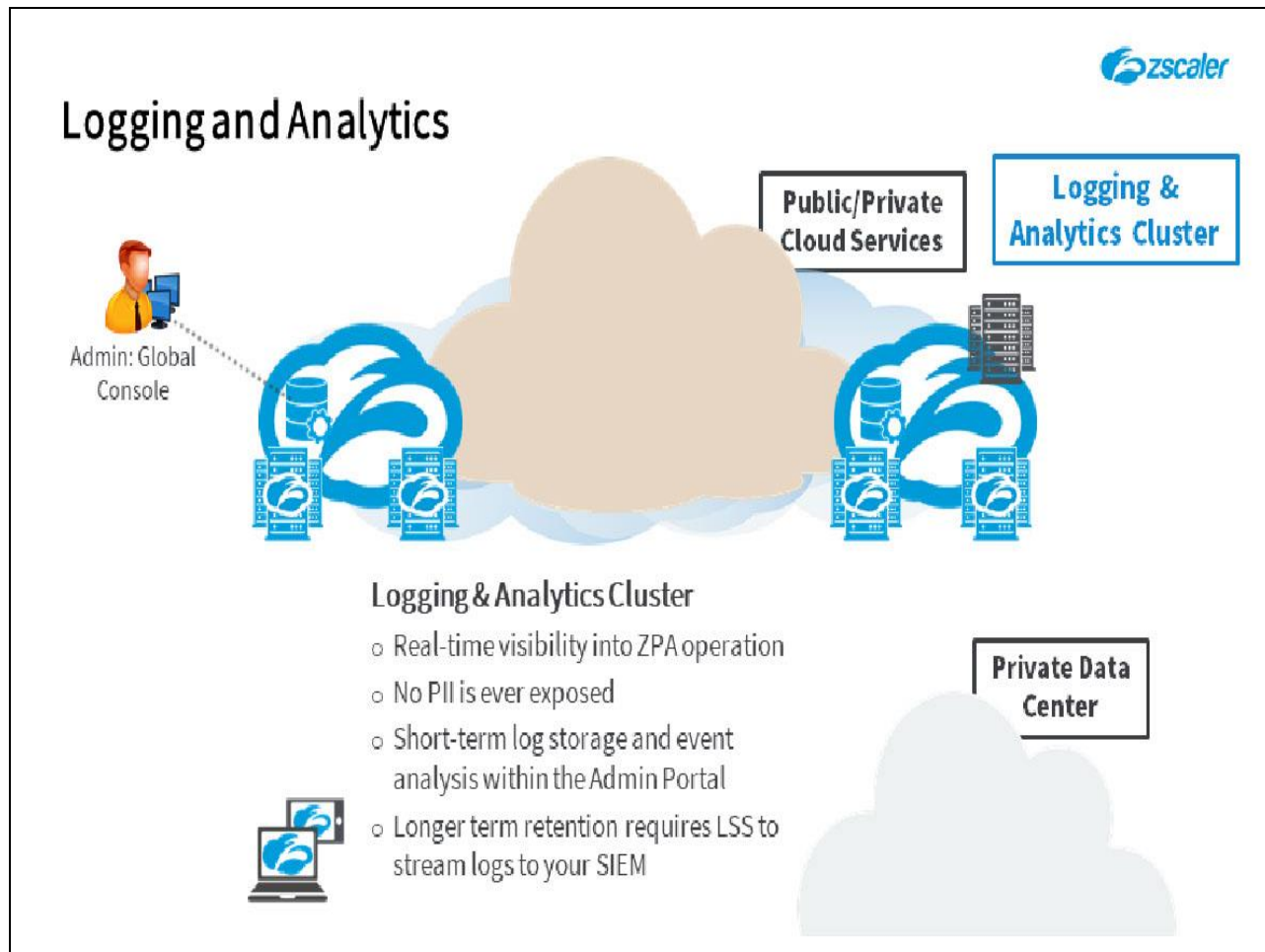
Slide 15 - Log Streaming Service



Slide notes

The final topic we will cover is an overview of the ZPA Log Streaming Service (LSS).

Slide 16 - Logging and Analytics

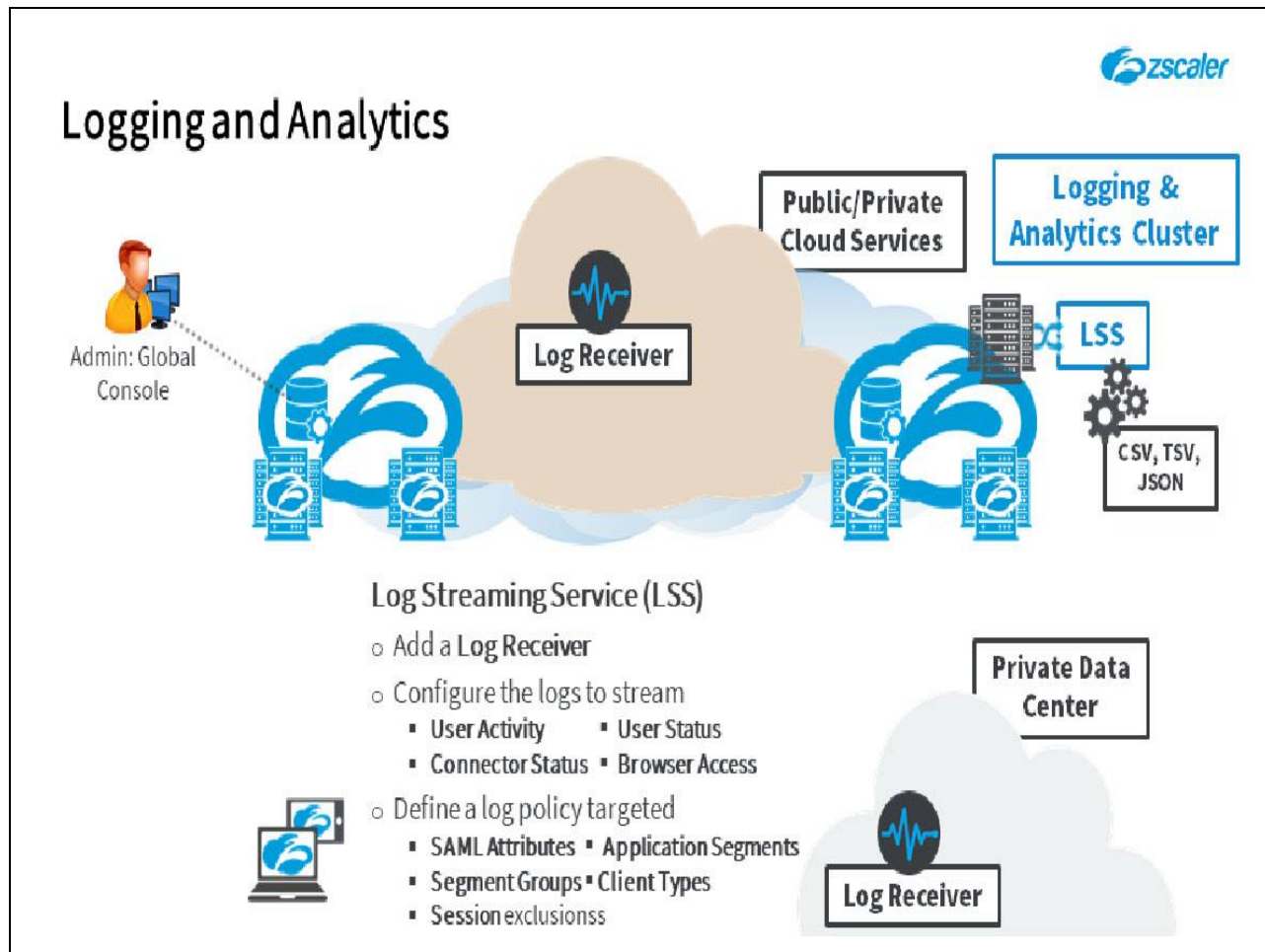


Slide notes

The Logging and Analytics Cluster provides centralized, real-time visibility into the operation of ZPA by analyzing events reported primarily by the ZPA-ZENs. No personally identifiable information (PII) is included in any logs created by ZPA, as security and privacy are the central tenets upon which the solution has been built.

However, the ZPA infrastructure and user logs that are sent to the Log Cluster are only available short-term for real-time viewing and analysis from the ZPA Admin Portal (14 Days at most). If longer log retention is required, you will need to configure LSS to stream ZPA logs to your internal SIEM.

Slide 17 - Logging and Analytics



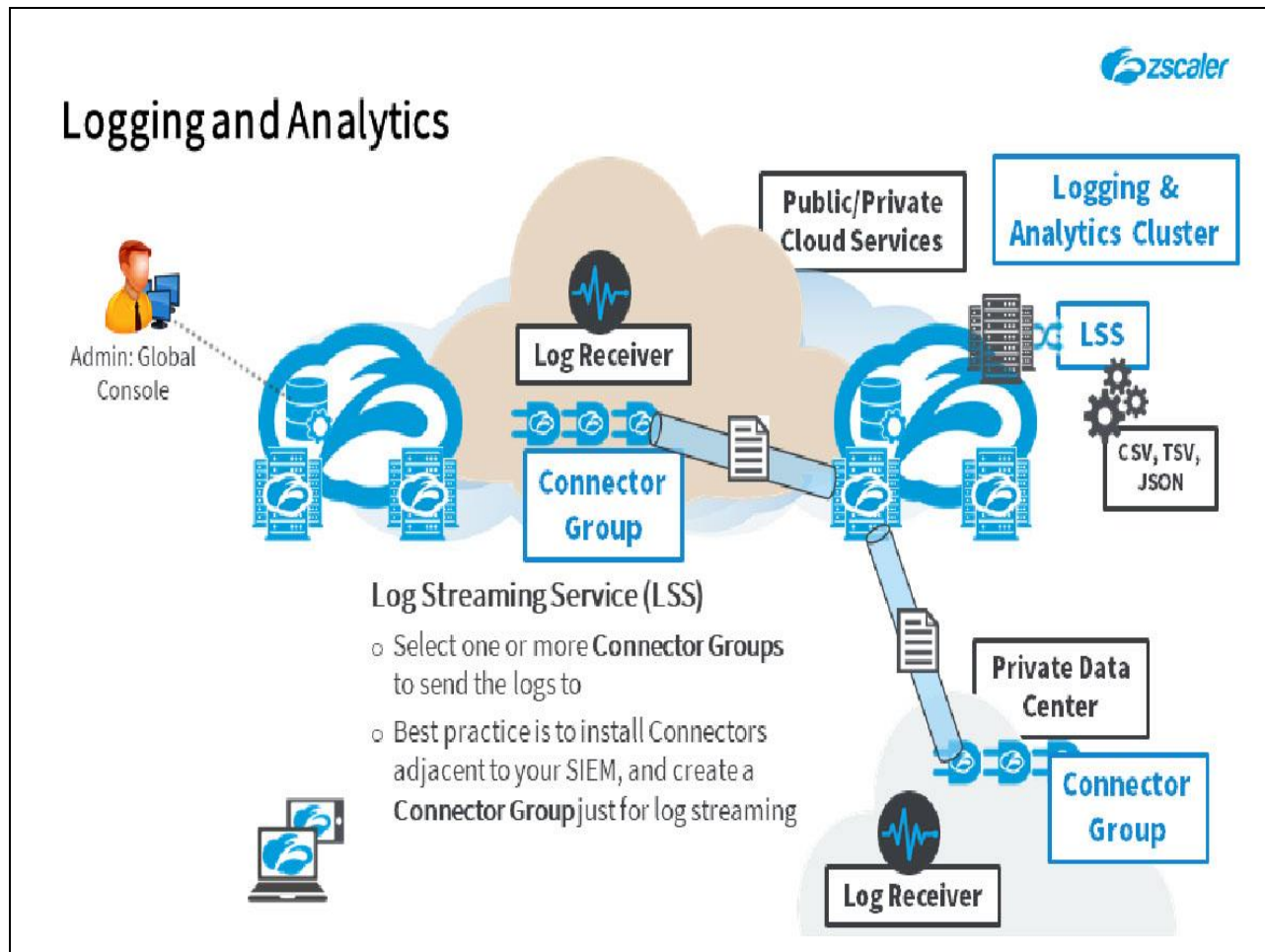
Slide notes

To enable log streaming you need to add at least one **Log Receiver** in the ZPA admin portal, specified by **FQDN** (or **IP Address**) and **TCP Port**. You need to specify the **Log Type** to be sent, the types available being: **User Activity**; **User Status**; **Connector Status**; and **Browser Access**. If you need to receive multiple **Log Types**, then you will need to create multiple **Log Receivers** (one for each type).

You must select the format for the logs (**CSV**, **TSV**, or **JSON**), plus you have the option to edit the log stream content in order to capture only the required fields and effectively create a custom log template. You can elect to receive all logs or define a streaming policy for the type of **Log Receiver**, the criteria available being dependent upon the **Log Type** you selected.

For example, you could create a **User Activity** policy where the receiver will only capture logs (i.e. include logs) for: Specified **SAML Attributes**; selected **Application Segments**; selected **Segment Groups**; the specified **Client Type**; or you can specify a specific set of **Session** status error codes to exclude.

Slide 18 - Logging and Analytics




Slide notes

LSS makes use of the Connector infrastructure for the delivery of logs to your SIEM and you need to select a **Connector Group** to send the logs to. This could be a regular **Connector Group**, although we strongly recommend that you install Connectors adjacent to your SIEM and add them to a group dedicated to receiving the logs.

Log streaming is a best effort service and if it comes to a conflict between streaming logs or supporting application access through a Connector, the Logs will be dropped. So, if you have a single **Connector Group** for both application access and log streaming, it is possible that you might lose logs when the Connectors get busy.

Once within your SIEM, you are free to analyze the logs, and use them to identify and remediate problems as necessary. You also have the option to store the logs long term for compliance reasons, or for later analysis.

Slide 19 - Logging and Analytics



LSS Caveats and Recommendations

Log Retention


- Retention within the ZPA Service (accessible within the Admin Portal) is 14 Days
- If longer retention is needed, then LSS configuration is required

Slide notes

There are some caveats with LSS that you need to be aware of, plus we have some general recommendations.

Firstly, the maximum log retention with the ZPA Service is **14 Days**, so if you require log retention longer than this, you will need to set up log streaming to your SIEM.

Slide 20 - Logging and Analytics



LSS Caveats and Recommendations

Log Retention

- Retention within the ZPA Service (accessible within the Admin Portal) is 14 Days
- If longer retention is needed, then LSS configuration is required


Log Retransmission

- After a Connector outage, only the last 15 Minutes of logs will be retransmitted

Slide notes

Should there be a problem reaching the Connectors specified for log streaming, once the Connectors become available again, only the last **15 mins** of logs will be retransmitted.

Slide 21 - LSS Caveats and Recommendations



LSS Caveats and Recommendations


- Log Retention**
 - Retention within the ZPA Service (accessible within the Admin Portal) is 14 Days
 - If longer retention is needed, then LSS configuration is required
- Log Retransmission**
 - After a Connector outage, only the last 15 Minutes of logs will be retransmitted
- Multiple Connector Groups**
 - If logs are streamed to multiple Connector Groups, the logs are duplicated to each group
 - Stream logs to multiple Connector Groups for redundancy

Slide notes

When setting up LSS, you have the option to select multiple **Connector Groups** for every Log Receiver that you add. If you select multiple groups, logs are duplicated to each group.

In the light of the previous point, this gives you a method for ensuring log redundancy should there be problems with a set of Connectors.

Slide 22 - LSS Caveats and Recommendations



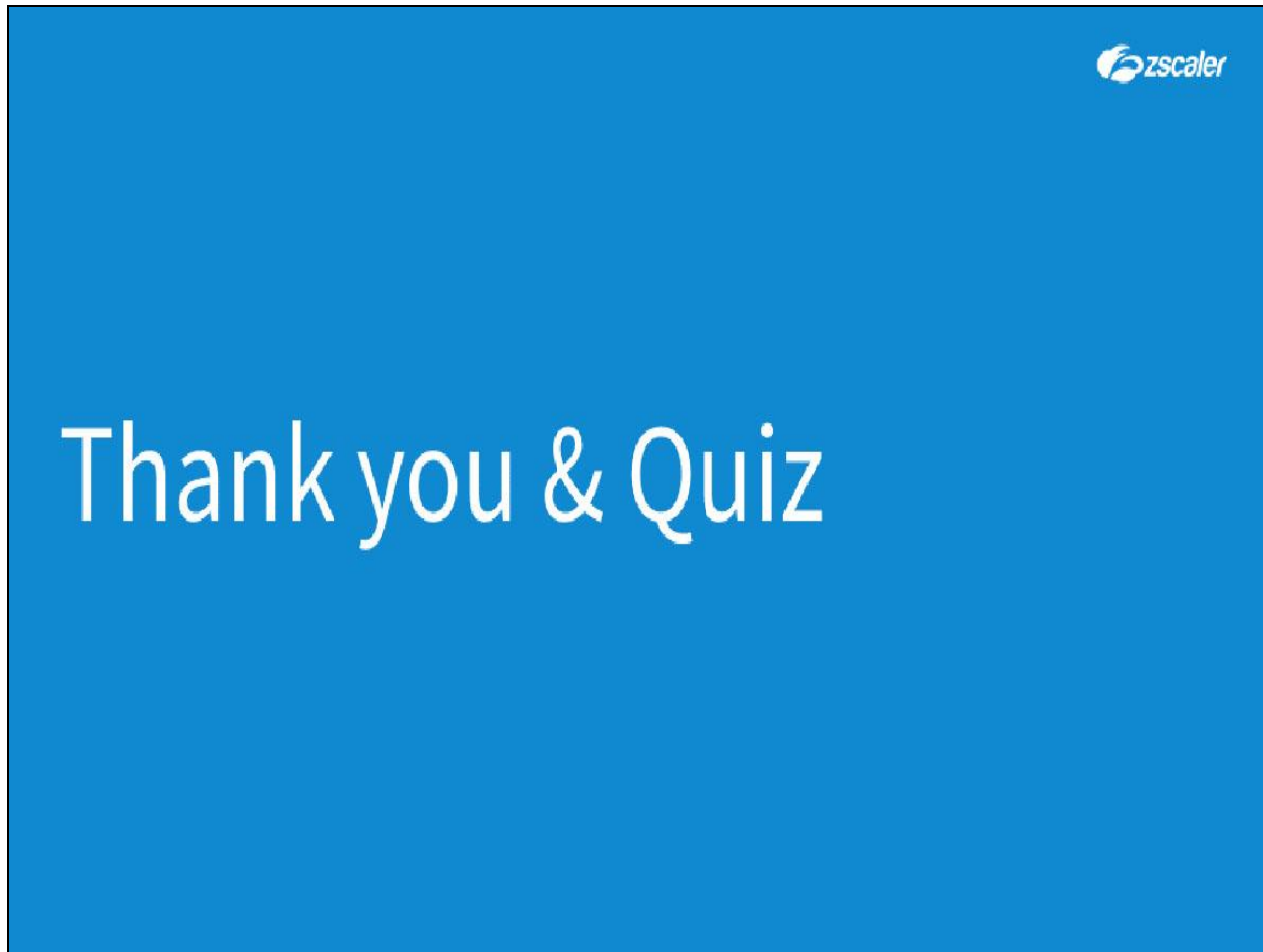
LSS Caveats and Recommendations

- Log Retention**
 - Retention within the ZPA Service (accessible within the Admin Portal) is 14 Days
 - If longer retention is needed, then LSS configuration is required
- Log Retransmission**
 - After a Connector outage, only the last 15 Minutes of logs will be retransmitted
- Multiple Connector Groups**
 - If logs are streamed to multiple Connector Groups, the logs are duplicated to each group
 - Stream logs to multiple Connector Groups for redundancy
- Log Connector Monitoring**
 - A Log Status configuration can be used to monitor the LSS Connectors
 - Configure triggers and alerts within your SIEM to notify of LSS Connector problems
 - Add LSS Connectors as necessary to ensure you have adequate capacity

Slide notes

One of the **Log Types** available is **Connector Status**. This gives you a tool to monitor availability of your LSS Connectors. You can stream **Connector Status** logs to your SIEM (preferably using redundant Connector Groups), where you can set up monitors and triggers to alert you of any LSS Connector related issues. This method can also be used to alert you to potential LSS capacity issues, which would allow you to add Connectors to the LSS **Connector Group(s)** in good time to avoid loss of logs.

Slide 23 - Thank you & Quiz



Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

What follows is a short quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.