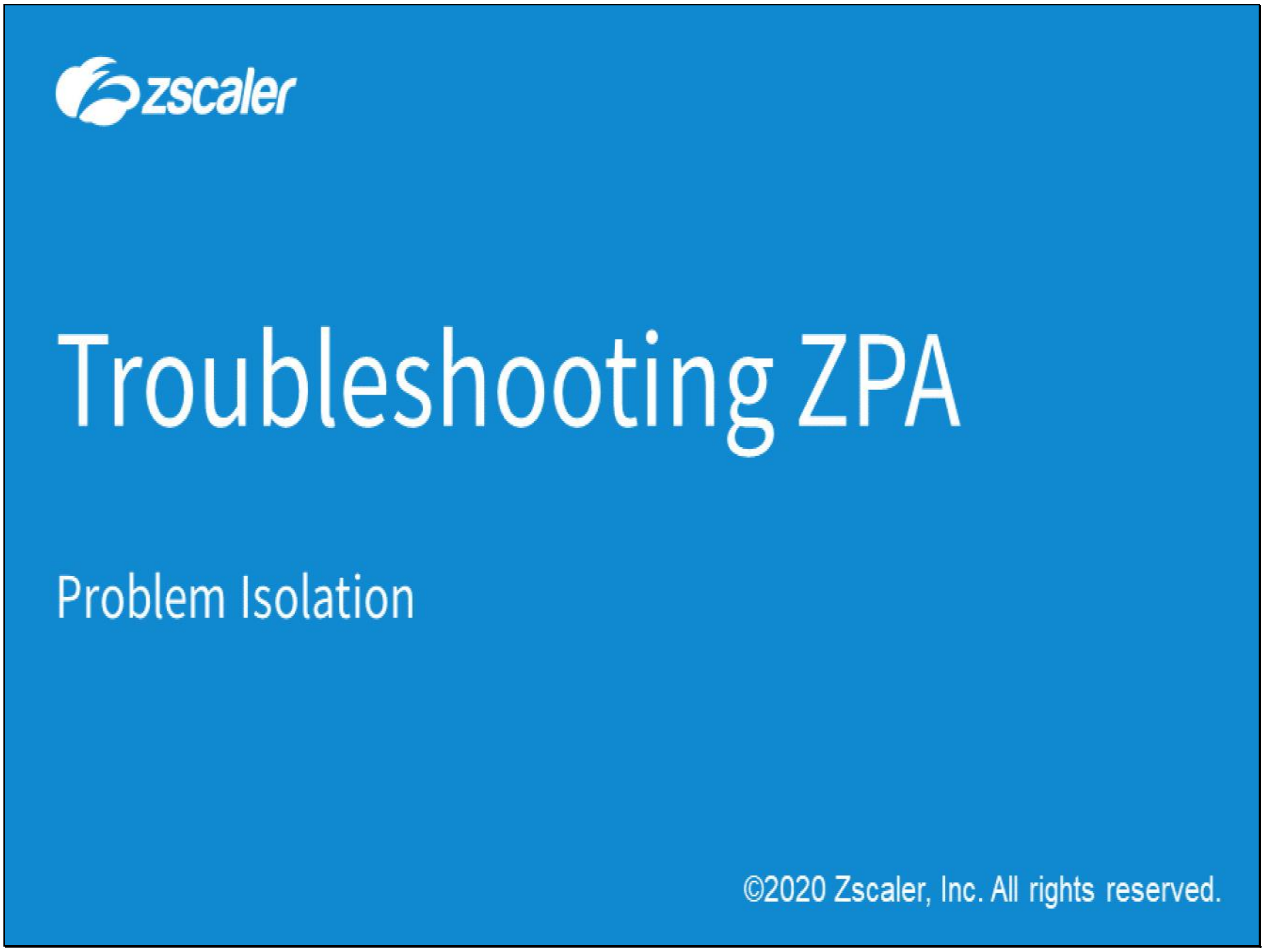
Slide 1 - Troubleshooting ZPA



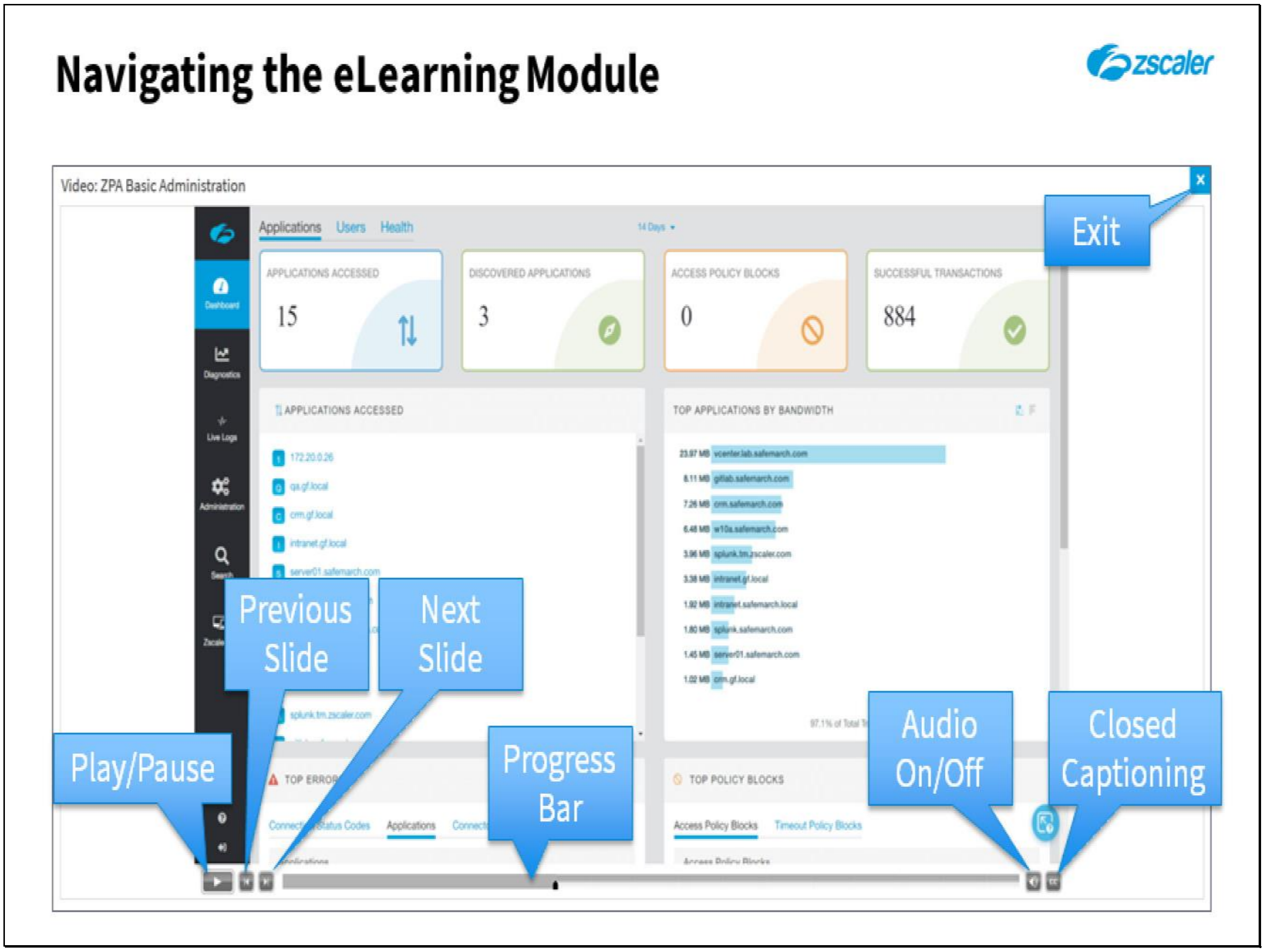
Troubleshooting ZPA

Problem Isolation

Slide notes

Welcome to this training module on problem isolation when troubleshooting ZPA.

Slide 2 - Navigating the eLearning Module



Navigating the eLearning Module

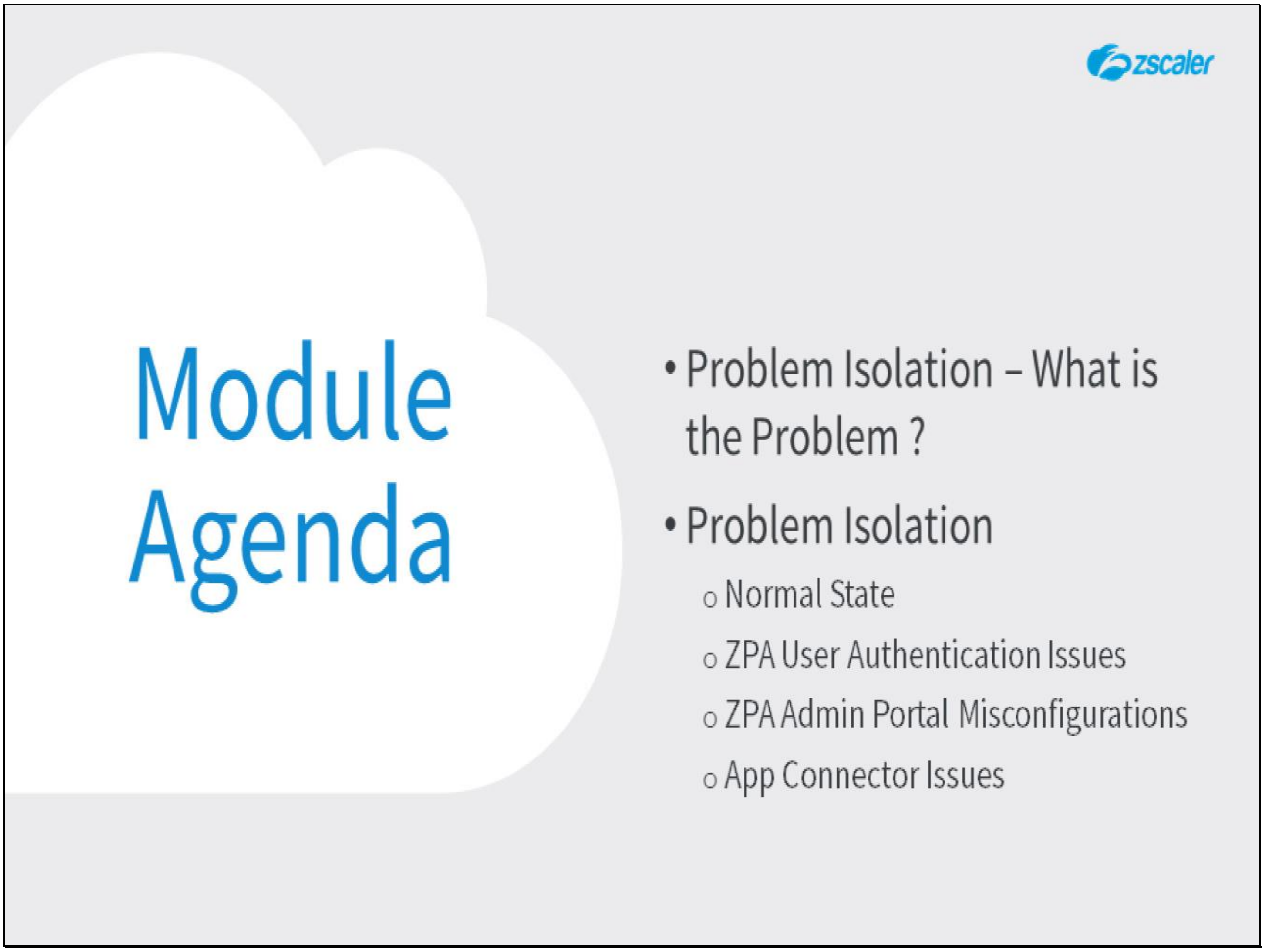
Video: ZPA Basic Administration

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 - Module Agenda



zscaler

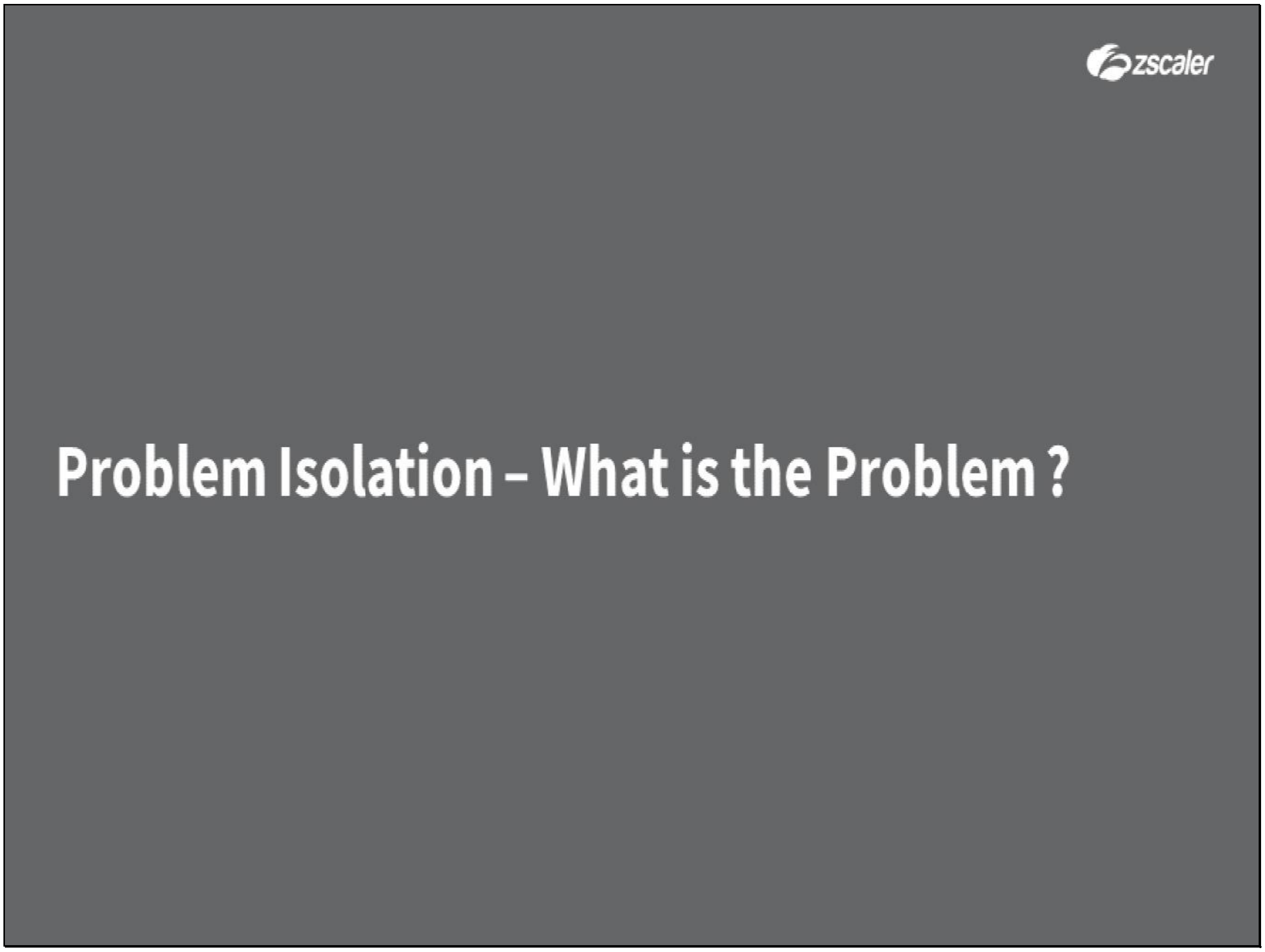
Module Agenda

- Problem Isolation – What is the Problem ?
- Problem Isolation
  - o Normal State
  - o ZPA User Authentication Issues
  - o ZPA Admin Portal Misconfigurations
  - o App Connector Issues

Slide notes

In this module, we will look at the following topics: Problem isolation in general, to identify precisely what the problem is. And then problem isolation in three situations: user authentication issues, ZPA admin portal misconfigurations, and App Connector issues.

Slide 4 - Problem Isolation – What is the Problem ?

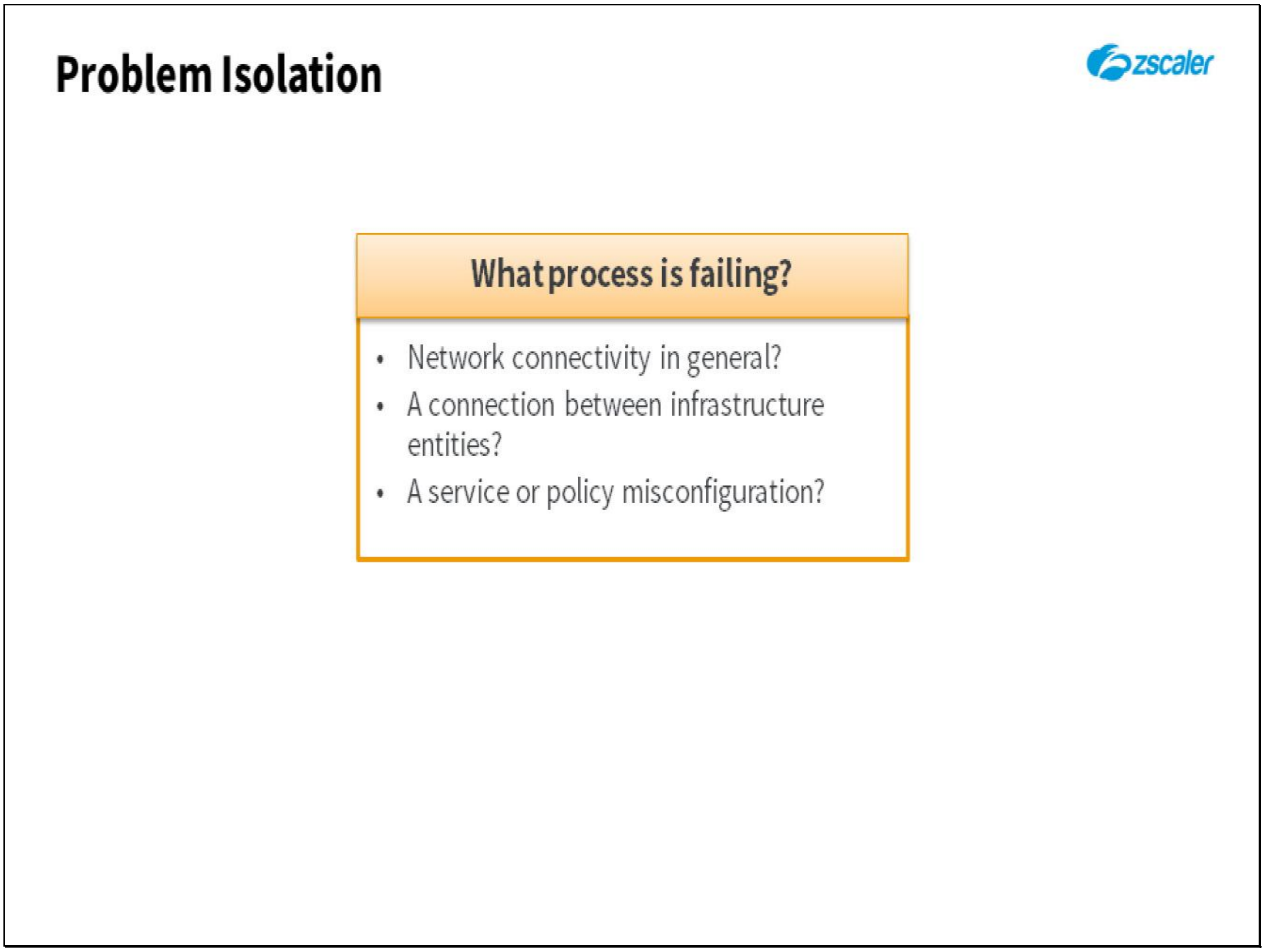


Problem Isolation – What is the Problem ?

Slide notes

In the first section, we will look at the concept of problem isolation in general, to identify precisely what the problem is.

Slide 5 - Problem Isolation



Problem Isolation

What process is failing?

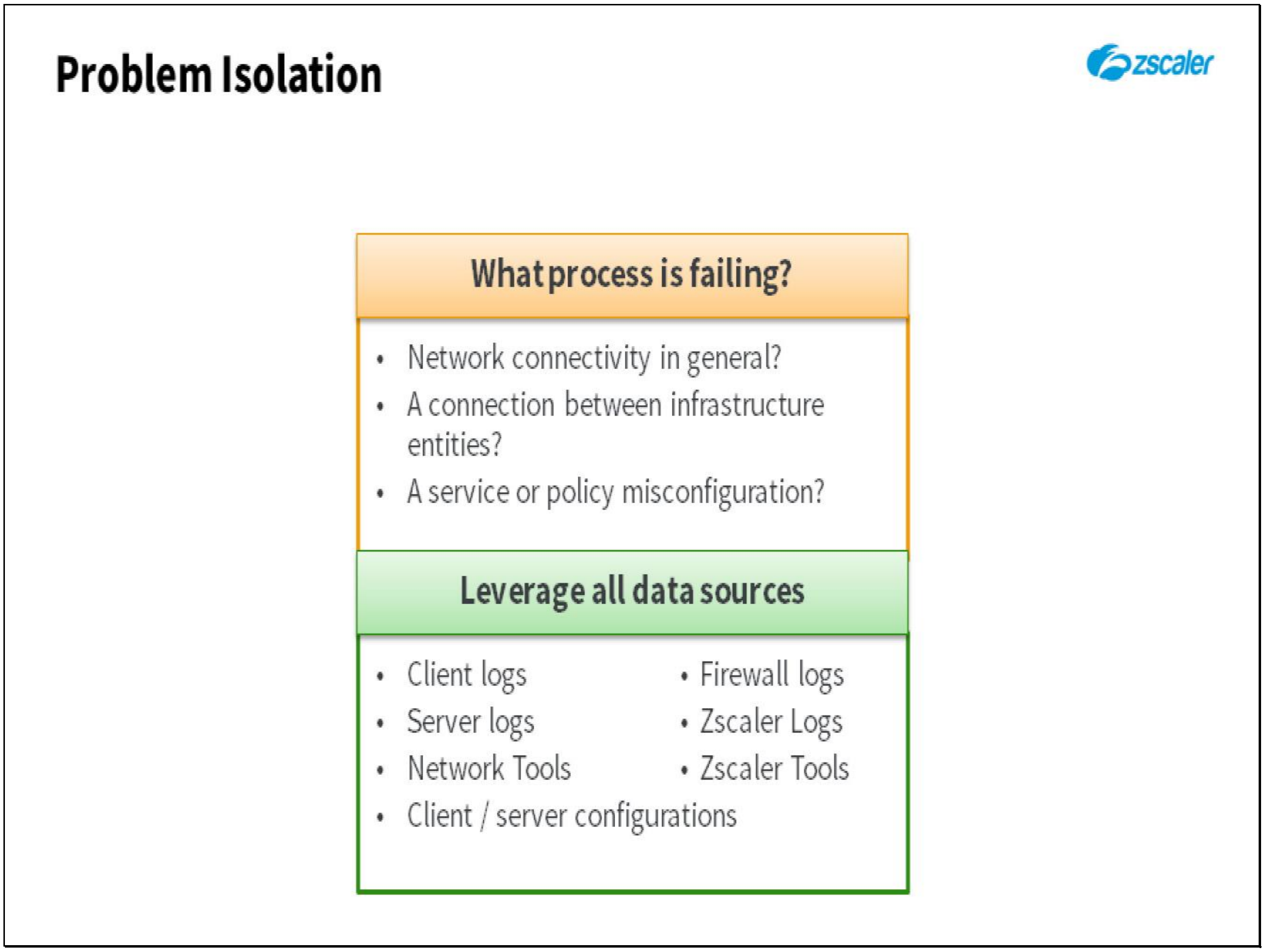
- Network connectivity in general?
- A connection between infrastructure entities?
- A service or policy misconfiguration?

Slide notes

Hopefully by this point you have localized the problem, so you know more or less **where** it is occurring, now we need to identify **what** logical process is failing.

Is there some general network connectivity issue? Is there a problem between infrastructure entities, for example between the Identity Provider and Service Provider in a SAML implementation? Or is there a misconfiguration somewhere, either within the infrastructure, or on the ZPA Cloud?

Slide 6 - Problem Isolation



Problem Isolation

What process is failing?

- Network connectivity in general?
- A connection between infrastructure entities?
- A service or policy misconfiguration?

Leverage all data sources

- Client logs
- Server logs
- Network Tools
- Client / server configurations
- Firewall logs
- Zscaler Logs
- Zscaler Tools

Slide notes

Once you have a good idea where a problem is occurring, you can make use of all the related sources of data to help you finally diagnose what the problem actually is. Logs can be a particularly helpful source of information, logs from software on the client device, the server the client is attempting to connect to, logs from some intermediate device or infrastructure component, such as; router or firewall, authentication server or IdP, and of course there are the ZPA Diagnostics logs.

You should make use of all the tools available to you, whether general networking tools, or those provided by Zscaler. Plus, you should start to review the configuration settings of the implicated components.

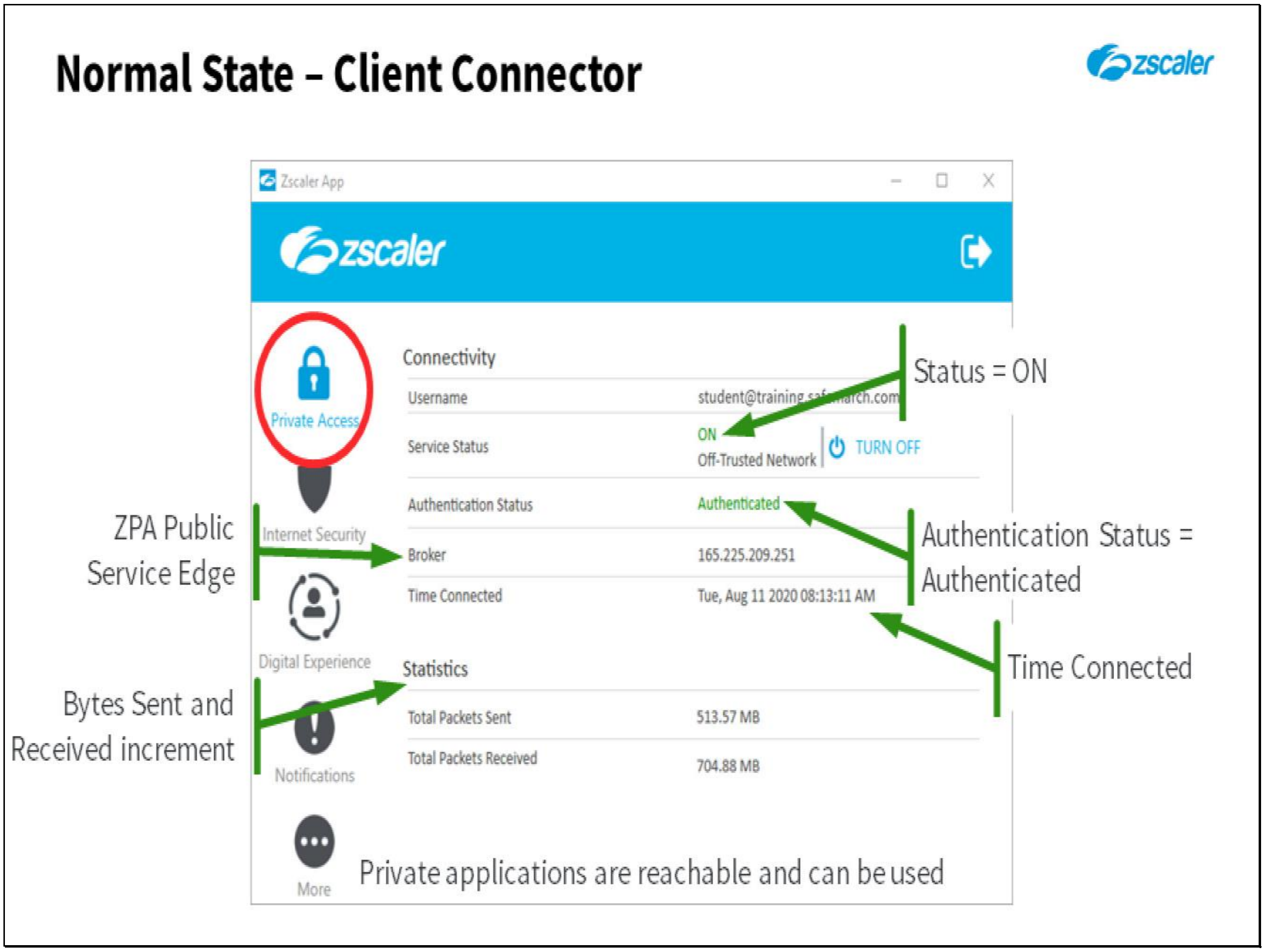
Slide 7 - Normal State

Normal State

Slide notes

In the next section, we will look at the **normal state**, when a ZPA user is successfully authenticated into the Zscaler Client Connector and has access to ZPA applications.

Slide 8 - Normal State – Client Connector



Normal State – Client Connector

Connectivity

Username student@training.safemarch.com

Service Status ON
Off-Trusted Network

Authentication Status Authenticated

Broker 165.225.209.251

Time Connected Tue, Aug 11 2020 08:13:11 AM

Statistics

Total Packets Sent 513.57 MB

Total Packets Received 704.88 MB

Status = ON

Authentication Status = Authenticated

Time Connected

ZPA Public Service Edge

Bytes Sent and Received increment

Private applications are reachable and can be used

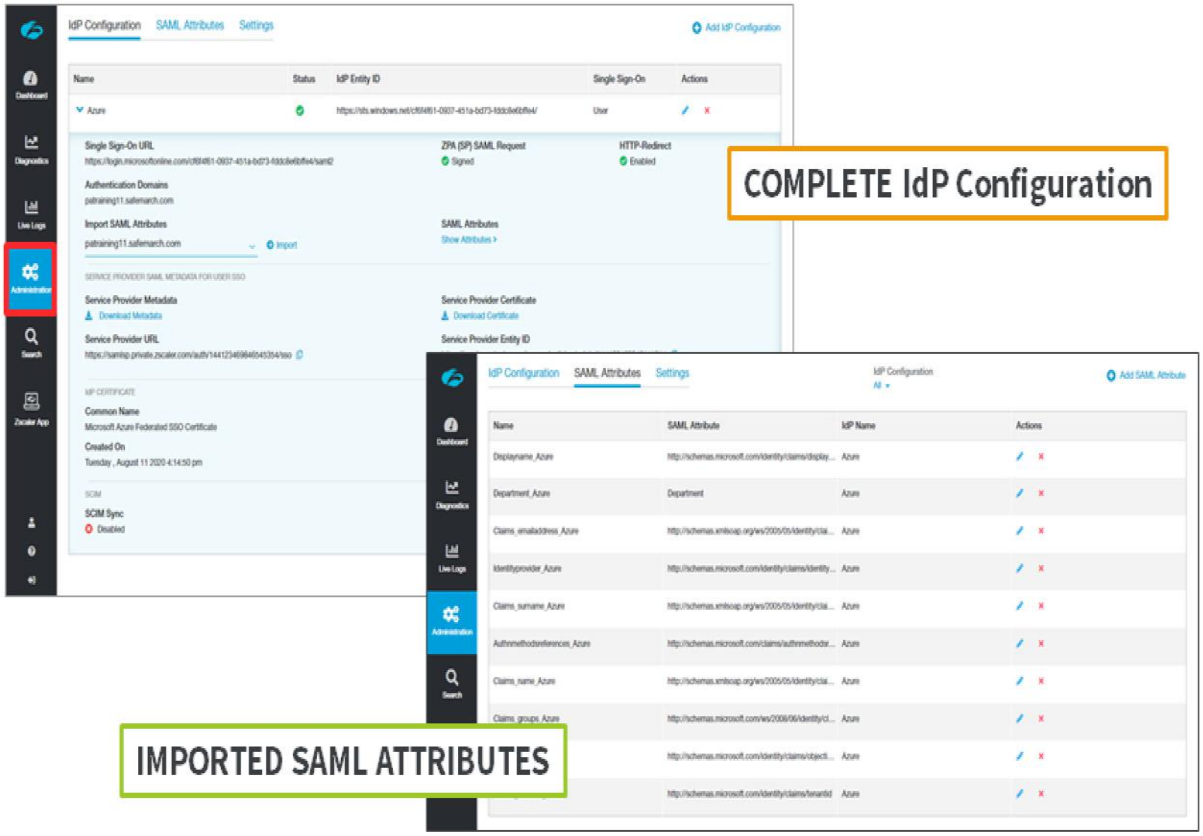
Slide notes

Here we can see the **Private Access** page of the Zscaler Client Connector for a user that is successfully authenticated, and has full access to the private applications they are authorized to use.

The ZPA **Service Status** is **ON**, the **Authentication Status** shows **Authenticated**, the **IP address of the ZPA Public Service Edge** that the user is connected to is shown, the **Time Connected** is indicated, as is the **Total Bytes Sent** and **Received** accessing the private applications.

Slide 9 - Normal State – IdP Configuration

Normal State – IdP Configuration



Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure	✓	https://sts.windows.net/cf6f4f61-0937-451a-bd73-fddc8e6bffe4/	User	

Single Sign-On URL
https://login.microsoftonline.com/cf6f4f61-0937-451a-bd73-fddc8e6bffe4/saml2

ZPA (SP) SAML Request
✓ Signed

HTTP-Redirect
✓ Enabled

Authentication Domains
patraining11.safemarch.com

Import SAML Attributes
patraining11.safemarch.com Import

SAML Attributes
Show Attributes >

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata
Download Metadata

Service Provider Certificate
Download Certificate

Service Provider URL
https://samlsp.private.zscaler.com/auth/144123469846545354/sso

Service Provider Entity ID

IdP CERTIFICATE

Common Name
Microsoft Azure Federated SSO Certificate

Created On
Tuesday , August 11 2020 4:14:50 pm

SCIM

SCIM Sync
Disabled

COMPLETE IdP Configuration

IdP Configuration SAML Attributes Settings IdP Configuration All ▾ Add SAML Attribute

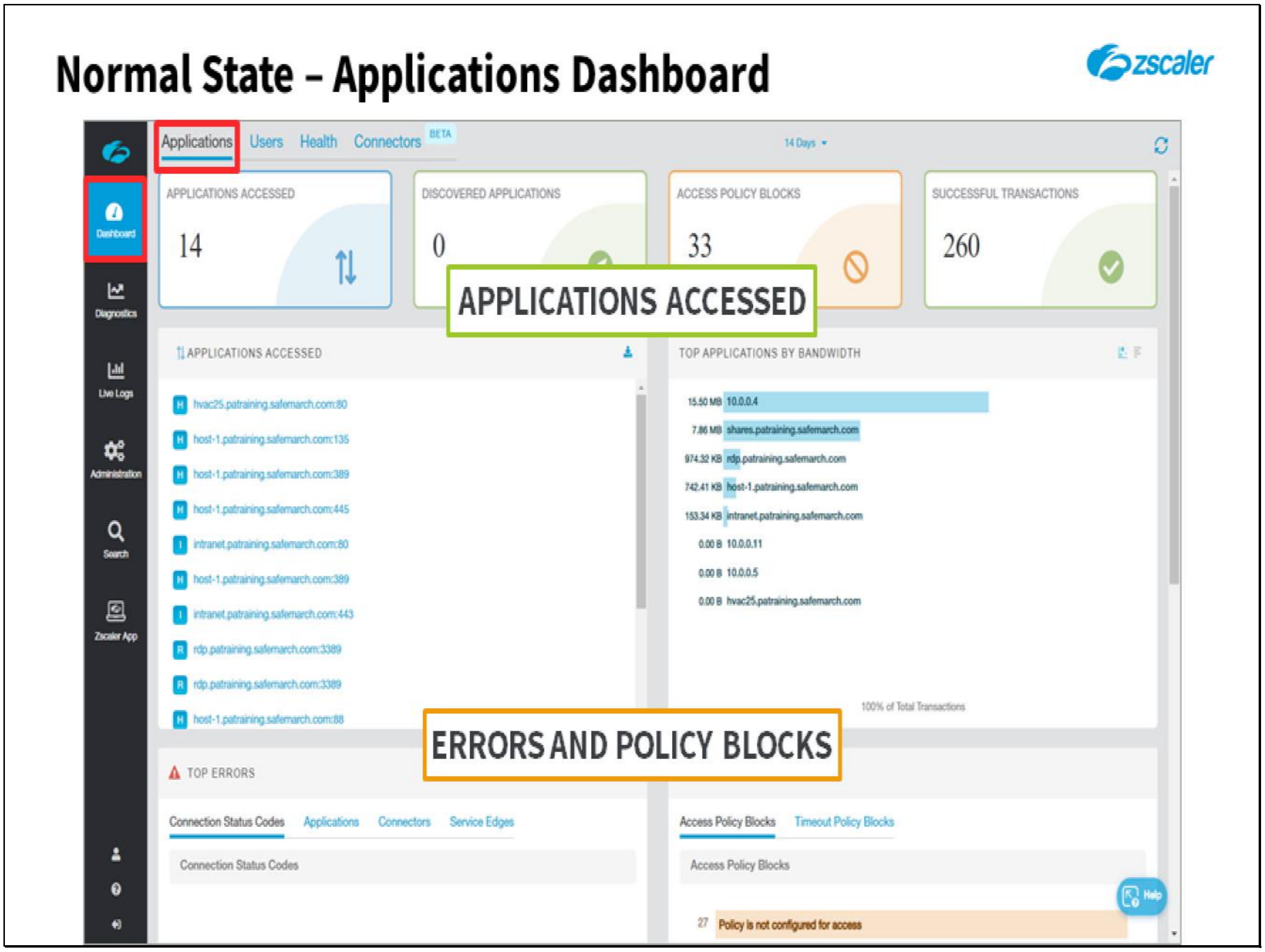
Name	SAML Attribute	IdP Name	Actions
Displayname_Azure	http://schemas.microsoft.com/identity/claims/display...	Azure	
Department_Azure	Department	Azure	
Claims_emailaddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/clai...	Azure	
Identityprovider_Azure	http://schemas.microsoft.com/identity/claims/identity...	Azure	
Claims_surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/clai...	Azure	
Authnmethodsreferences_Azure	http://schemas.microsoft.com/claims/authnmethodsr...	Azure	
Claims_name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/clai...	Azure	
Claims_groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/cl...	Azure	
	http://schemas.microsoft.com/identity/claims/objecti...	Azure	
	http://schemas.microsoft.com/identity/claims/tenantid	Azure	

IMPORTED SAML ATTRIBUTES

Slide notes

In the ZPA admin portal, under the **Administration** menu, you can verify that the required SAML IdP configuration is set up correctly and that SAML attributes have been imported and saved.

Slide 10 - Normal State – Applications Dashboard



Normal State – Applications Dashboard

APPLICATIONS ACCESSED

ERRORS AND POLICY BLOCKS

APPLICATIONS ACCESSED	DISCOVERED APPLICATIONS	ACCESS POLICY BLOCKS	SUCCESSFUL TRANSACTIONS
14	0	33	260

APPLICATIONS ACCESSED

- H hvac25.patraining.safemarch.com:80
- H host-1.patraining.safemarch.com:135
- H host-1.patraining.safemarch.com:389
- H host-1.patraining.safemarch.com:445
- I intranet.patraining.safemarch.com:80
- H host-1.patraining.safemarch.com:389
- I intranet.patraining.safemarch.com:443
- R rdp.patraining.safemarch.com:3389
- R rdp.patraining.safemarch.com:3389
- H host-1.patraining.safemarch.com:88

TOP APPLICATIONS BY BANDWIDTH

15.50 MB	10.0.0.4
7.86 MB	shares.patraining.safemarch.com
974.32 KB	rdp.patraining.safemarch.com
742.41 KB	host-1.patraining.safemarch.com
153.34 KB	intranet.patraining.safemarch.com
0.00 B	10.0.0.11
0.00 B	10.0.0.5
0.00 B	hvac25.patraining.safemarch.com

100% of Total Transactions

TOP ERRORS

Connection Status Codes | Applications | Connectors | Service Edges

Connection Status Codes

Access Policy Blocks | Timeout Policy Blocks

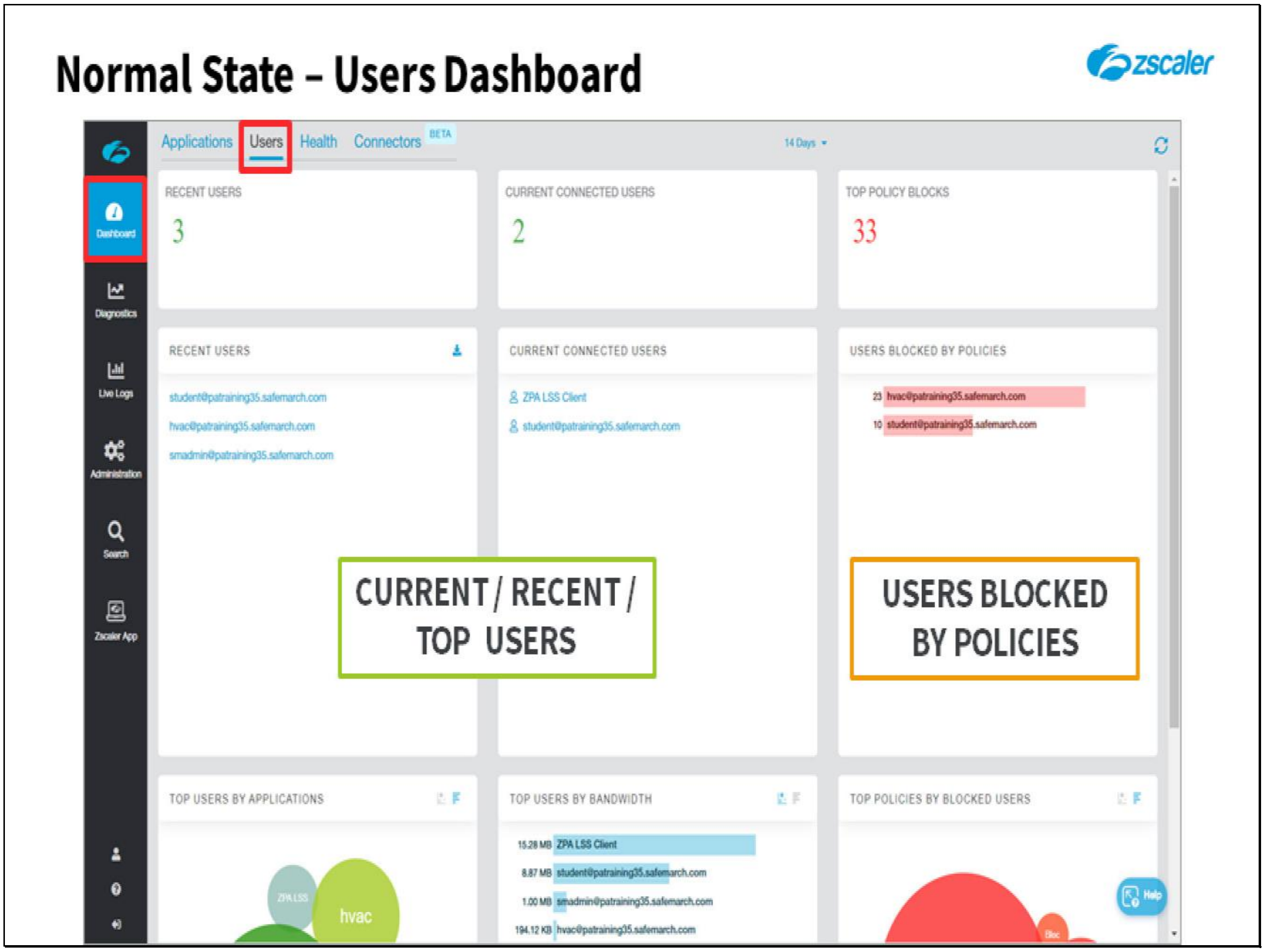
Access Policy Blocks

27 Policy is not configured for access

Slide notes

On the **Applications** Dashboard, you can view lists and statistics for the private applications available, and currently being accessed by your users. Also listed here, if applicable, are current **ACCESS ERRORS** and **POLICY BLOCKS**.

Slide 11 - Normal State – Users Dashboard



Normal State – Users Dashboard

CURRENT / RECENT / TOP USERS

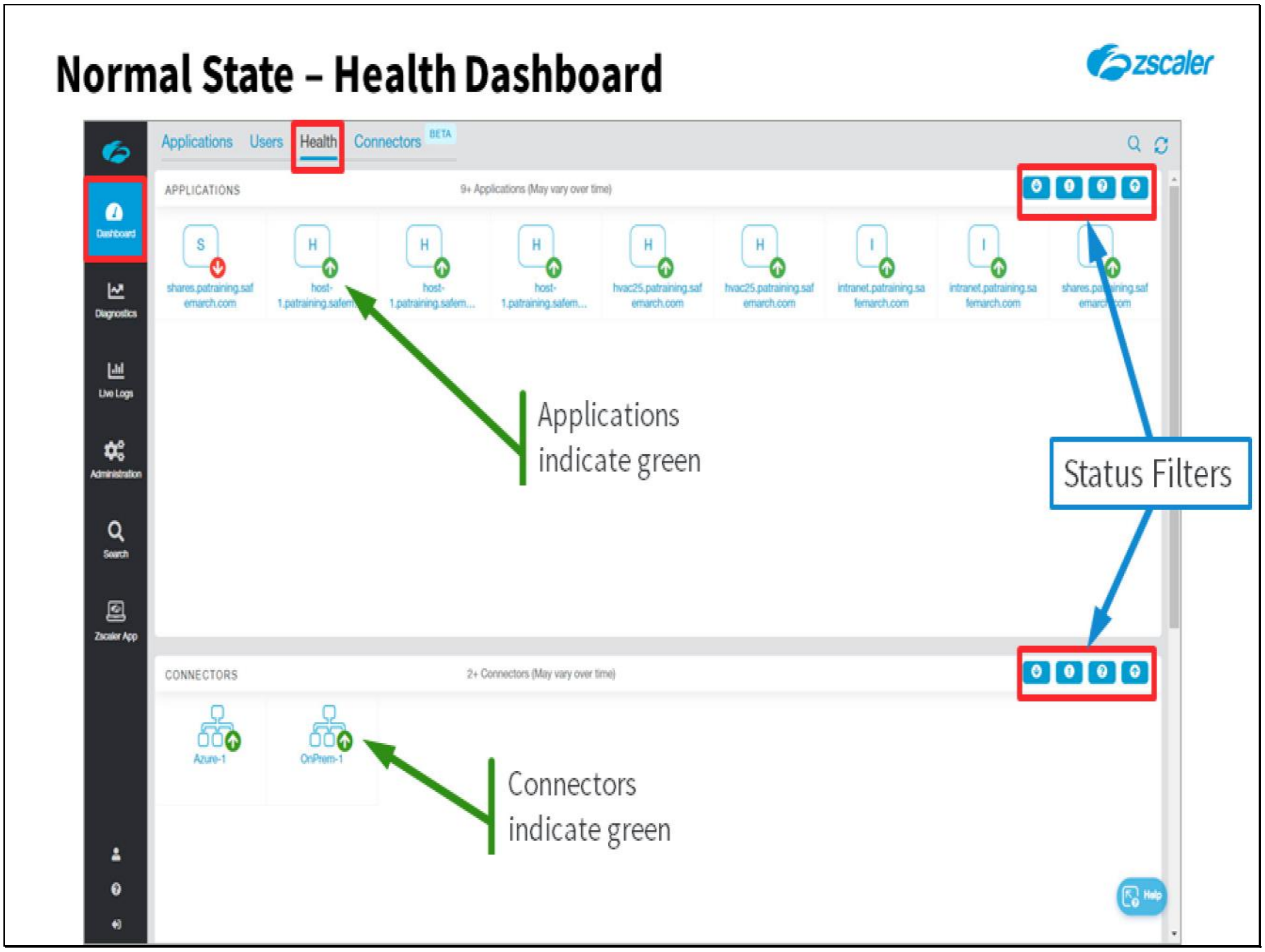
USERS BLOCKED BY POLICIES

zscaler
Applications
Users
Health
Connectors
BETA
14 Days
Dashboard
Diagnostics
Live Logs
Administration
Search
Zscaler App
RECENT USERS
3
CURRENT CONNECTED USERS
2
TOP POLICY BLOCKS
33
RECENT USERS
student@patraining35.safemarch.com
hvac@patraining35.safemarch.com
smadmin@patraining35.safemarch.com
CURRENT CONNECTED USERS
ZPA LSS Client
student@patraining35.safemarch.com
USERS BLOCKED BY POLICIES
23 hvac@patraining35.safemarch.com
10 student@patraining35.safemarch.com
TOP USERS BY APPLICATIONS
ZPA LSS
hvac
TOP USERS BY BANDWIDTH
15.28 MB ZPA LSS Client
8.87 MB student@patraining35.safemarch.com
1.00 MB smadmin@patraining35.safemarch.com
194.12 KB hvac@patraining35.safemarch.com
TOP POLICIES BY BLOCKED USERS
Bloc
Help

Slide notes

On the **Users** Dashboard, you can view lists and statistics on the currently connected, and recently connected users, including, if applicable, the **USERS BLOCKED BY POLICIES**.

Slide 12 - Normal State – Health Dashboard



Normal State – Health Dashboard

Applications indicate green

Status Filters

Connectors indicate green

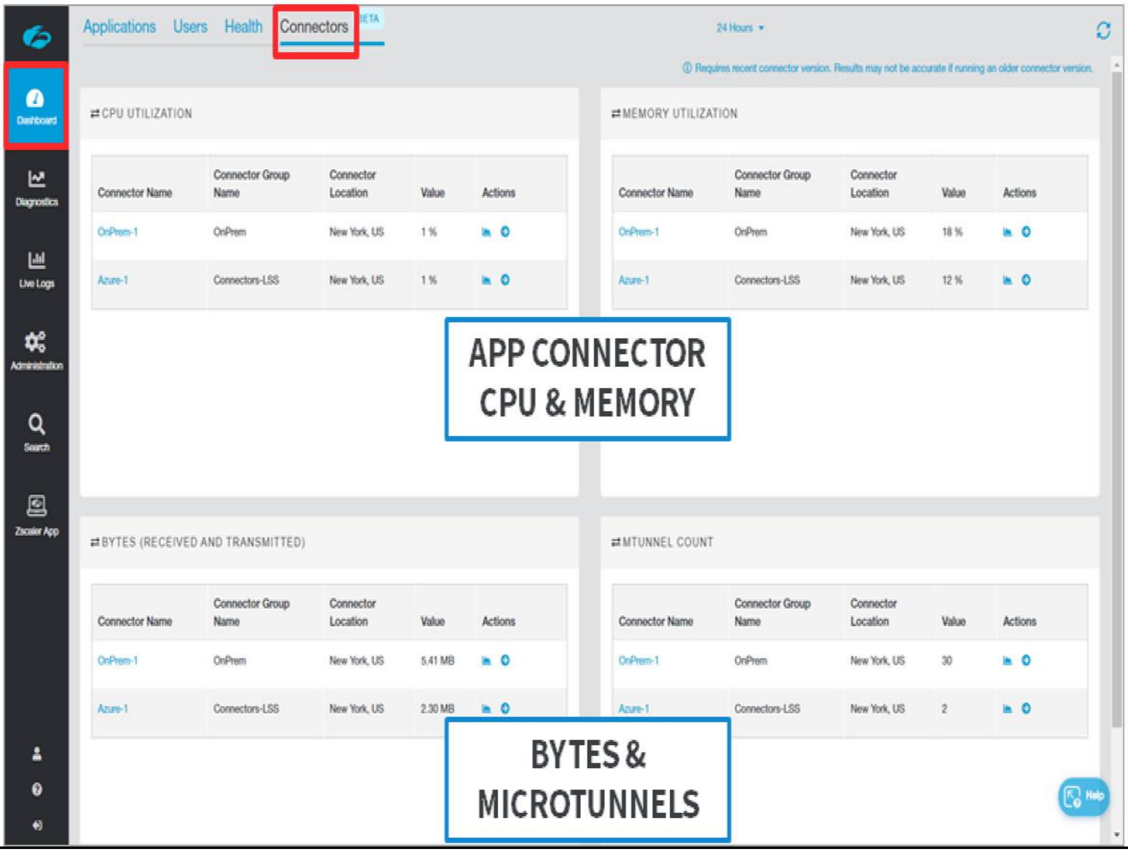
zscaler
Applications
Users
Health
Connectors
BETA
Dashboard
Diagnostics
Live Logs
Administration
Search
Zscaler App
APPLICATIONS
9+ Applications (May vary over time)
shares.patraining.safemarch.com
host-1.patraining.safem...
host-1.patraining.safem...
host-1.patraining.safem...
hvac25.patraining.safemarch.com
hvac25.patraining.safemarch.com
intranet.patraining.safemarch.com
intranet.patraining.safemarch.com
shares.patraining.safemarch.com
CONNECTORS
2+ Connectors (May vary over time)
Azure-1
OnPrem-1
Help

Slide notes

The **Health** Dashboard gives you an overview of the current state of all of your infrastructure components; APPLICATIONS, SERVERS, and CONNECTORS. Filters are available to allow you to quickly display those components that are in the **Down**, **Unhealthy**, or **Unknown** states.

Slide 13 - Normal State – Connectors Dashboard

Normal State – Connectors Dashboard



ⓘ Requires recent connector version. Results may not be accurate if running an older connector version.

CPU UTILIZATION

Connector Name	Connector Group Name	Connector Location	Value	Actions
OnPrem-1	OnPrem	New York, US	1 %	
Azure-1	Connectors-LSS	New York, US	1 %	

MEMORY UTILIZATION

Connector Name	Connector Group Name	Connector Location	Value	Actions
OnPrem-1	OnPrem	New York, US	18 %	
Azure-1	Connectors-LSS	New York, US	12 %	

APP CONNECTOR CPU & MEMORY

BYTES (RECEIVED AND TRANSMITTED)

Connector Name	Connector Group Name	Connector Location	Value	Actions
OnPrem-1	OnPrem	New York, US	5.41 MB	
Azure-1	Connectors-LSS	New York, US	2.30 MB	

MTUNNEL COUNT

Connector Name	Connector Group Name	Connector Location	Value	Actions
OnPrem-1	OnPrem	New York, US	30	
Azure-1	Connectors-LSS	New York, US	2	

BYTES & MICROTUNNELS

Slide notes

The **Connectors** Dashboard lists the busiest App Connectors within a selected timeframe, based on **CPU** and **Memory** utilization, **Bytes transmitted and received** and the number of application-specific Microtunnels (**Mtunnels)**.

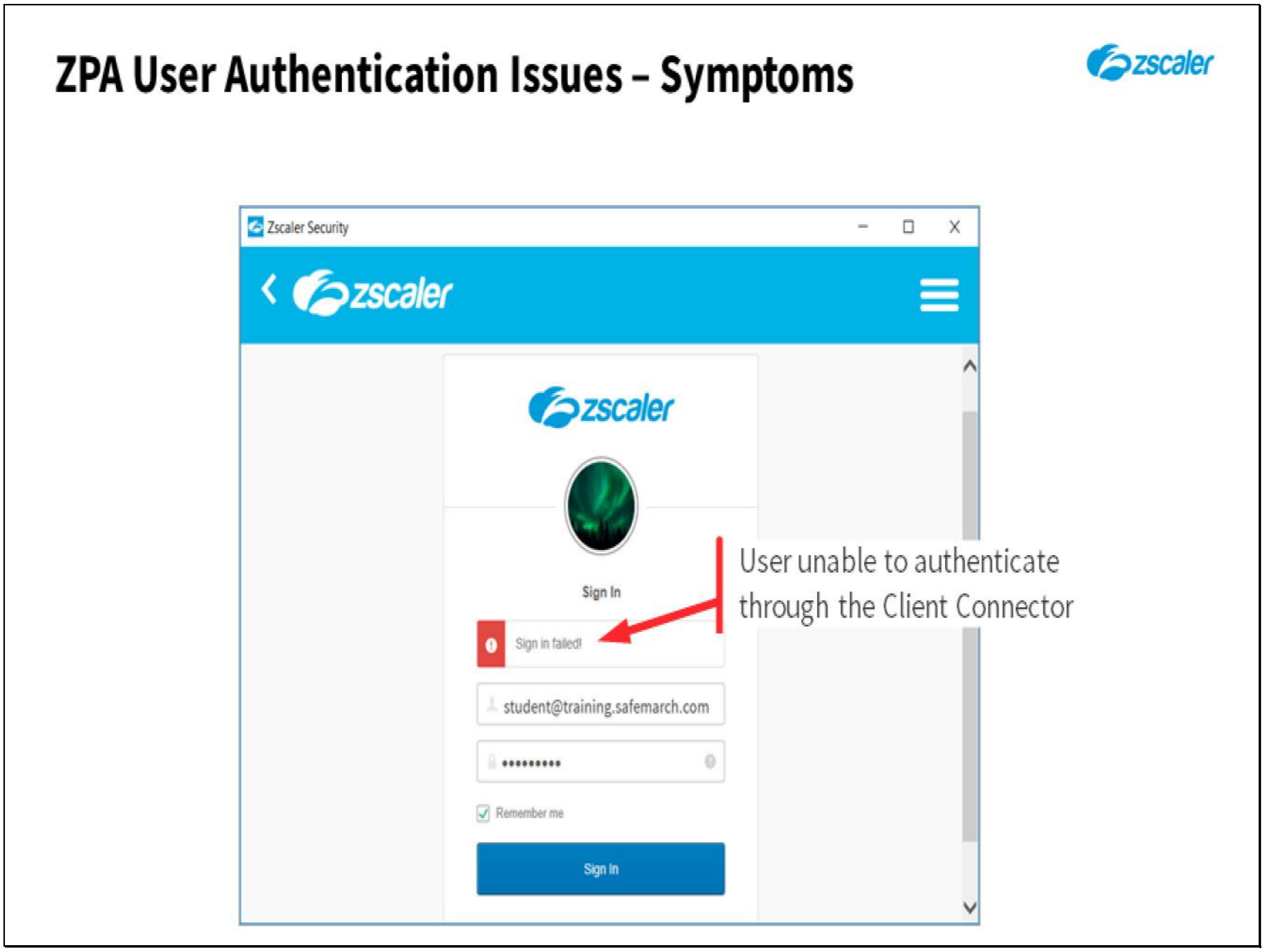
Slide 14 - ZPA User Authentication Issues

ZPA User Authentication Issues

Slide notes

In the next section, we will look at symptoms and possible causes for when a ZPA user is unable to authenticate.

Slide 15 - ZPA User Authentication Issues – Symptoms



ZPA User Authentication Issues – Symptoms

Sign in failed!

student@training.safemarch.com

•••••••••

User unable to authenticate through the Client Connector

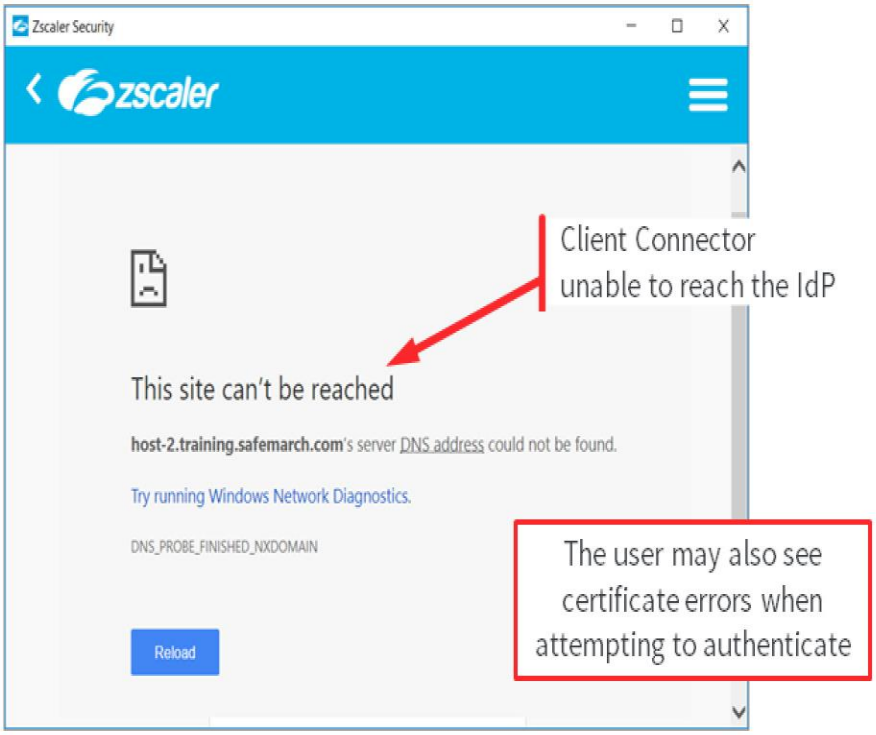
Slide notes

It is important to note that end user authentication issues will be identical for both Browser Access and Zscaler Client Connector users.

If the user is unable to authenticate with a ‘Sign in failed’ error (or similar), this usually indicates a simple username, or password problem. Either the user is not providing the correct password, or the username is unknown to the IdP. This is most likely to be simple end user error, although it may also be caused by account provisioning or synchronization issues.

Slide 16 - ZPA User Authentication Issues – Symptoms

ZPA User Authentication Issues – Symptoms



This site can't be reached

host-2.training.safemarch.com's server DNS address could not be found.

Try running Windows Network Diagnostics.

DNS_PROBE_FINISHED_NXDOMAIN

Client Connector unable to reach the IdP

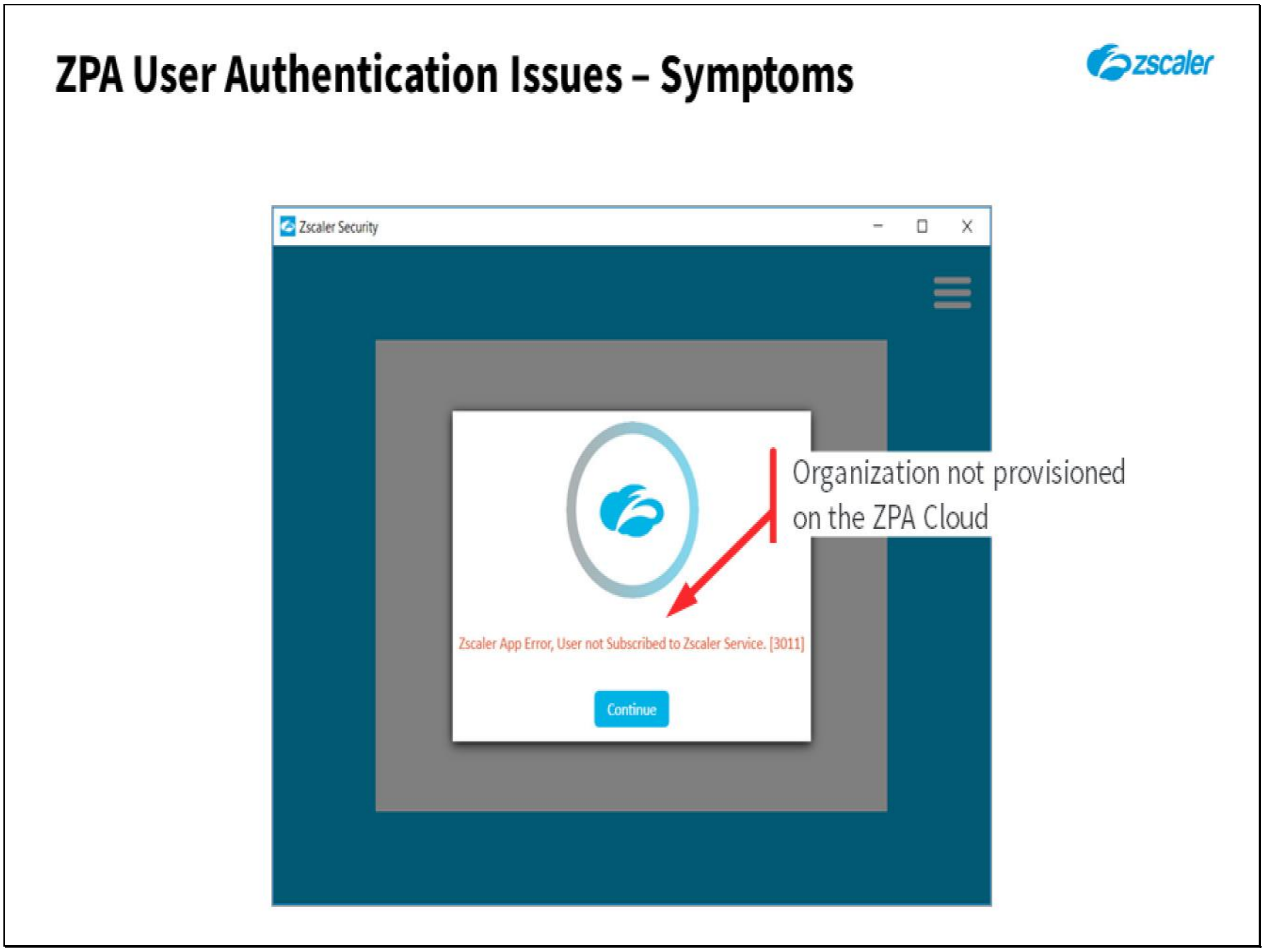
The user may also see certificate errors when attempting to authenticate

Slide notes

If a user sees an DNS error or '404' page while authenticating, this indicates that the IdP login page cannot be reached. This could be due to a bad IdP configuration at the ZPA admin portal, or more likely is an accessibility problem from the network that the user is connected to; a DNS configuration is preventing the resolution of the hostname, or a firewall is blocking access to it.

Alternatively, the end user may be able to reach the destination service, but a certificate error is displayed that prevents authentication. This could be due to a bad certificate on the IdP (in which case everyone will be affected), or it could indicate that some intermediate system is attempting to do SSL inspection of the Zscaler Client Connector traffic.

Slide 17 - ZPA User Authentication Issues – Symptoms



ZPA User Authentication Issues – Symptoms

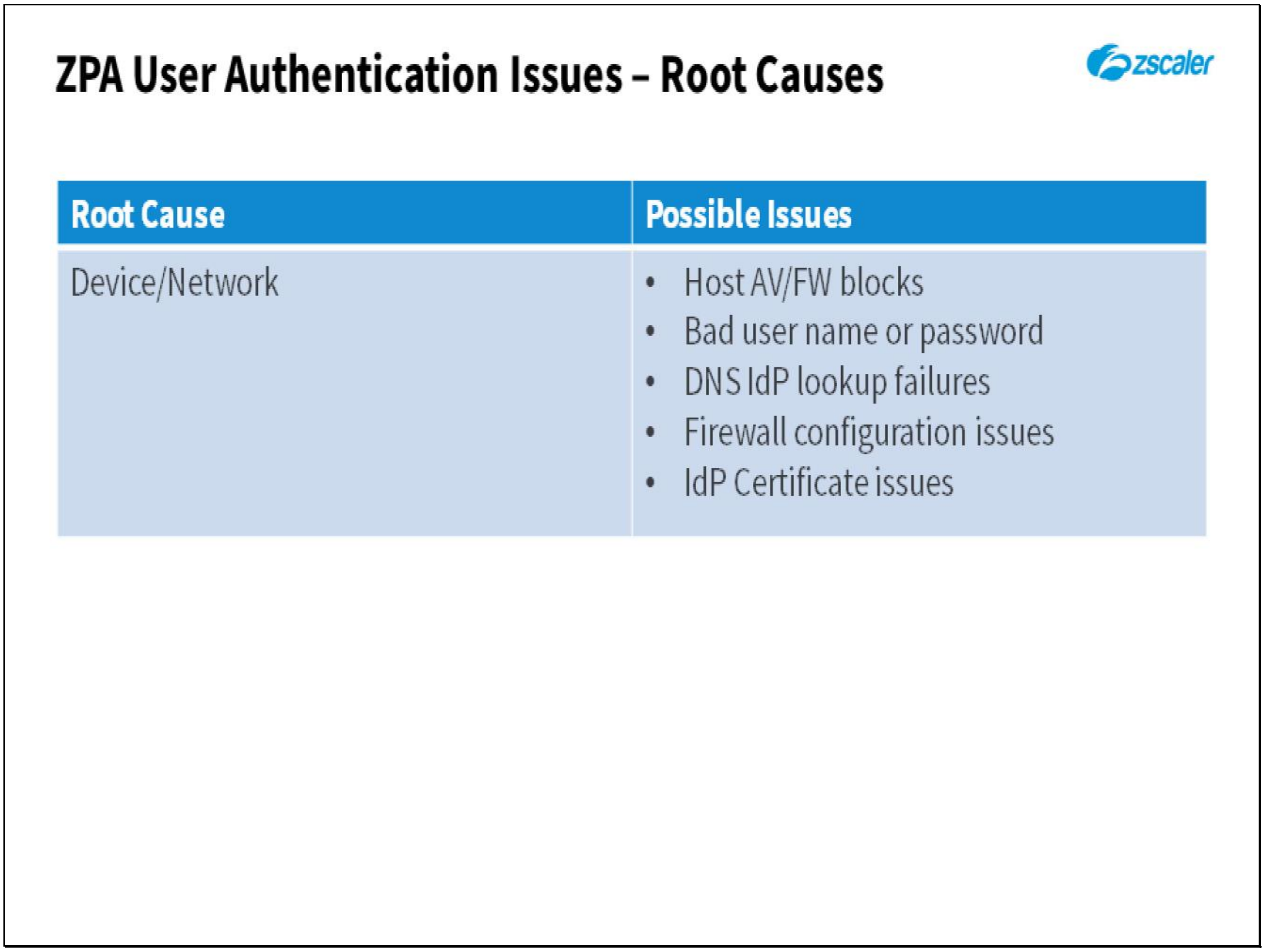
Zscaler App Error, User not Subscribed to Zscaler Service. [3011]

Organization not provisioned on the ZPA Cloud

Slide notes

If the end user sees a ‘User not subscribed to Zscaler Service’ error, this probably indicates a provisioning problem that should be escalated to Zscaler.

Slide 18 - ZPA User Authentication Issues – Root Causes



ZPA User Authentication Issues – Root Causes

Root Cause	Possible Issues
Device/Network	• Host AV/FW blocks • Bad user name or password • DNS IdP lookup failures • Firewall configuration issues • IdP Certificate issues

Slide notes

There are three main root causes for an inability of the end user to authenticate into Zscaler, and the first root cause that we will look at is ‘Device/Network Issues’. There are a number of potential problems with the end user device, or the network it is connected to that may prevent a successful authentication, some possibilities are listed here:

- An Antivirus client, or Personal Firewall on the end user device may interfere with authentication traffic, check that the necessary white-listing, and ‘allow’ rules have been added.

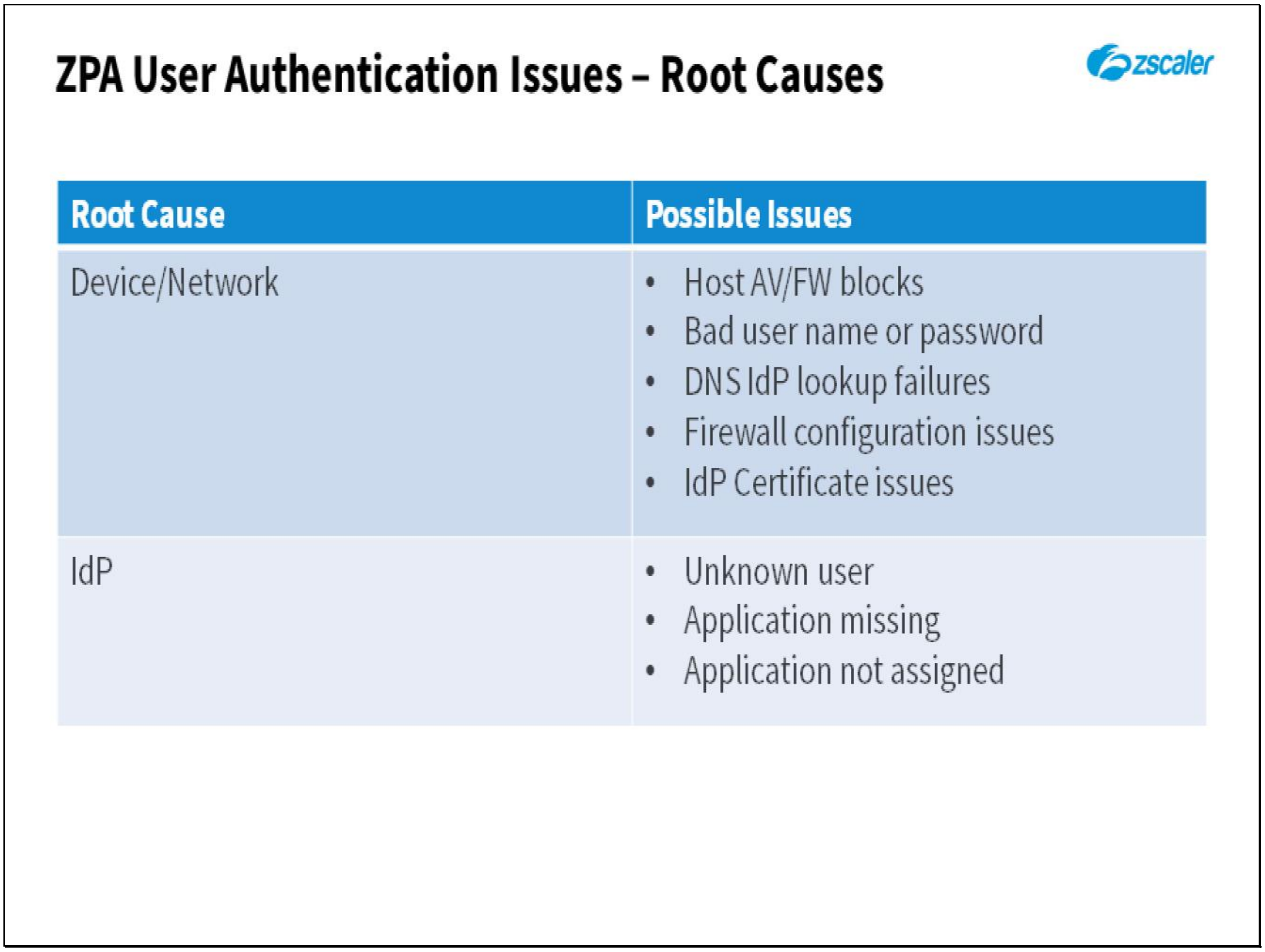
- The end user may simply have entered a bad username or password, have them verify their account details, and if necessary check the directory server, or force a password update.

- The DNS server on the network may not be able to resolve the IdP FQDN, making it unreachable. In this case, check the local networks DNS environment for potential problems.

- Even if the DNS server resolves the IdP host, a firewall configuration may still make it unreachable. Check the firewall for ACLs or filters they may block access to the IdP.

- The end user may be able to reach the IdP, but is unable to authenticate due to certificate issues. This may be a problem with the certificate on the IdP, or more likely, it may indicate that some appliance or service is attempting to inspect SSL traffic.

Slide 19 - ZPA User Authentication Issues – Root Causes



ZPA User Authentication Issues – Root Causes

Root Cause	Possible Issues
Device/Network	• Host AV/FW blocks • Bad user name or password • DNS IdP lookup failures • Firewall configuration issues • IdP Certificate issues
IdP	• Unknown user • Application missing • Application not assigned

Slide notes

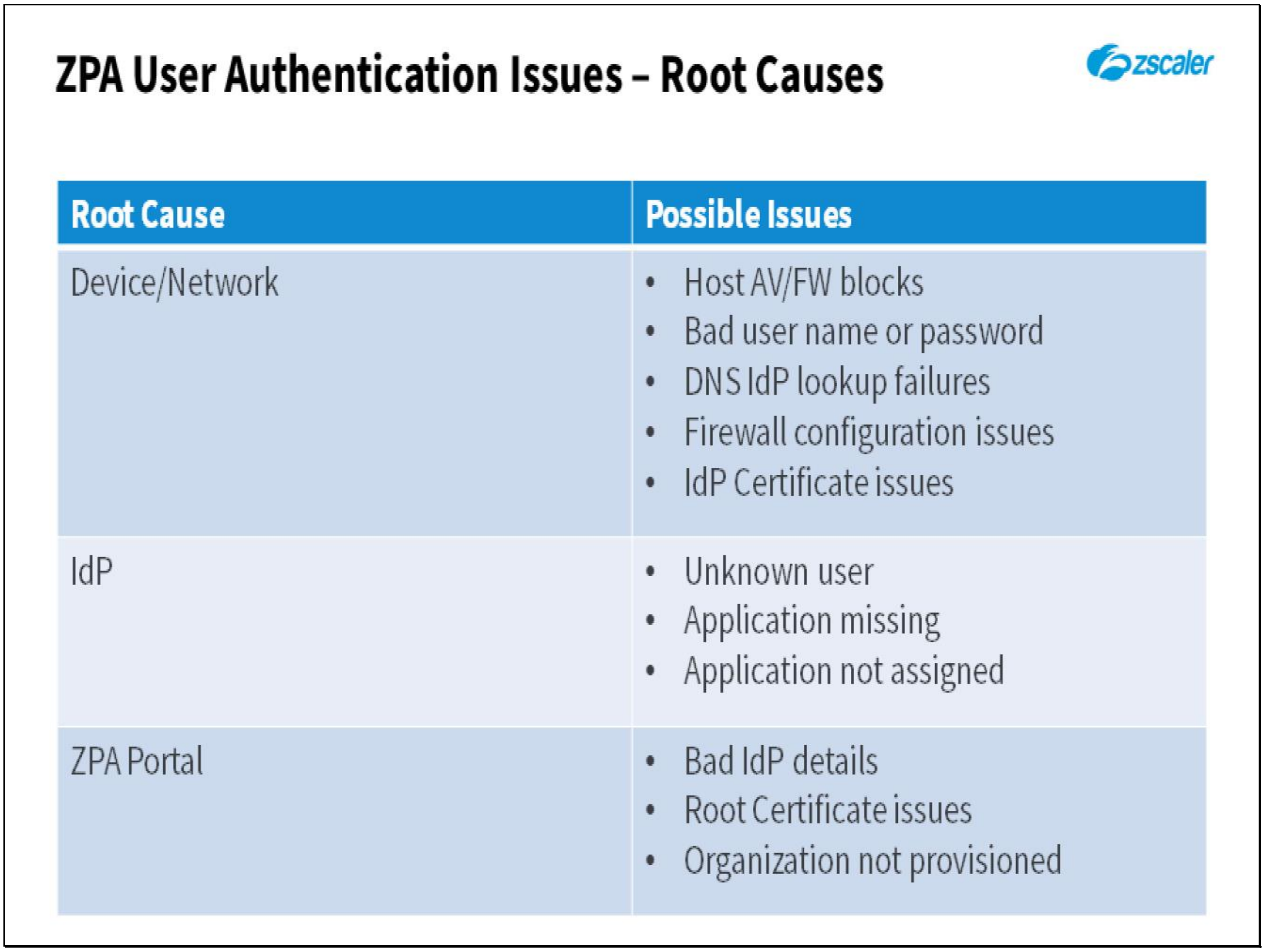
Possible ‘IdP’ issues include:

- The end user may not be known to the IdP. Depending on how the IdP is set up, this could be caused by directory synchronization, or update issues. Force a manual sync of the directory (if appropriate) and check whether that user is now populated to the IdP.

- The IdP must be configured to accept access requests from specific ‘Service Providers’ (’Relying Parties’ in the Microsoft World), aka ‘Applications’. Check that Zscaler Private Access is correctly set up in the IdP as a valid Application.

- Typically, the Application must also be assigned to users or groups within the IdP, check that this has been done for the user in question.

Slide 20 - ZPA User Authentication Issues – Root Causes



ZPA User Authentication Issues – Root Causes

Root Cause	Possible Issues
Device/Network	• Host AV/FW blocks • Bad user name or password • DNS IdP lookup failures • Firewall configuration issues • IdP Certificate issues
IdP	• Unknown user • Application missing • Application not assigned
ZPA Portal	• Bad IdP details • Root Certificate issues • Organization not provisioned

Slide notes

Finally, for potential authentication issues, we will look at possible ‘ZPA Portal Issues’:

- There could be problems with the IdP configuration on the ZPA admin portal. Use the **Import** option in the IdP Configuration screen to confirm that you can successfully authenticate with a valid user.

- A related issue, the certificate on the IdP may be invalid, possibly it has been allowed to expire. Validate the certificate during your test, and refresh it if necessary.

- It may be that the end user’s organization has not yet been provisioned for ZPA access, this will require a support escalation with Zscaler.

Slide 21 - ZPA Admin Portal Misconfigurations

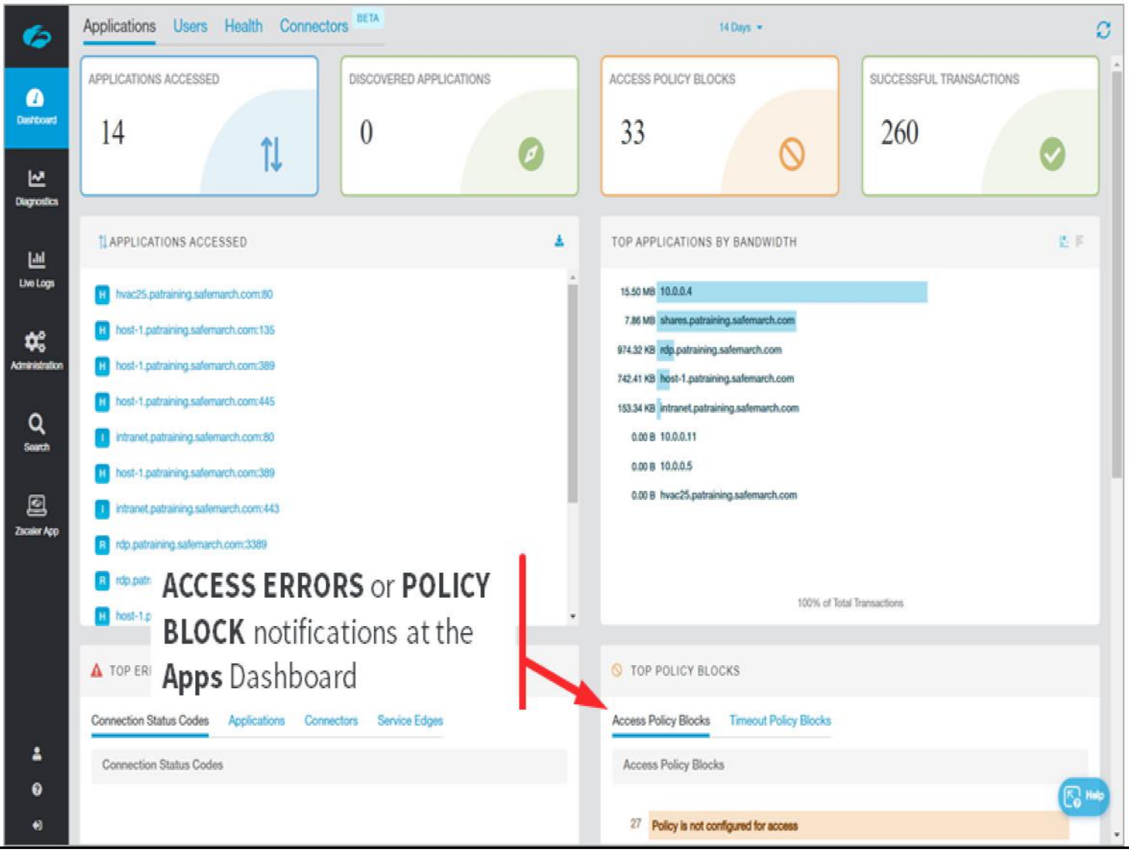
ZPA Admin Portal Misconfigurations

Slide notes

In the next section, we will look at symptoms and possible causes for when there are ZPA admin portal misconfigurations.

Slide 22 - ZPA Admin Portal Misconfigurations – Symptoms

ZPA Admin Portal Misconfigurations – Symptoms



APPLICATIONS ACCESSED 14

DISCOVERED APPLICATIONS 0

ACCESS POLICY BLOCKS 33

SUCCESSFUL TRANSACTIONS 260

APPLICATIONS ACCESSED

- H hvac25.patraining.safemarch.com:80
- H host-1.patraining.safemarch.com:135
- H host-1.patraining.safemarch.com:389
- H host-1.patraining.safemarch.com:445
- I intranet.patraining.safemarch.com:80
- H host-1.patraining.safemarch.com:389
- I intranet.patraining.safemarch.com:443
- R rdp.patraining.safemarch.com:3389
- R rdp.patr
- H host-1.p

TOP APPLICATIONS BY BANDWIDTH

15.50 MB	10.0.0.4
7.86 MB	shares.patraining.safemarch.com
974.32 KB	rdp.patraining.safemarch.com
742.41 KB	host-1.patraining.safemarch.com
153.34 KB	intranet.patraining.safemarch.com
0.00 B	10.0.0.11
0.00 B	10.0.0.5
0.00 B	hvac25.patraining.safemarch.com

100% of Total Transactions

TOP ERI

Connection Status Codes | Applications | Connectors | Service Edges

Connection Status Codes

TOP POLICY BLOCKS

Access Policy Blocks | Timeout Policy Blocks

Access Policy Blocks

27 Policy is not configured for access

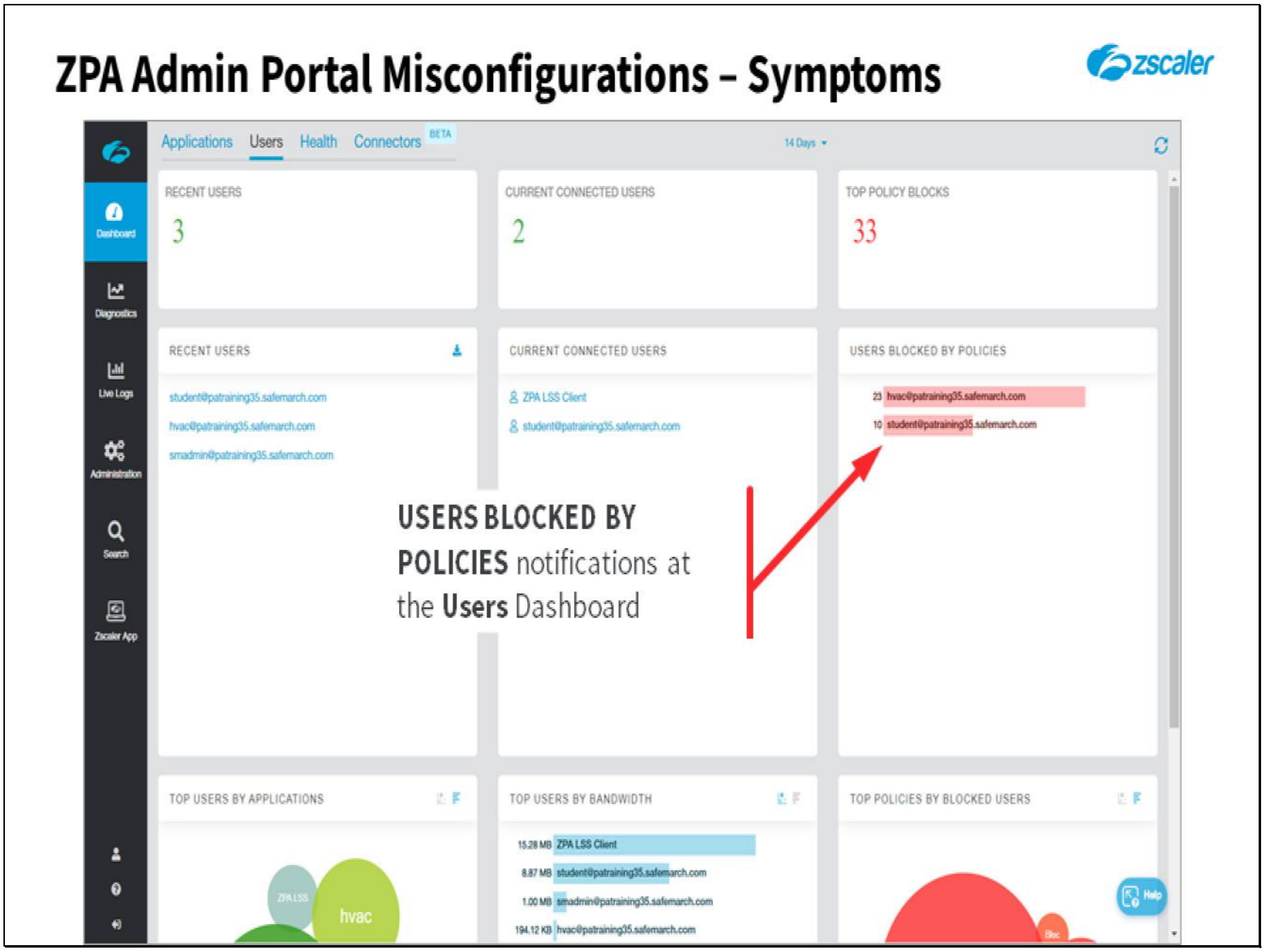
ACCESS ERRORS or **POLICY BLOCK** notifications at the **Apps** Dashboard

Slide notes

Symptoms you may see that indicate misconfigurations at the ZPA admin portal, can include ‘ACCESS ERRORS’ or ‘POLICY BLOCKS’ indicated on the **Applications** Dashboard.

These policy blocks may be legitimate blocks due to unauthorized user access requests, or they may indicate an incorrect policy configuration. Drill down to the **Diagnostic** information for each of the errors to understand the root cause.

Slide 23 - ZPA Admin Portal Misconfigurations – Symptoms



ZPA Admin Portal Misconfigurations – Symptoms

RECENT USERS 3

CURRENT CONNECTED USERS 2

TOP POLICY BLOCKS 33

RECENT USERS

student@patraining35.safemarch.com
hvac@patraining35.safemarch.com
smadmin@patraining35.safemarch.com

CURRENT CONNECTED USERS

ZPA LSS Client
student@patraining35.safemarch.com

USERS BLOCKED BY POLICIES

23 hvac@patraining35.safemarch.com
10 student@patraining35.safemarch.com

TOP USERS BY APPLICATIONS

TOP USERS BY BANDWIDTH

15.28 MB ZPA LSS Client
8.87 MB student@patraining35.safemarch.com
1.00 MB smadmin@patraining35.safemarch.com
194.12 KB hvac@patraining35.safemarch.com

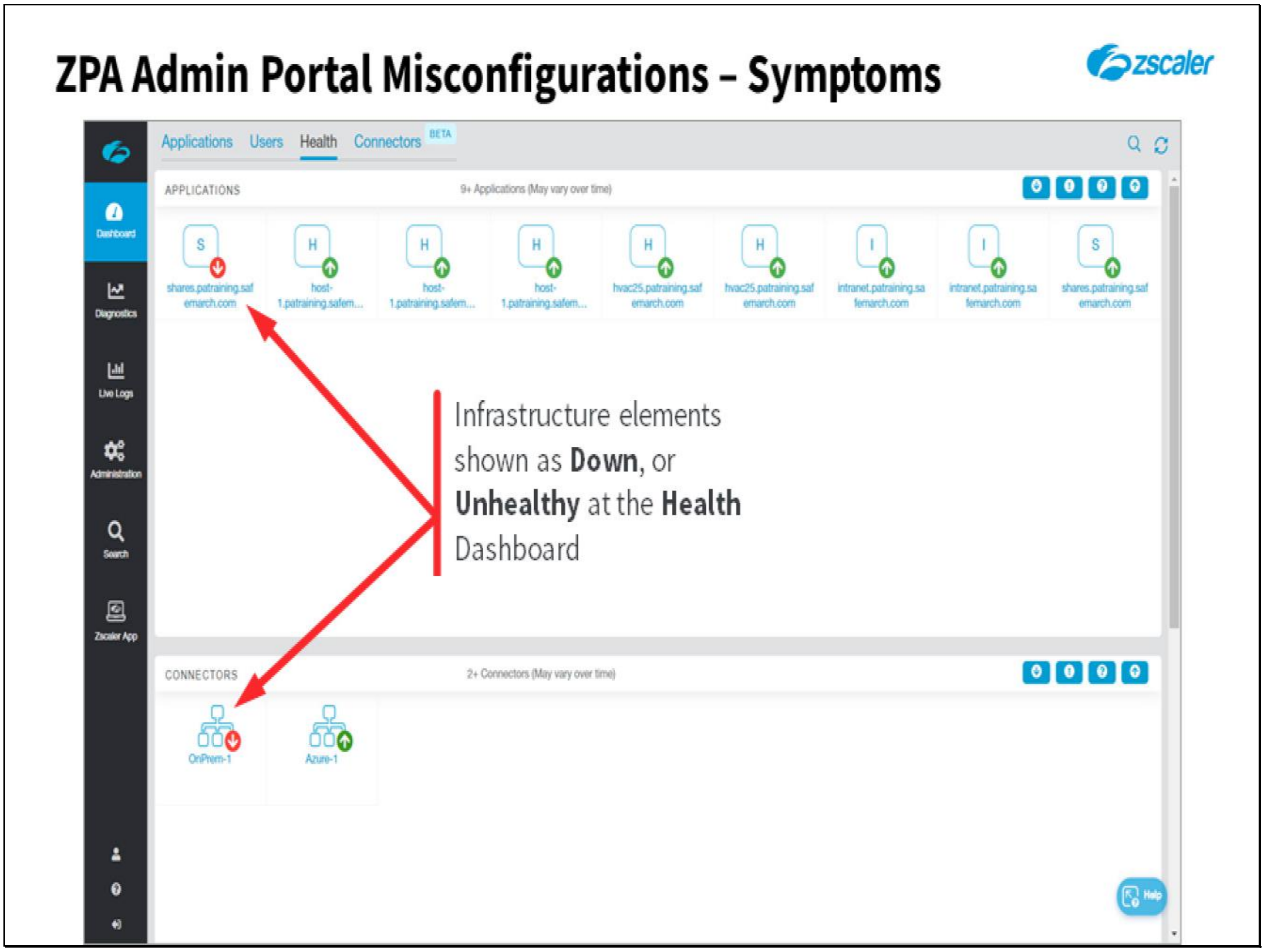
TOP POLICIES BY BLOCKED USERS

USERS BLOCKED BY POLICIES notifications at the **Users** Dashboard

Slide notes

Similarly, you may see ‘USERS BLOCKED BY POLICIES’ notifications in the **Users** Dashboard. Once again, these may be legitimate blocks, or could be due to a bad policy configuration. Use the drill down capability to better understand what is going on for each case.

Slide 24 - ZPA Admin Portal Misconfigurations – Symptoms



ZPA Admin Portal Misconfigurations – Symptoms

Infrastructure elements shown as **Down**, or **Unhealthy** at the **Health** Dashboard

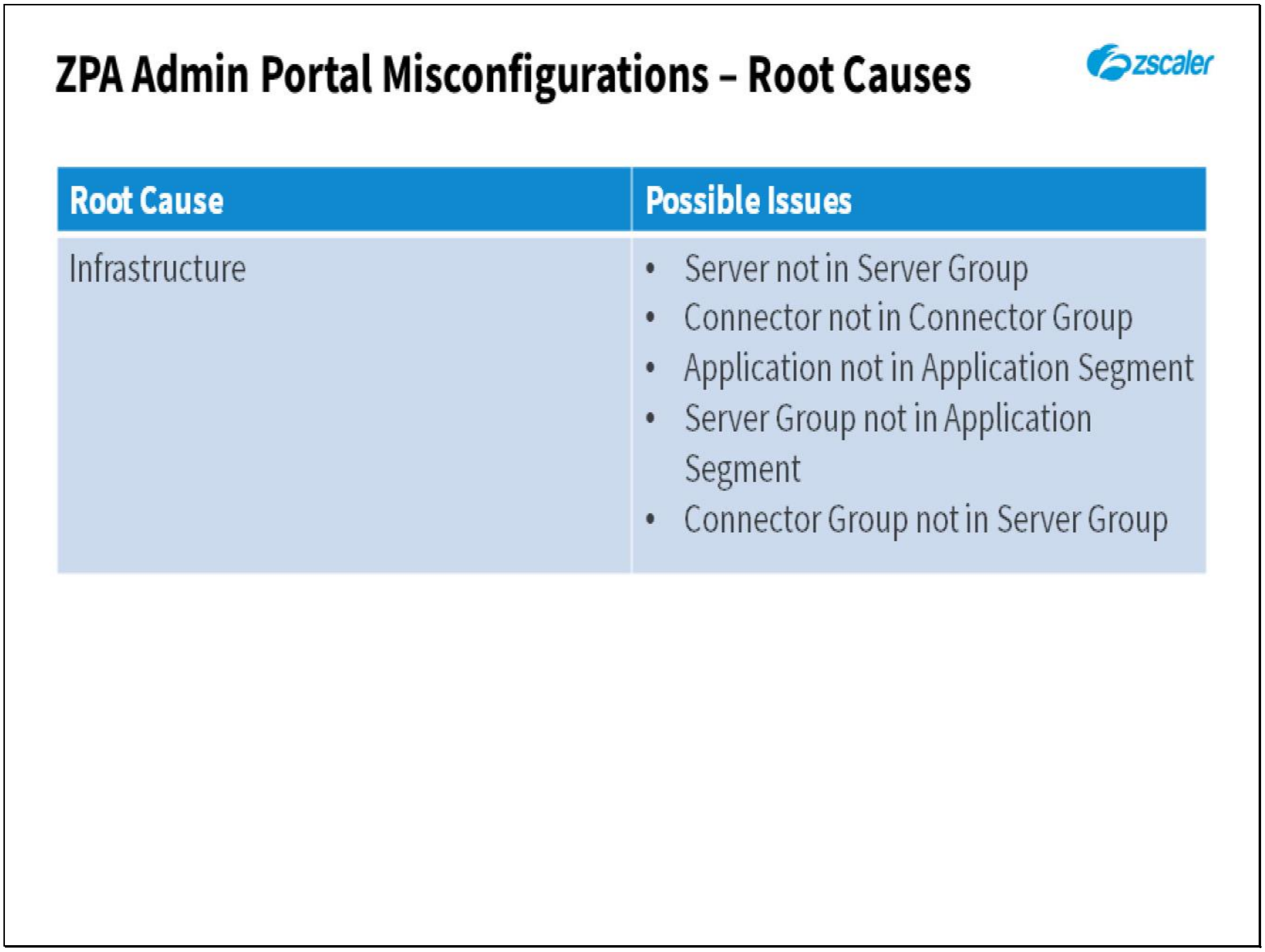
zscaler
Applications
Users
Health
Connectors
BETA
Dashboard
Diagnostics
Live Logs
Administration
Search
Zscaler App
APPLICATIONS
9+ Applications (May vary over time)
S
shares.patraining.safemarch.com
H
host-1.patraining.safem...
H
host-1.patraining.safem...
H
host-1.patraining.safem...
H
hvac25.patraining.safemarch.com
H
hvac25.patraining.safemarch.com
I
intranet.patraining.safemarch.com
I
intranet.patraining.safemarch.com
S
shares.patraining.safemarch.com
CONNECTORS
2+ Connectors (May vary over time)
OnPrem-1
Azure-1
Help

Slide notes

Another possible symptom of a misconfiguration could be a **Down**, or **Unhealthy** status notification for your infrastructure components; ‘APPLICATIONS’, ‘SERVERS’, and ‘CONNECTORS’. Review the status of your infrastructure at the **Health** Dashboard, and review configurations as necessary.

Plus of course, end users will be complaining of an inability to access their applications!

Slide 25 - ZPA Admin Portal Misconfigurations – Root Causes



ZPA Admin Portal Misconfigurations – Root Causes

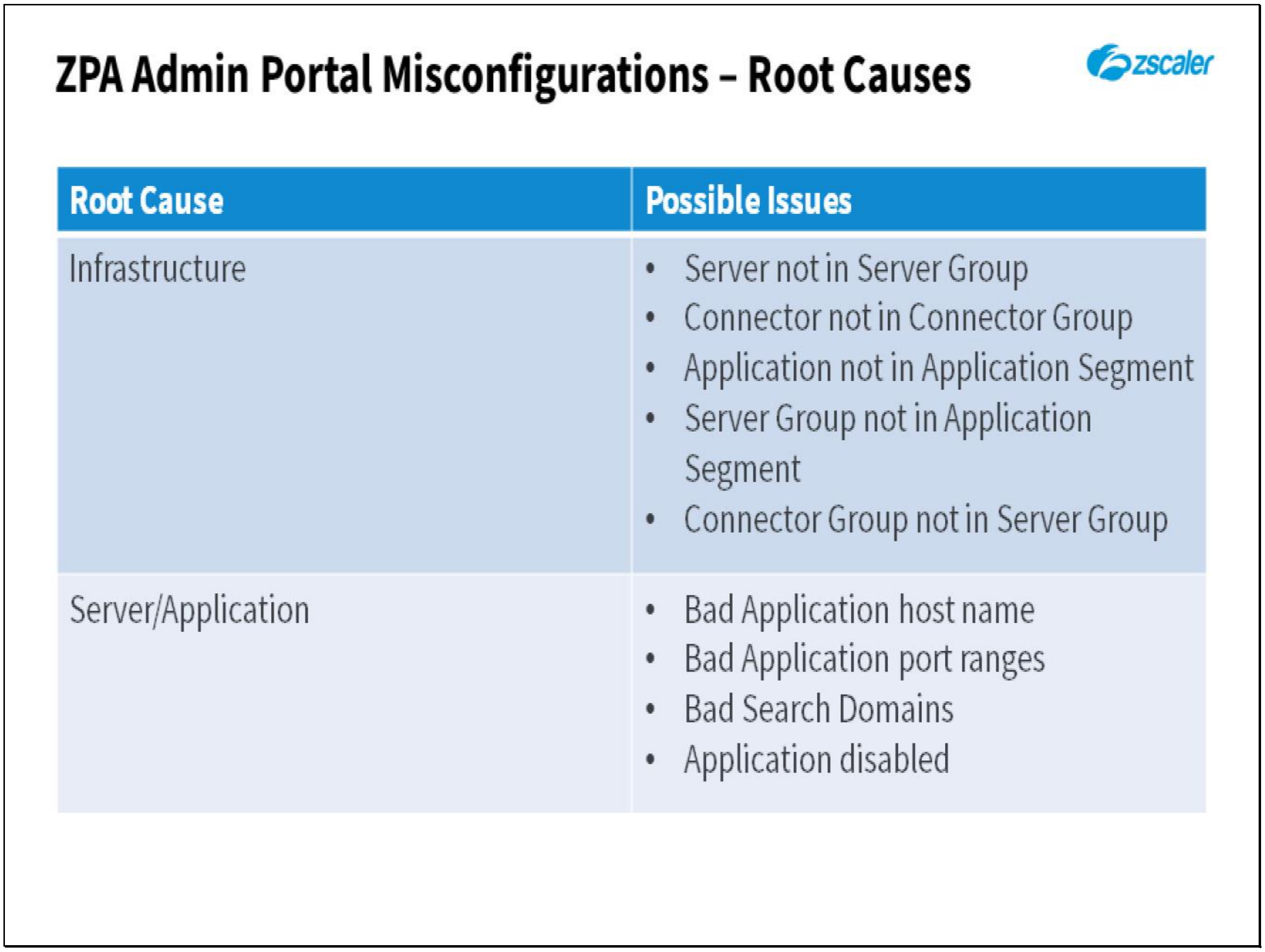
Root Cause	Possible Issues
Infrastructure	• Server not in Server Group • Connector not in Connector Group • Application not in Application Segment • Server Group not in Application Segment • Connector Group not in Server Group

Slide notes

The ‘Infrastructure Issues’ root cause, largely has to do with missing group memberships. For example:

- The relevant ‘Server’ may not be a member of the correct ‘Server Group’;
- The App Connector adjacent to the application, may not be in the correct ‘Connector Group’;
- The Application itself may not be in the correct ‘Application Segment’;
- The applicable Server Group may not be selected in the Application Segment;
- Or the relevant ‘Connector Group’ may not be selected in the ‘Server Group’.
- Review all your group memberships carefully to ensure all configurations are valid.

Slide 26 - ZPA Admin Portal Misconfigurations – Root Causes



ZPA Admin Portal Misconfigurations – Root Causes

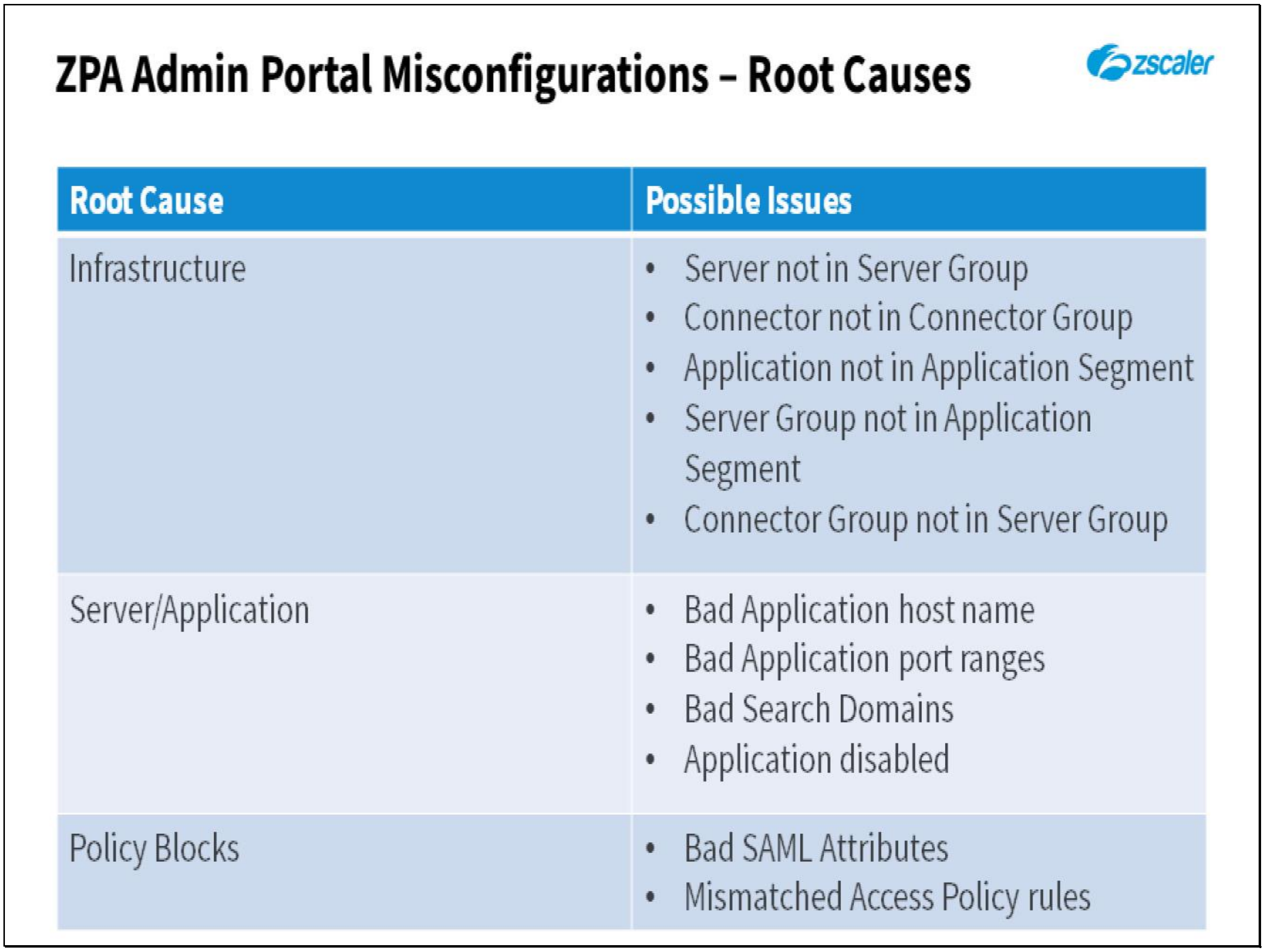
Root Cause	Possible Issues
Infrastructure	• Server not in Server Group • Connector not in Connector Group • Application not in Application Segment • Server Group not in Application Segment • Connector Group not in Server Group
Server/Application	• Bad Application host name • Bad Application port ranges • Bad Search Domains • Application disabled

Slide notes

For ‘Server/Application Issues’:

- The hostname specified for an individual application may be incorrect;
- Or, the port range specified for it may be in error. Check the configuration for each application carefully.
- The ‘Search Domains’ configuration for the organization may be incorrect, and users are requesting an application by hostname that is not matched to a valid FQDN. Review the **DNS Search Domains** configuration on the **Administration > Application Management > Application Segments** page to ensure it is correct and complete.
- Or, it may simply be that the application is disabled. Check whether there is good reason for it to be in that state, and if possible enable it.

Slide 27 - ZPA Admin Portal Misconfigurations – Root Causes



ZPA Admin Portal Misconfigurations – Root Causes

Root Cause	Possible Issues
Infrastructure	• Server not in Server Group • Connector not in Connector Group • Application not in Application Segment • Server Group not in Application Segment • Connector Group not in Server Group
Server/Application	• Bad Application host name • Bad Application port ranges • Bad Search Domains • Application disabled
Policy Blocks	• Bad SAML Attributes • Mismatched Access Policy rules

Slide notes

For the 'Policy Blocks' root cause, you will need to check whether any policy blocks are actually legitimate, where a user has attempted to access an application that they are not authorized to use. Misconfigurations here can occur in a number of areas:

- There may be a mismatch in the SAML attributes known to the ZPA system, and those returned by the IdP. Or, there could be a misconfiguration on the IdP in terms of what attribute to map to the 'claim' returned to Zscaler on user authentication. Review the SAML attribute configuration carefully, and create or re-configure attributes as necessary.

- Check the Access Policy Rules. Ensure that both the configuration, and the logic are correct, remembering that rules are read from the top down with a first match algorithm.

- Ensure that the attribute values returned by the user on authentication are actually correct, …so that the policy rule logic can be correctly applied to them.

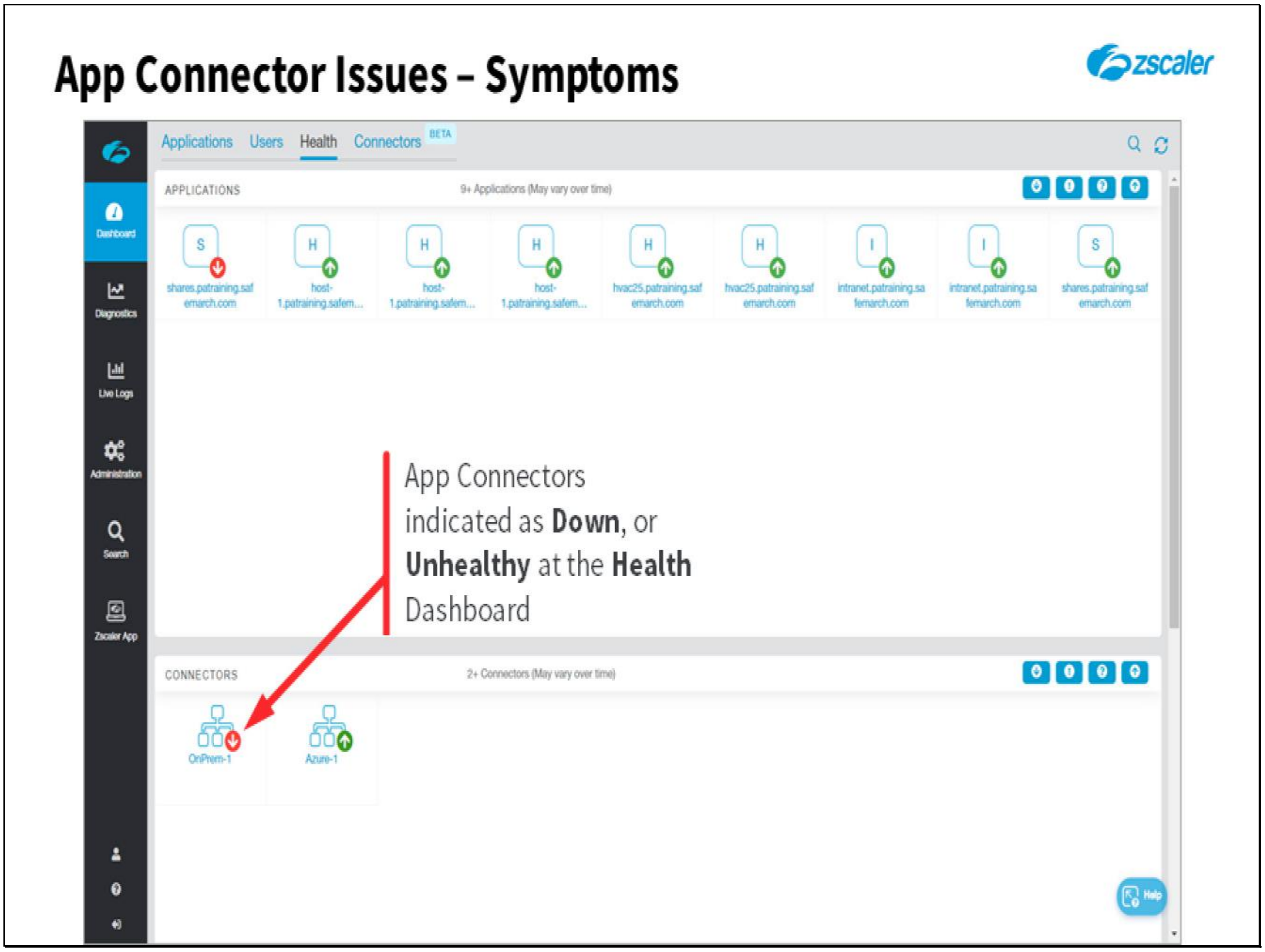
Slide 28 - App Connector Issues

App Connector Issues

Slide notes

In the final section, we will look at symptoms and possible causes for when there are App Connector issues.

Slide 29 - App Connector Issues – Symptoms



App Connector Issues – Symptoms

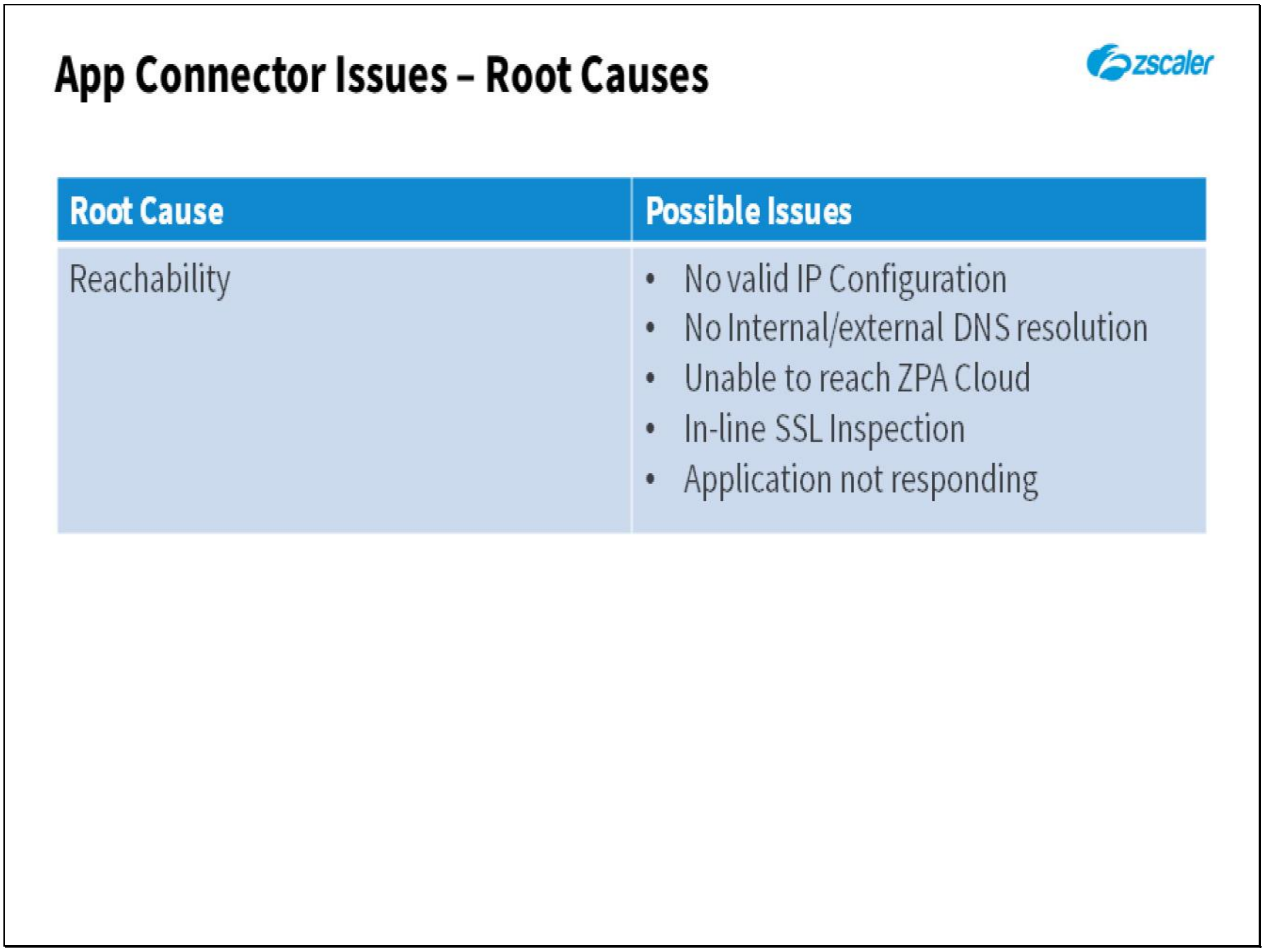
App Connectors indicated as **Down**, or **Unhealthy** at the **Health** Dashboard

zscaler
Applications
Users
Health
Connectors
BETA
Dashboard
Diagnostics
Live Logs
Administration
Search
Zscaler App
APPLICATIONS
9+ Applications (May vary over time)
S
shares.patraining.safemarch.com
H
host-1.patraining.safem...
H
host-1.patraining.safem...
H
host-1.patraining.safem...
H
hvac25.patraining.safemarch.com
H
hvac25.patraining.safemarch.com
I
intranet.patraining.safemarch.com
I
intranet.patraining.safemarch.com
S
shares.patraining.safemarch.com
CONNECTORS
2+ Connectors (May vary over time)
OnPrem-1
Azure-1
Help

Slide notes

The primary symptoms here are that users complain of no application access, and Connectors are shown as being **Down**, or **Unhealthy** in the **Health** Dashboard.

Slide 30 - App Connector Issues – Root Causes



App Connector Issues – Root Causes

Root Cause	Possible Issues
Reachability	• No valid IP Configuration • No Internal/external DNS resolution • Unable to reach ZPA Cloud • In-line SSL Inspection • Application not responding

Slide notes

‘Reachability Issues’ can be caused by the items listed here:

- The Connector host may have a bad IP configuration for the subnet it is connected to. Check that the VM has a properly configure static IP configuration, or enable DHCP for the VM.

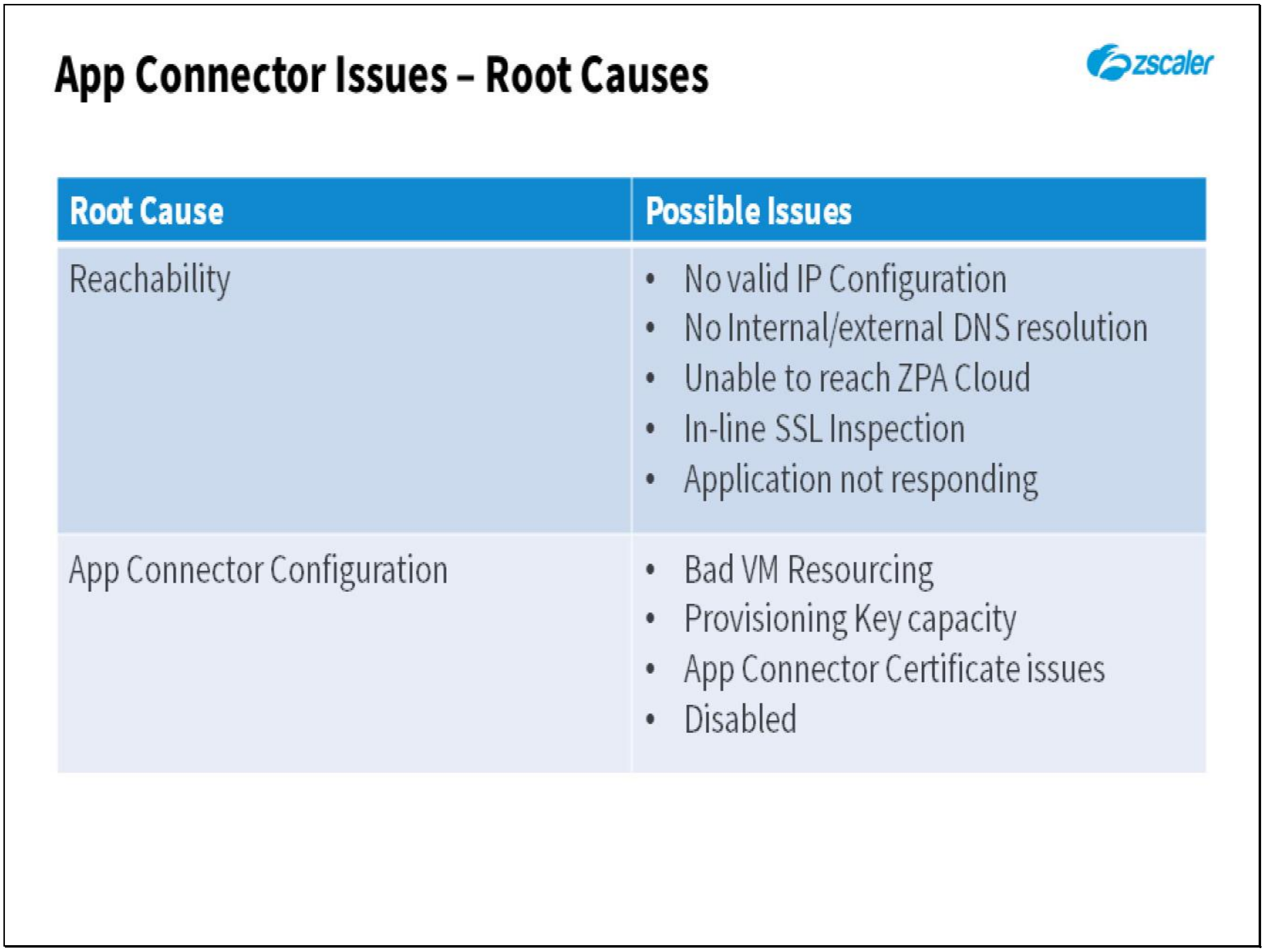
- The DNS environment may be an issue. Check that the Connector (or a host adjacent to it) can successfully resolve both internal and external hosts.

- An outbound firewall may prevent the Connector from reaching the ZPA cloud infrastructure. Ensure that access outbound on port 443 is enabled for the Connector VMs.

- The termination of the outbound connections from a Connector to the ZPA cloud infrastructure for in-line SSL inspection is not supported, so be sure that no appliance or proxy service is attempting to do SSL inspection on these connections.

- The application may be for some reason unreachable, down, or not responding to user requests for various reasons. Check that it is actually available, and accepting connections from valid users.

Slide 31 - App Connector Issues – Root Causes



App Connector Issues – Root Causes

Root Cause	Possible Issues
Reachability	• No valid IP Configuration • No Internal/external DNS resolution • Unable to reach ZPA Cloud • In-line SSL Inspection • Application not responding
App Connector Configuration	• Bad VM Resourcing • Provisioning Key capacity • App Connector Certificate issues • Disabled

Slide notes

And finally, ‘App Connector Configuration’ issues include:

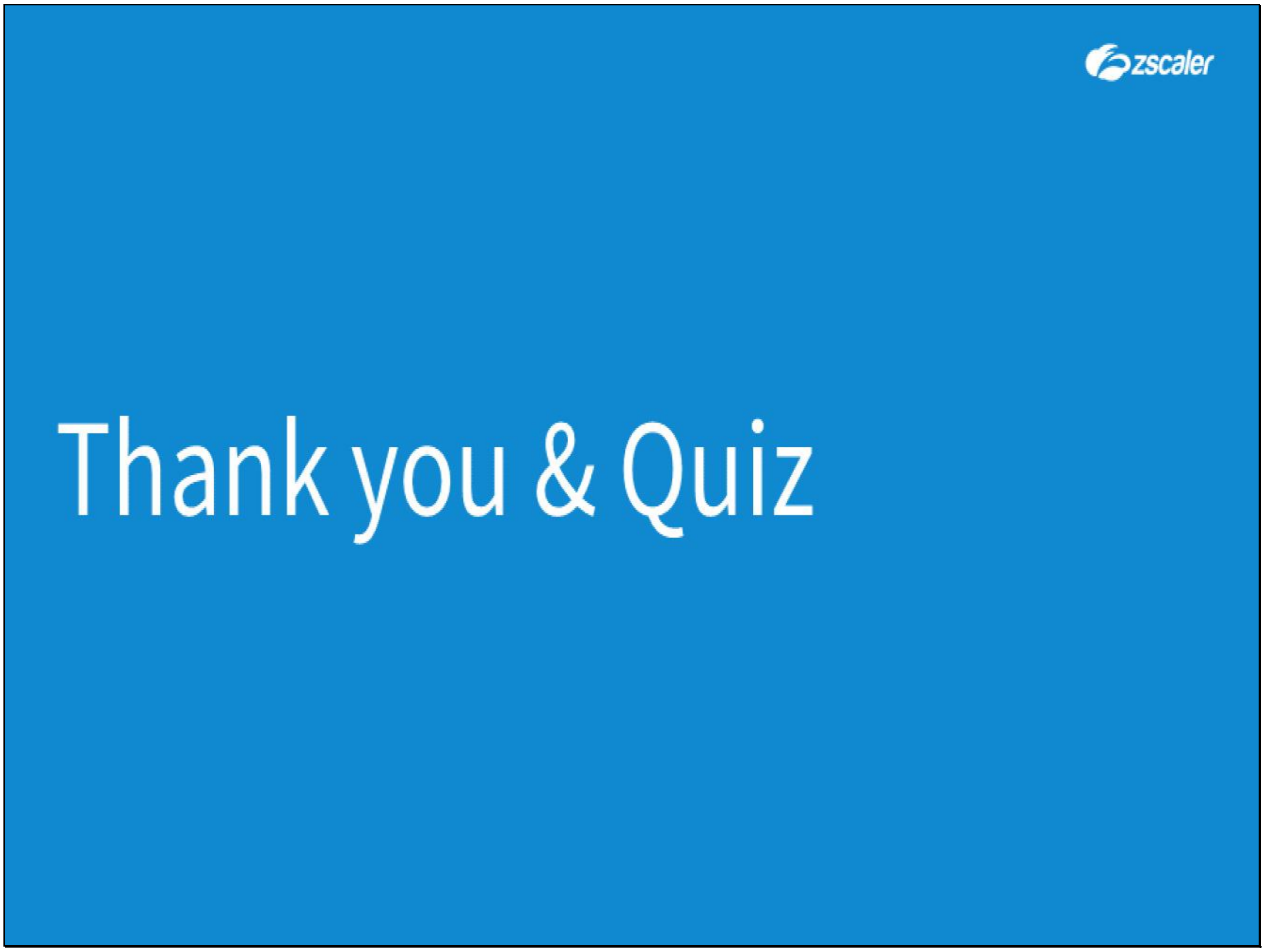
- The Connector VM may have inadequate resources allocated, in terms of CPUs, and RAM, which may cause performance issues. Always ensure that your Connector VMs are properly resourced according to the deployment guidelines.

- Connector ‘Provisioning Keys’ can only be used for the specified number of times. If you are trying to bring up a new Connector and it won’t accept the key, check the ‘Max # Of Connectors’, and the ‘# Of Enrolled Connectors’ on the **Administration > Connector Management > Connector Provisioning Keys** page.

- Ensure that the certificate deployed to the Connector is correct, and still valid.

- Finally, verify that the Connector is enabled!

Slide 32 - Thank you & Quiz



Thank you & Quiz

Slide notes

Thank you for following this training module on problem isolation. 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.