

Slide 1 - Troubleshooting ZPA



Troubleshooting ZPA

Troubleshooting Tools

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on some of the tools available for troubleshooting ZPA.

Slide 2 - Navigating the eLearning Module

Navigating the eLearning Module

The screenshot shows the Zscaler Basic Administration interface. On the left, there's a sidebar with 'Dashboard', 'Diagnostics', 'Live Logs', 'Administration', and a 'Search' bar. The main area has tabs for 'Applications', 'Users', and 'Health'. A date range selector shows '14 Days'. Key metrics include 'APPLICATIONS ACCESSED' (15), 'DISCOVERED APPLICATIONS' (3), 'ACCESS POLICY BLOCKS' (0), and 'SUCCESSFUL TRANSACTIONS' (884). Below these are sections for 'TOP APPLICATIONS BY BANDWIDTH' and 'TOP POLICY BLOCKS'. At the bottom, there are buttons for 'Play/Pause', 'Previous Slide', 'Next Slide', 'Progress Bar', 'Audio On/Off', and 'Closed Captioning'. A large blue arrow points from the 'Exit' button at the top right towards the 'X' button in the top right corner of the slide frame.

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

Module Agenda



- Standard Troubleshooting Tools
- Zscaler Troubleshooting Tools
- ZPA Admin Portal Tools
 - The Health Dashboard
 - The Diagnostics Page

Slide notes

In this module, we will first review some standard network connectivity troubleshooting tools, then move on to look at some Zscaler-specific tools, and finally some ZPA-specific tools; incl. CLI Commands for App Connectors, the **Health** Dashboard in the admin portal, and the **Diagnostics** page.

Slide 4 - Standard Troubleshooting Tools



Slide notes

In the first section, we will review some commonly used standard troubleshooting tools.

Slide 5 - Troubleshooting Tools – General

Troubleshooting Tools – General



```
!ipconfig /all
Configuration

Interface . . . . . : peterlaptop
  Dns Suffix . . . . . :
  D Enabled . . . . . : Hybrid
  I Enabled . . . . . : No
  S Search List . . . . . : lan

  Adapter Ethernet 2:
    Dns-specific DNS Suffix . . . . . :
    M . . . . . : Zscaler Network Adapter 1.0.2.0
    Address . . . . . : 00-FF-9F-CD-EA-80
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
    IPV4 Address . . . . . : 192.168.0.100(Preferred)
      Subnet Mask . . . . . : 255.255.0.0(Preferred)
      Lease Obtain . . . . . : 117599951
      Lease End . . . . . : 100.64.0.3
    T1 . . . . . : 100.64.0.4
    T2 . . . . . : 100.64.0.5
```

Windows ipconfig, or
MAC ifconfig

- Use the **/all** or **-a** options for full details

Slide notes

The first tool that we look at is the **ipconfig** (Windows) or **ifconfig** (MAC) utility. This tool allows you to review the interface configuration for the network adapters installed on a Windows or MAC PC.

For full details use the options **/all** (Windows), or **-a** (MAC). Verify that the device has a valid IP configuration, that it has a valid gateway set, and that there is a valid DNS server configuration.

Slide 6 - Troubleshooting Tools – General

Troubleshooting Tools – General



```
ipconfig /all

Configuration

   . . . . . : peterlaptop
   . . . . . : Hybrid
   > Enabled. . . . . : No
   > Enabled. . . . . : No
   > Search List. . . . . : lan
   > Ethernet 2:

   n-specific DNS Suffix . :
   M . . . . . : Zscaler Network Adapter 1.0.2.0
   Address . . . . . : 00-FF-99-CD-EA-80
   Subnet Mask . . . . . : 255.255.0.0
   Default Gateway . . . . . : 192.168.0.1
   IPv4 Address . . . . . : 192.168.0.2(Preferred)
   Metric . . . . . : 100
   Subnet Mask . . . . . : 255.255.0.0
   Default Gateway . . . . . :
   ID . . . . . : 137509951
   Link Layer DUID. . . . . : 00-01-00-01-10-47-54-73-1C-39-47-2C-1
   T6 . . . . . : 192.168.0.3
   T6 . . . . . : 192.168.0.4
   T6 . . . . . : 192.168.0.5

ipconfig /all

ipconfig /all

ping cse.com [191.161.65.42] with 32 bytes of data:
From 191.161.65.42: bytes=32 time=0ms TTL=64

Ping statistics for 191.161.65.42:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

ping 8.8.8.8 with 32 bytes of data:
From 8.8.8.8: bytes=32 time=0ms TTL=64

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Windows ipconfig, or
MAC ifconfig

- Use the **/all** or **-a** options for full details

Ping from an affected
PC

- Local and Internet destinations
- By FQDN and by IP

Slide notes

The next tool we will talk about is the **ping** utility, available at the command line on both Windows and MAC OS X machines. This can be used to evaluate the extent of a network outage, you can ping local addresses to confirm the device has connectivity, then ping Internet addresses to confirm that the gateway does actually go somewhere.

Also ping by FQDN, to verify that DNS resolution is working, and if not ping by IP address, for example to the 8.8.8.8 address of the public Google DNS service. Check the round-trip time for the pings, to get a feel for the end-to-end latency on the connection.

In the ZPA context, use ping from the Zscaler App host to confirm connectivity to internal hosts (the default GW), external hosts, and to key components of the ZPA public infrastructure (from <https://ips.zscaler.com/zpa>). If you ping a private application by FQDN, it should resolve to a **100.64.0.0/16** IP address on the client device, but will not respond to any pings.

Also use ping from an App Connector (or a host adjacent to it) for the same purpose.

Slide 7 - Troubleshooting Tools – General

Troubleshooting Tools – General



```
!ipconfig /all

Configuration

   . . . . . : petrelaptop
   m Suffix . . . . . :
   . . . . . : Hybrid
   i Enabled . . . . . : No
   i Enabled . . . . . : No
   i Search List . . . . . : lan

Interface Ethernet 2:

v-Specific DNS Suffix . . . . . :
   M . . . . . : zscaler Network Adapter 1.0.2.0
   Address . . . . . : 00:ff:9f:cd:ea:00
   Duration Enabled . . . . . : Yes
   IPv4 Address . . . . . : 10.0.0.100(Preferred)
      A . . . . . : 100.64.0.2(Preferred)
   Mask . . . . . : 255.255.0.0
   MTU . . . . . :
   ID . . . . . : 11799951
   Last GUID . . . . . : 00-00-00-00-1d-17-54-73-39-47-2c-00
      A . . . . . : 100.64.0.3
      A . . . . . : 100.64.0.4
      A . . . . . : 100.64.0.5
```

Windows ipconfig, or
MAC ifconfig

- Use the `/all` or `-a` options for full details

```

2010 Microsoft Corporation. All rights reserved.

www.googlepublicip.com

curl www.googlepublicip.com

curl www.googlepublicip.com [151.191.65.47] with 32 bytes of data:
  by curl/7.19.0 libcurl/7.19.0 OpenSSL/1.0.2g zlib/1.2.8
  from 151.191.65.47 socket=3 times=1/1ms TTL=98
  from 151.191.65.47 socket=3 times=1/1ms TTL=98
  from 151.191.65.47 socket=3 times=1/1ms TTL=98
  by curl/7.19.0 libcurl/7.19.0 OpenSSL/1.0.2g zlib/1.2.8
  from 151.191.65.47 socket=3 times=1/1ms TTL=98

:statistics for 151.191.65.47:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
mintime 1ms, maxtime 28ms, Average = 19ms

curl www.googlepublicip.com

curl www.googlepublicip.com

curl www.googlepublicip.com [151.191.65.47] with 32 bytes of data:
  by curl/7.19.0 libcurl/7.19.0 OpenSSL/1.0.2g zlib/1.2.8
  from 151.191.65.47 socket=3 times=1/1ms TTL=98
  from 151.191.65.47 socket=3 times=1/1ms TTL=98
  from 151.191.65.47 socket=3 times=1/1ms TTL=98
  by curl/7.19.0 libcurl/7.19.0 OpenSSL/1.0.2g zlib/1.2.8
  from 151.191.65.47 socket=3 times=1/1ms TTL=98

:statistics for 151.191.65.47:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
mintime 1ms, maxtime 28ms, Average = 19ms

curl www.googlepublicip.com

curl www.googlepublicip.com
```

- Local and Internet destinations
- By FQDN and by IP

```
[Version 10.0.1403]
Copyright. All rights reserved.

scert.cn.com

cn.com [155.181.193.67]
30 hops:

  0 ms    2 ms  daldevice.lan [192.168.1.1]
  1 ms    11 ms  129.196.4-62.8cf1.ip-proximus.be [62.14.
  1 ms    14 ms  as-83-100.ipstrv5.ip.belgacom.be [95.183.24.
  1 ms    14 ms  as-13-100.ipstrv5.ip.belgacom.be [95.183.24.
  1 ms    15 ms  brv-01-100.telia.net [62.115.44.97]
  1 ms    18 ms  adn-063-100.telia.net [62.115.44.66]
  1 ms    19 ms  adn-02-100.telia.net [62.115.44.51]
  *      Request timed out.
  *      Request timed out.
  0 ms    19 ms  151.181.193.67
```

- Traceroute from an affected PC
 - Local and Internet destinations

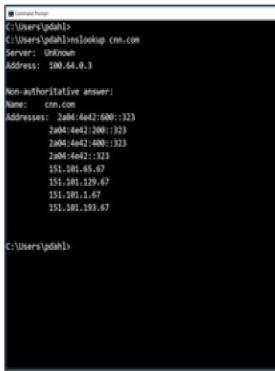
Slide notes

Next is the **traceroute** utility (MAC), **tracert** on Windows. This tool will tell you the full path of the traffic to the destination address, and the round-trip times for each hop. It can be used to identify where in the route a problem is occurring. Trace the route to local destinations (such as the default gateway) to confirm local connectivity, and to Internet destinations to confirm end-to-end connectivity.

Once again, in the ZPA context, use tracert from the Zscaler Client Connector, and from an App Connector VM (or a host adjacent to it) to evaluate the full path to internal hosts, external hosts, and to key components of the ZPA public infrastructure.

Slide 8 - Troubleshooting Tools – General

Troubleshooting Tools – General



A screenshot of a Windows command-line window titled 'cmd.exe'. The command entered is 'nslookup cn.com'. The output shows the FQDN 'cn.com' and its IP addresses: 2a01:4e42:600::323, 2a01:4e42:4000::323, 2a01:4e42::323, 2a01:4e42:1::323, 151.101.65.67, 151.101.129.67, 151.101.1.67, and 151.101.193.67. The prompt 'C:\Users\pdahl>' is visible at the bottom.

Use nslookup on
Windows or Mac

- Forward resolution of FQDN
- Reverse resolution of IP address

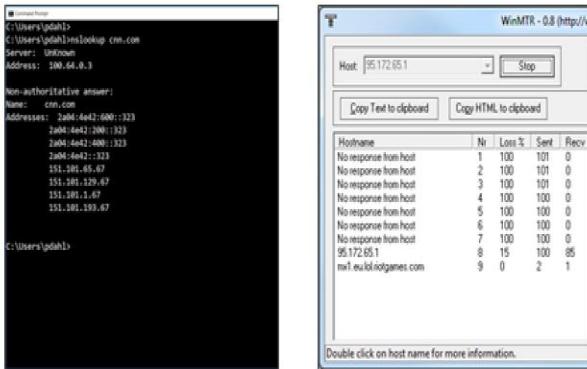
Slide notes

You can use the **nslookup** network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any specific DNS record. You can use this utility to forward resolve a FQDN to an IP address, or reverse resolve a public IP address to the matching FQDN.

For ZPA troubleshooting, use this tool to verify correct DNS resolution for internal and external hosts on the private network.

Slide 9 - Troubleshooting Tools – General

Troubleshooting Tools – General



Use nslookup on
Windows or Mac

- Forward resolution of FQDN
- Reverse resolution of IP address

WinMTR diagnostic
tool

- Combined 'ping' and 'traceroute' in a GUI-based app
- Exportable results

Slide notes

The **WinMTR** utility combines the functions of the command line ping and traceroute commands in a GUI-based application for Windows. It also allows the export of data to a file, which could subsequently be uploaded on a support ticket if necessary.

Slide 10 - Troubleshooting Tools – General

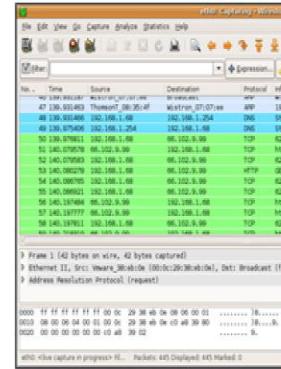
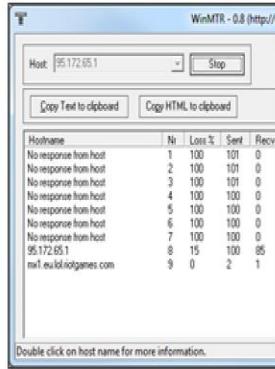
Troubleshooting Tools – General



```
c:\> nslookup
<User>:psdah>
C:\Users\psdah>nslookup cn.com
Server: 0.0.0.0
Address: 10.64.0.3

Non-authoritative answer:
Name:  cn.com
Addresses:  2a01:4e42:600::323
          2a01:4e42:600::123
          2a01:4e42:600::123
          2a01:4e42:600::123
          151.101.65.67
          151.101.129.67
          151.101.1.67
          151.101.193.67

C:\Users\psdah>
```



Use nslookup on Windows or Mac

- Forward resolution of FQDN
- Reverse resolution of IP address

WinMTR diagnostic tool

- Combined 'ping' and 'traceroute' in a GUI-based app
- Exportable results

Protocol Analyzer such as Wireshark

- Capture packets during transactions
- Analyze connection and debug protocol flows

Slide notes

If necessary, you can also use a **Protocol Analyzer** such as Wireshark, to capture packets on the wire as transactions take place. The packet captures can be saved to file for analysis of the protocol flows, or to be uploaded to a support ticket.

Note that a Protocol Analyzer should be a tool of last resort, as it can be quite a labor-intensive process to actually capture the traces. You must first identify where the captures are required and get an Analyzer in place. Also, you may need to do simultaneous captures at multiple places on the network path.

Slide 11 - Zscaler Troubleshooting Tools



Slide notes

In the next section, we will look at some of the Zscaler-specific troubleshooting tools available.

Slide 12 - Troubleshooting Tools - Zscaler

Troubleshooting Tools - Zscaler



A screenshot of the Zscaler Trust website. The top navigation bar includes "Cloud Private Access", "Support", "Log In", and "Logout". Below the navigation is a header with "Cloud Status" and "Network Status" tabs, both of which are currently selected. The "Cloud Status" section displays a table with columns for "Service" and "Status". The services listed are: ZPA Traffic Forwarding (OK), Authentication (OK), DNS (OK), Zscaler App Admin (OK), App Routing (OK), Client Enrollment (OK), Config Distribution (OK), Dashboard (OK), Diagnostics (OK), Downloads (OK), Health (OK), and Security (OK). The "Network Status" section displays a table with columns for "Region" and "Status". The regions listed are: Asia (OK) and North America (OK).

Check the Zscaler Trust site

- Check the status of the ZPA Cloud
- Check for on-going incidents

<https://trust.private.zscaler.com/>

Slide notes

As mentioned in previous modules, one of your first checks when an end user calls in with a problem should be the **Zscaler Trust site** for the ZPA Cloud on the URL shown here, to check for known outages or known issues.

Slide 13 - Troubleshooting Tools - Zscaler

Troubleshooting Tools - Zscaler



The screenshot shows two main sections. On the left, the 'Cloud Status' page displays various service status indicators (green bars) for services like Staff Forwarding, Authentication, DNS, Zscaler App Admin, App Routing, Client Enrollment, Config Distribution, Dashboard, Diagnostics, Downloads, Health, and Security. On the right, the 'ZPA Configuration Requirements' page lists specific port requirements for different protocols and ports, such as TCP/UDP ports for Application, Connector, and Local DNS Services.

Protocol	Port	Source	Description	State
TCP/UDP	All	Application Ports	Local Application Services	N/A
TCP	53	Connector	Local DNS Services	N/A
UDP	53	Connector	Local DNS Services	N/A
UDP	520	Connector	Local RDP Services	N/A
TCP	443	Connector	http://zscalerphotos.zscaler.net/	N/A
<small>Local endpoint must be enabled SSL connection. Note that outbound restriction is a specific item, or allowing requests through a proxy, requires additional configuration. Please refer to configuration guide for specific protocols for details.</small>				
TCP	443	Connector	AMF unencrypted outbound access to TCP 443	N/A

Check the Zscaler Trust site

- Check the status of the ZPA Cloud
- Check for on-going incidents

<https://trust.private.zscaler.com/>

Review Zscaler configuration requirements

- ZPA-specific requirements
- Same information on the /ZPA page for all Clouds

<https://ips.zscaler.net>

Slide notes

If necessary, you can use the ZPA configuration requirements page at the URL listed here to review what your settings should be, and check for misconfigurations.

Slide 14 - Troubleshooting Tools – Client Connector Logs

Troubleshooting Tools – Client Connector Logs

The screenshot shows the Zscaler Client Connector application window. On the left, there's a sidebar with icons for Private Access, Internet Security, Digital Experience, Notifications, and More. The main area has a 'Settings' header with a toggle for 'Show notifications in system tray'. Below this is a 'Troubleshoot' section containing 'Start Packet Capture', 'Report an Issue', 'Restart Service', 'Repair App', and a prominent 'Clear Logs' button which is highlighted with a red box. Underneath is an 'About' section with app version information and links to update the app or policy. On the right, a 'Log Locations' section lists paths for Windows and OSX. At the bottom, a system tray icon is shown with a context menu open, where 'Export Logs' is highlighted with a red box. The Zscaler logo is in the top right corner.

- Log Locations
 - Windows
 - C:\ProgramData\Zscaler
 - OSX
 - ~/Library/ApplicationSupport/com.zscaler.Zscaler/
 - /var/log/zscaler/ZSATunnel_*.log

Slide notes

The troubleshooting tools available on the **More** tab of the Client Connector can be enabled in the Client Connector portal, under **Administration > Zscaler App Support**. Besides being able to clear log files, you can also set different log modes that determine what type of information is stored in the various logs. For example, the **Debug** Mode logs all client connector activity that could assist Zscaler Support with troubleshooting issues.

To manually collect the log files, navigate to the directories listed here. The recommended way to collect the log files is by using the **Export Logs** function. Log files are then exported as a zip file which can be attached to a support ticket.

Slide 15 - Troubleshooting Tools – Client Connector Logs**Troubleshooting Tools – Client Connector Logs**

Log File Name	Content
ApplInfo	<ul style="list-style-type: none">System and App info
Setupapi.dev	<ul style="list-style-type: none">If error in driver installation
ZSAAuth	<ul style="list-style-type: none">Authentication/Login issues
ZSAService	<ul style="list-style-type: none">Service/Registry or session related issues
ZSATray	<ul style="list-style-type: none">UI/Interaction or Windows proxy settings
ZSATunnel	<ul style="list-style-type: none">Traffic/Network issues
ZSAUpdate	<ul style="list-style-type: none">App update/Auto update issues

Slide notes

This table lists the log filenames and what type of information is contained in each of the files.

Slide 16 - Troubleshooting Tools – Client Connector Error Codes

Troubleshooting Tools – Client Connector Error Codes

The screenshot shows a web page titled "Zscaler Client Connector Errors". It includes a sidebar with navigation links for "Cloud Authentication Error Codes" and "Cloud Error Codes". The main content is a table with four rows, each representing an error code. The columns are "Error Code", "Error Message", "Error Description", and "Resolution". Row 1: Error Code 1, Message "Internal Error, Please Contact Administrator.", Description "This is a generic error.", Resolution "Export logs and contact Zscaler Support.". Row 2: Error Code 2, Message "Zscaler Internet Security Authentication Error.", Description "This authentication error occurs when the user's cookie is expired or is no longer valid.", Resolution "Have the user reauthenticate to Zscaler Client Connector. If the issue persists, export logs and contact Zscaler Support.". Row 3: Error Code 3, Message "Zscaler Internet Security Enrollment Version Error.", Description "This error occurs when the device runs a version that is not supported by the cloud.", Resolution "Upgrade to the latest version of Zscaler Client Connector.". Row 4: Error Code 4, Message "Enrollment System Bad Timestamp Error, Please", Description "This error occurs when there is a time mismatch between the device and the cloud.", Resolution "Check the system time and ensure that it is accurate.".

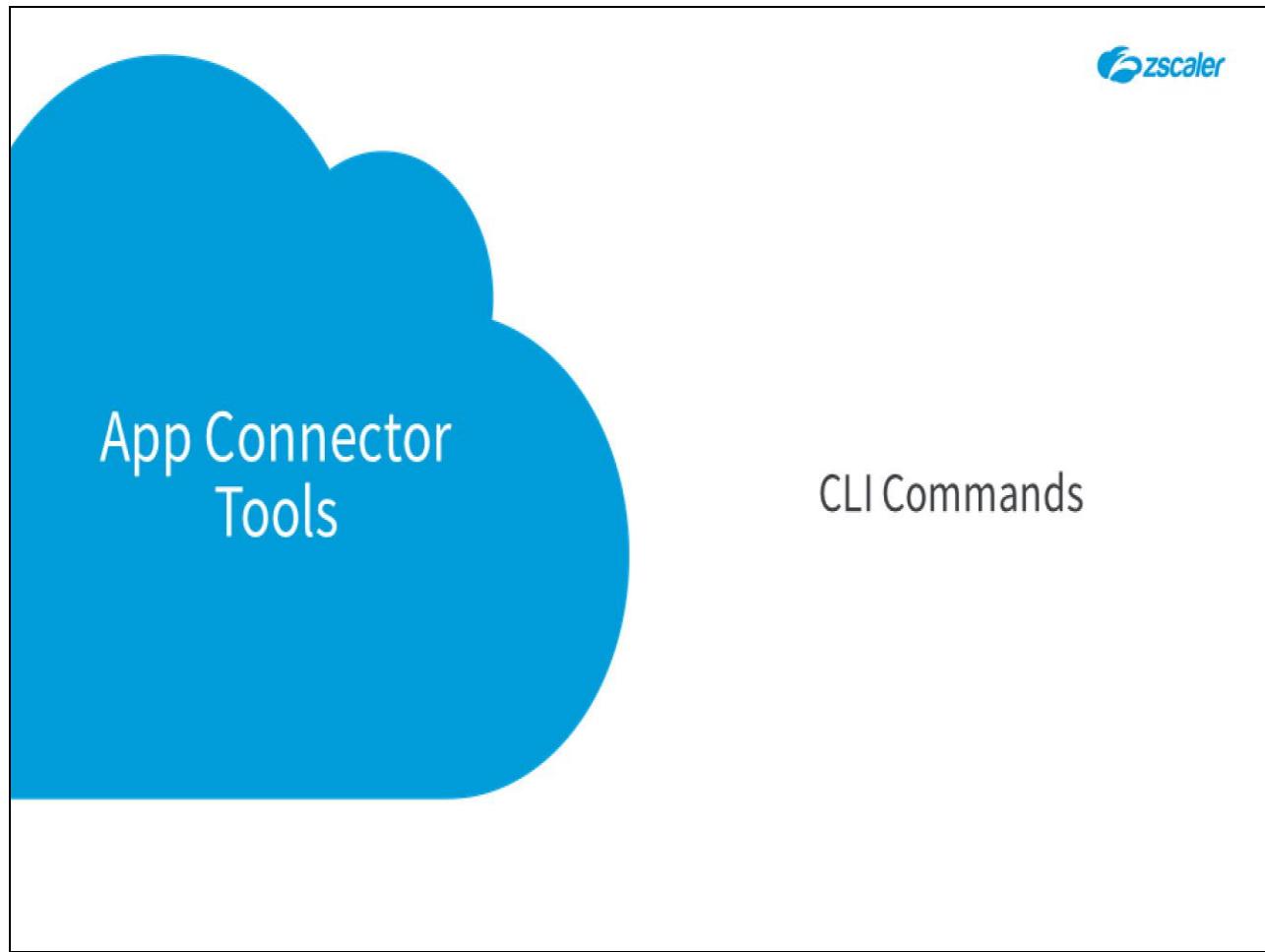
Error Code	Error Message	Error Description	Resolution
1	Zscaler Client Connector Internal Error, Please Contact Administrator.	This is a generic error.	Export logs and contact Zscaler Support.
2	Zscaler Internet Security Authentication Error.	This authentication error occurs when the user's cookie is expired or is no longer valid.	Have the user reauthenticate to Zscaler Client Connector. If the issue persists, export logs and contact Zscaler Support.
3	Zscaler Internet Security Enrollment Version Error.	This error occurs when the device runs a version that is not supported by the cloud.	Upgrade to the latest version of Zscaler Client Connector.
4	Enrollment System Bad Timestamp Error, Please	This error occurs when there is a time mismatch between the device and the cloud.	Check the system time and ensure that it is accurate.

<https://help.zscaler.com/z-app/zscaler-app-errors>

Slide notes

The Help portal URL listed here provides more detailed information about any error codes that you may see in log files.

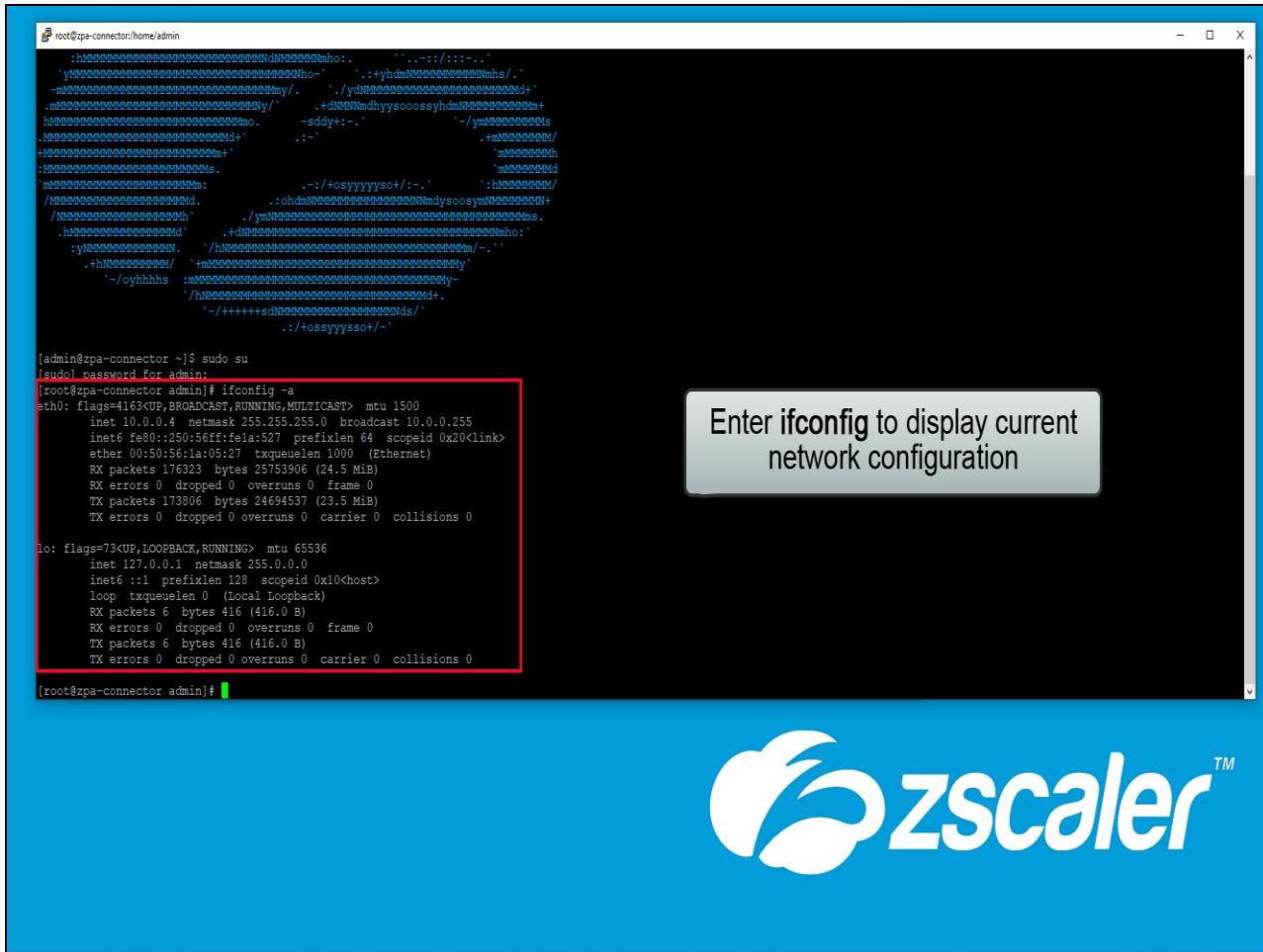
Slide 17 - App Connector Tools



Slide notes

If you have access to an App Connector VM, you can use CLI commands to check the state and performance of the Connector. The following demonstration shows a few examples of CLI commands commonly used for troubleshooting.

Slide 19 - Slide 19



```
root@zpa-connector:/home/admin
[admin@zpa-connector ~]$ sudo su
[sudo] password for admin:
[root@zpa-connector admin]# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.4  netmask 255.255.255.0  broadcast 10.0.0.255
                inet6 fe80::2e8:1ff:fe00:27  prefixlen 64  scopeid 0x20clink
                    ether 00:50:56:1a:05:27  txqueuelen 1000  (Ethernet)
                    RX packets 176323  bytes 25753906 (24.5 MiB)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 173806  bytes 24694537 (23.5 MiB)
                    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scopeid 0x10<host>
                    loop  txqueuelen 0  (Local Loopback)
                    RX packets 6  bytes 416 (416.0 B)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 6  bytes 416 (416.0 B)
                    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
[root@zpa-connector admin]#
```

Enter **ifconfig** to display current network configuration



Slide notes

Enter **ifconfig** to display the App Connector's current network configuration.

Slide 20 - Slide 20

```
root@zpa-connector:/home/admin .:/+ossyyysso+/` [admin@zpa-connector ~]5 sudo su [sudo] password for admin: [root@zpa-connector admin]# ifconfig -a eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.0.0.4 netmask 255.255.255.0 broadcast 10.0.0.255 inet6 fe80::250:56ff:fea:527 prefixlen 64 scopeid 0x20<link> ether 00:50:56:1a:05:27 txqueuelen 1000 (Ethernet) RX packets 176323 bytes 25753906 (24.5 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 173806 bytes 24694537 (23.5 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 0 (Local Loopback) RX packets 6 bytes 416 (416.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 6 bytes 416 (416.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 [root@zpa-connector admin]# ping intranet.patraining11.safemarch.com PING intranet.patraining11.safemarch.com (10.0.0.9) 56(44) bytes of data. 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=1 ttl=128 time=0.206 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=2 ttl=128 time=0.302 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=3 ttl=128 time=0.288 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=4 ttl=128 time=0.309 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=5 ttl=128 time=0.290 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=6 ttl=128 time=0.299 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=7 ttl=128 time=0.308 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=8 ttl=128 time=0.326 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=9 ttl=128 time=0.199 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=10 ttl=128 time=0.332 ms 64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=11 ttl=128 time=0.275 ms --- intranet.patraining11.safemarch.com ping statistics --- 11 packets transmitted, 11 received, 0% packet loss, time 10002ms rtt min/avg/max/mdev = 0.206/0.447/1.990/0.489 ms [root@zpa-connector admin]#
```

Use ping to confirm that a private application can be reached



Slide notes

Use a **ping** command to confirm that a private application can be reached.

Slide 21 - Slide 21

```
root@zpa-connector:~# ping intranet.patraining11.safemarch.com
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=5 ttl=128 time=0.290 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=6 ttl=128 time=0.299 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=7 ttl=128 time=0.308 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=8 ttl=128 time=0.326 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=9 ttl=128 time=1.99 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=10 ttl=128 time=0.332 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=11 ttl=128 time=0.275 ms
^C
--- intranet.patraining11.safemarch.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10002ms
rtt min/avg/max/mdev = 0.206/0.447/1.900/0.489 ms
[root@zpa-connector admin]# dig broker.prod.zpath.net

; <>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <>> broker.prod.zpath.net
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<- opcode: QUERY, status: NOERROR, id: 52492
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4000
;; QUESTION SECTION:
;broker.prod.zpath.net.      IN      A

;; ANSWER SECTION:
broker.prod.zpath.net. 600   IN      CNAME   co2br.global-gslb.prod.zpath.net.
co2br.global-gslb.prod.zpath.net. 600 IN CNAME zapp2saml.gslb.prod.zpath.net.
zapp2saml.gslb.prod.zpath.net. 60 IN  CNAME   was1.co2br.gslb.prod.zpath.net.
was1.co2br.gslb.prod.zpath.net. 192 IN A      165.225.9.253
was1.co2br.gslb.prod.zpath.net. 192 IN A      165.225.9.254
was1.co2br.gslb.prod.zpath.net. 192 IN A      165.225.9.250
was1.co2br.gslb.prod.zpath.net. 192 IN A      165.225.9.249
was1.co2br.gslb.prod.zpath.net. 192 IN A      165.225.9.251
was1.co2br.gslb.prod.zpath.net. 192 IN A      165.225.9.252

;; Query time: 29 msec
;; SERVER: 10.0.0.8453(10.0.0.8)
;; WHEN: Fri Aug 21 13:04:45 PDT 2020
;; MSG SIZE rcvd: 232

[root@zpa-connector admin]#
```

Use dig to verify the App Connector can DNS resolve to ZPA cloud



Slide notes

Use **dig** to verify the App Connector can DNS resolve to the ZPA cloud infrastructure.

Slide 22 - Slide 22

```
root@zpa-connector:/home/admin
mtr (0.0.0.0)
Keys: Help Display mode Restart statistics Order of fields quit

Host
1. 10.0.0.254
2. 10.101.0.1
3. 184-170-224-225.cloud.skytap.com
4. lag-32-100-99.ear2.Washington1.Level13.net
5. ???
6. Google-level13-60G.WashingtonDC.Level13.net
7. 108.170.240.97
8. 108.170.235.113
9. iad30s14-in-fl4.1e100.net

My traceroute [v0.85] Fri Aug 21 13:05:18 2020
Packets Pings
Loss% Snt Last Avg Best Wst StDev
0.0% 3 0.4 0.4 0.4 0.4 0.0
0.0% 3 0.8 0.9 0.8 1.1 0.0
0.0% 3 1.0 3.9 1.0 9.8 5.0
0.0% 3 2.9 2.9 2.9 3.0 0.0
0.0% 3 3.6 3.6 3.6 3.6 0.0
0.0% 3 4.8 4.8 4.7 5.1 0.0
0.0% 3 4.6 4.9 4.6 5.5 0.0
0.0% 3 3.6 3.7 3.6 3.7 0.0
```

Use mtr to show the path between the App Connector and a destination

The Zscaler logo is displayed at the bottom right of the slide.

Slide notes

Use **mtr** to show the path between the App Connector and a destination.

The command output shows the hops and network statistics for the full data path between App Connector and destination.

Slide 23 - Slide 23

```
root@zpa-connector:~/home/admin
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=6 ttl=128 time=0.299 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=7 ttl=128 time=0.308 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=8 ttl=128 time=0.326 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=9 ttl=128 time=1.99 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=10 ttl=128 time=0.332 ms
64 bytes from HOST-1.patraining11.safemarch.com (10.0.0.9): icmp_seq=11 ttl=128 time=0.275 ms
^C
--- intranet.patraining11.safemarch.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10002ms
rtt min/avg/max/mdev = 0.206/0.447/1.990/0.499 ms
[root@zpa-connector admin]# dig broker.prod.zpath.net

; <>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <>> broker.prod.zpath.net
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<< opcode: QUERY, status: NOERROR, id: 52492
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4000
;; QUESTION SECTION:
;broker.prod.zpath.net. IN A

;; ANSWER SECTION:
broker.prod.zpath.net. 600 IN CNAME co2br.global-gslb.prod.zpath.net.
co2br.global-gslb.prod.zpath.net. 600 IN CNAME zapp2saml.gslb.prod.zpath.net.
zapp2saml.gslb.prod.zpath.net. 60 IN CNAME was1.co2br.gslb.prod.zpath.net.
was1.co2br.gslb.prod.zpath.net. 192 IN A 165.225.9.253
was1.co2br.gslb.prod.zpath.net. 192 IN A 165.225.9.254
was1.co2br.gslb.prod.zpath.net. 192 IN A 165.225.9.250
was1.co2br.gslb.prod.zpath.net. 192 IN A 165.225.9.249
was1.co2br.gslb.prod.zpath.net. 192 IN A 165.225.9.251
was1.co2br.gslb.prod.zpath.net. 192 IN A 165.225.9.252

;; Query time: 29 msec
;; SERVER: 10.0.0.8#53(10.0.0.8)
;; WHEN: Fri Aug 21 13:04:45 PDT 2020
;; MSG SIZE rcvd: 232

[root@zpa-connector admin]# mtr google.com
[root@zpa-connector admin]#
```



Slide notes

Slide 24 - Slide 24

```
root@zpa-connector:~# top
top - 13:05:39 up 2:27, 4 users, load average: 0.05, 0.03, 0.05
Tasks: 108 total, 2 running, 106 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.3 us, 0.3 sy, 0.0 ni, 99.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Mem: 1884388 total, 1398884 free, 307528 used, 177976 buff/cache
Swap: 0 total, 0 free, 0 used. 1410772 avail Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
1149 root      20   0 432912 155856 1796 S  1.0  8.3  1:26.91 zpa-connector
375 root      20   0 37952  4604 4272 S  0.7  0.2  0:00.79 systemd-journal
1710 zscaler  20   0 941444 25520 3632 S  0.3  1.4  0:25.82 image.bin
  1 root      20   0 125820  6504 3900 S  0.0  0.3  0:02.66 systemd
  2 root      20   0     0     0  0 S  0.0  0.0  0:00.00 kthreadd
  3 root      20   0     0     0  0 S  0.0  0.0  0:00.04 ksftirqd/0
  5 root      0 -20    0     0  0 S  0.0  0.0  0:00.00 kworker/0:0H
  6 root      20   0     0     0  0 S  0.0  0.0  0:00.12 kworker/u4:0
  7 root      rt   0     0     0  0 S  0.0  0.0  0:00.01 migration/0
  8 root      20   0     0     0  0 S  0.0  0.0  0:00.00 rcu_bh
  9 root      20   0     0     0  0 S  0.0  0.0  0:00.00 rcuob/0
 10 root     20   0     0     0  0 S  0.0  0.0  0:00.00 rcuob/1
 11 root     20   0     0     0  0 S  0.0  0.0  0:00.48 rcu_sched
 12 root     20   0     0     0  0 S  0.0  0.0  0:00.21 rcuos/0
 13 root     20   0     0     0  0 R  0.0  0.0  0:00.41 rcuos/1
 14 root      rt   0     0     0  0 S  0.0  0.0  0:00.02 watchdog/0
 15 root      rt   0     0     0  0 S  0.0  0.0  0:00.01 watchdog/1
 16 root      rt   0     0     0  0 S  0.0  0.0  0:00.00 migration/1
 20 root     20   0     0     0  0 S  0.0  0.0  0:00.07 ksftirqd/1
 19 root     0 -20    0     0  0 S  0.0  0.0  0:00.01 kworker/1:0H
 20 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 khelper
 21 root     20   0     0     0  0 S  0.0  0.0  0:00.00 kdvtmmpfs
 22 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 netns
 23 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 perf
 24 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 writeback
 25 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 kintegrityd
 26 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 bioset
 27 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 kblockd
 28 root     0 -20    0     0  0 S  0.0  0.0  0:00.00 md
 29 root     20   0     0     0  0 S  0.0  0.0  0:00.60 kworker/0:1
 33 root     20   0     0     0  0 S  0.0  0.0  0:00.00 khungtaskd
 34 root     20   0     0     0  0 S  0.0  0.0  0:00.00 kswapd0
 35 root     25   5     0     0  0 S  0.0  0.0  0:00.00 ksmd
 36 root     39  19     0     0  0 S  0.0  0.0  0:00.02 khungpacerd
```

Use top to check CPU utilization across all cores on all processors



Slide notes

The **top** command can be used to check CPU utilization across all cores on all processors.

Slide 25 - Slide 25

```
root@zpa-connector:~# top
Tasks: 108 total, 2 running, 106 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.3 us, 0.2 sy, 0.0 ni, 99.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Mem: 1864388 total, 1398804 free, 307528 used, 177976 buff/cache
Swap: 0 total, 0 free, 0 used. 1410776 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1148 root 20 0 432912 155856 1796 S 1.0 8.3 1:26.97 zpa-connector
1710 zscaler 20 0 941444 25520 3632 S 0.3 1.4 0:25.84 image.bin
1 root 20 0 125820 6504 3900 S 0.0 0.3 0:02.66 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
3 root 20 0 0 0 0 S 0.0 0.0 0:00.00 ksoftirqd/0
5 root 0-20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
6 root 20 0 0 0 0 S 0.0 0.0 0:00.12 kworker/0:10
7 root rt 0 0 0 0 S 0.0 0.0 0:00.01 migration/0
8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/0
10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/1
11 root 20 0 0 0 0 S 0.0 0.0 0:00.48 rcu_sched
12 root 20 0 0 0 0 S 0.0 0.0 0:00.21 rcuos/0
13 root 20 0 0 0 0 R 0.0 0.0 0:00.41 rcuos/1
14 root rt 0 0 0 0 S 0.0 0.0 0:00.02 watchdog/0
15 root rt 0 0 0 0 S 0.0 0.0 0:00.01 watchdog/1
16 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/1
17 root 20 0 0 0 0 S 0.0 0.0 0:00.07 ksoftirqd/1
19 root 0-20 0 0 0 S 0.0 0.0 0:00.00 kworker/1:0H
20 root 0-20 0 0 0 S 0.0 0.0 0:00.00 khelper
21 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
22 root 0-20 0 0 0 S 0.0 0.0 0:00.00 netns
23 root 0-20 0 0 0 S 0.0 0.0 0:00.00 perf
24 root 0-20 0 0 0 S 0.0 0.0 0:00.00 writeback
25 root 0-20 0 0 0 S 0.0 0.0 0:00.00 integrityd
26 root 0-20 0 0 0 S 0.0 0.0 0:00.00 bioset
27 root 0-20 0 0 0 S 0.0 0.0 0:00.00 kblockd
28 root 0-20 0 0 0 S 0.0 0.0 0:00.00 md
29 root 20 0 0 0 0 S 0.0 0.0 0:00.60 kworker/0:1
33 root 20 0 0 0 0 S 0.0 0.0 0:00.00 khungtaskd
34 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kswapd0
35 root 25 5 0 0 0 S 0.0 0.0 0:00.00 ksmd
36 root 39 19 0 0 0 S 0.0 0.0 0:00.02 khugepaged
37 root 20 0 0 0 0 S 0.0 0.0 0:00.00 fsnotify_mark
[root@zpa-connector admin]#
```



Slide notes

Slide 26 - Slide 26

The screenshot shows a terminal window with the following content:

```
root@zpa-connector:/home/admin
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1145 root 20 0 432912 155856 1796 S 1.0 8.3 1:26.97 zpa-connector
1710 zscaler 20 0 941444 25520 3632 S 0.3 1.4 0:25.84 image.bin
  1 root 20 0 125820 6504 3900 S 0.0 0.3 0:02.66 systemd
  2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
  3 root 20 0 0 0 0 S 0.0 0.0 0:00.04 ksoftirqd/0
  5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
  6 root 20 0 0 0 0 S 0.0 0.0 0:00.12 kworker/0:0H
  7 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
  8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
  9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/0
10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/1
11 root 20 0 0 0 0 S 0.0 0.0 0:00.48 rcu_sched
12 root 20 0 0 0 0 S 0.0 0.0 0:00.21 rcuos/0
13 root 20 0 0 0 0 R 0.0 0.0 0:00.41 rcuos/1
14 root rt 0 0 0 0 S 0.0 0.0 0:00.02 watchdog/0
15 root rt 0 0 0 0 S 0.0 0.0 0:00.00 watchdog/1
16 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/1
17 root 20 0 0 0 0 S 0.0 0.0 0:00.07 ksoftirqd/1
19 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/1:0H
20 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 khelper
21 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
22 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 netns
23 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 perf
24 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 writeback
25 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 integrityd
26 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 bioset
27 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kblockd
28 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 md
29 root 20 0 0 0 0 S 0.0 0.0 0:00.60 kworker/0:1
33 root 20 0 0 0 0 S 0.0 0.0 0:00.00 khungtaskd
34 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kswapd0
35 root 25 5 0 0 0 S 0.0 0.0 0:00.00 ksmd
36 root 39 19 0 0 0 S 0.0 0.0 0:00.02 khugepaged
37 root 20 0 0 0 0 S 0.0 0.0 0:00.00 fsnotify_mark
[root@zpa-connector admin]# free
total used free shared buff/cache available
Mem: 1884388 307020 1399408 16912 177960 1411292
Swap: 0 0 0
[root@zpa-connector admin]#
```

A callout bubble points to the command `free` with the text "Use free to check memory utilization".



Slide notes

The command **free** lets you check memory utilization.

Slide 27 - Slide 27

The screenshot shows a terminal window with the following content:

```
root@zpa-connector:/home/admin
[6 root 20 0 0 0 0 S 0.0 0.0 0:00:12 kworker/u4:0
7 root rt 0 0 0 0 0 S 0.0 0.0 0:00:01 migration/0
8 root 20 0 0 0 0 0 S 0.0 0.0 0:00:00 rcu_bh
9 root 20 0 0 0 0 0 S 0.0 0.0 0:00:00 rcu_bh/0
10 root 20 0 0 0 0 0 S 0.0 0.0 0:00:00 rcu_bh/1
11 root 20 0 0 0 0 0 S 0.0 0.0 0:00:48 rcu_sched
12 root 20 0 0 0 0 0 S 0.0 0.0 0:00:21 rcu_bh/0
13 root 20 0 0 0 0 R 0.0 0.0 0:00:41 rcu_bh/1
14 root rt 0 0 0 0 0 S 0.0 0.0 0:00:02 watchdog/0
15 root rt 0 0 0 0 0 S 0.0 0.0 0:00:00 watchdog/1
16 root rt 0 0 0 0 0 S 0.0 0.0 0:00:00 migration/1
17 root 20 0 0 0 0 0 S 0.0 0.0 0:00:07 ksftirqd/1
18 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 kworker/l:0H
19 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 kworker/l:0H
20 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 khelper
21 root 20 0 0 0 0 0 S 0.0 0.0 0:00:00 kdevtmpfs
22 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 netns
23 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 perf
24 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 writeback
25 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 integrityd
26 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 bioset
27 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 kblockd
28 root 0 -20 0 0 0 0 S 0.0 0.0 0:00:00 md
29 root 20 0 0 0 0 0 S 0.0 0.0 0:00:60 kworker/0:1
30 root 20 0 0 0 0 0 S 0.0 0.0 0:00:00 khungtaskd
31 root 20 0 0 0 0 0 S 0.0 0.0 0:00:00 kswapd0
32 root 25 5 0 0 0 0 S 0.0 0.0 0:00:00 ksmd
33 root 39 19 0 0 0 0 S 0.0 0.0 0:00:02 khugepaged
34 root 20 0 0 0 0 0 S 0.0 0.0 0:00:00 fsnotify_mark
[root@zpa-connector admin]# free
total used free shared buff/cache available
Mem: 1884388 307020 1399408 16912 177960 1411292
Swap: 0 0 0
[root@zpa-connector admin]# sudo df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sdal 8.0G 1.1G 7.0G 13% /
devtmpfs 902M 0 902M 0% /dev
tmpfs 921M 0 921M 0% /dev/shm
tmpfs 921M 17M 904M 2% /run
tmpfs 921M 0 921M 0% /sys/fs/cgroup
tmpfs 195M 0 185M 0% /run/user/1000
[root@zpa-connector admin]#
```

A callout box points to the command `sudo df -h` in the terminal window.

zscaler™

Slide notes

App Connectors generate logs that are stored on disk. Enter **sudo df -h** to display the disk space utilization on the App Connector.

Slide 28 - Slide 28

The screenshot shows a terminal window with the following command history:

```
root@zpa-connector:~# ss -uln | wc -l && ss -tn state connected | wc -l
Enter
ss -uln | wc -l && ss -tn state connected | wc -l
to check he number of used ports
```

Below the command, the output is shown:

```
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/0
10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/1
11 root 20 0 0 0 0 S 0.0 0.0 0:00.48 rcu_sched
12 root 20 0 0 0 0 S 0.0 0.0 0:00.21 rcuos/0
13 root 20 0 0 0 0 R 0.0 0.0 0:00.41 rcuos/1
14 root rt 0 0 0 0 S 0.0 0.0 0:00.02 watchdog/0
15 root rt 0 0 0 0 S 0.0 0.0 0:00.01 watchdog/1
16 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/1
17 root 20 0 0 0 0 S 0.0 0.0 0:00.07 ksoftirqd/1
18 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/1:0H
20 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 khelper
21 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
22 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 netns
23 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 perf
24 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 writeback
25 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 integrityd
26 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 bioset
27 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kblockd
28 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 md
29 root 20 0 0 0 0 S 0.0 0.0 0:00.60 kworker/0:1
33 root 20 0 0 0 0 S 0.0 0.0 0:00.00 khungtaskd
34 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kswapd0
35 root 25 5 0 0 0 S 0.0 0.0 0:00.00 ksmd
36 root 39 19 0 0 0 S 0.0 0.0 0:00.02 khugepaged
37 root 20 0 0 0 0 S 0.0 0.0 0:00.00 fsnotify_mark
```

Following this, the `free` command is run:

```
[root@zpa-connector admin]# free
total        used        free      shared  buff/cache   available
Mem:    1884388     307020   1399408     16912      177960    1411292
Swap:          0          0          0          0          0          0
```

Then, the `df -h` command is run:

```
[root@zpa-connector admin]# sudo df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdal      8.0G  1.1G  7.0G  13% /
devtmpfs        902M    0M  902M   0% /dev
tmpfs          921M    0M  921M   0% /dev/shm
tmpfs          921M   17M  904M   2% /run
tmpfs          921M    0M  921M   0% /sys/fs/cgroup
tmpfs          185M    0M  185M   0% /run/user/1000
```

Finally, the command `ss -uln | wc -l && ss -tn state connected | wc -l` is run again, with the output highlighted in red:

```
[root@zpa-connector admin]# ss -uln | wc -l && ss -tn state connected | wc -l
10
39
```

A large Zscaler logo is overlaid on the bottom right of the terminal window.

Slide notes

The number of used and free ports can be obtained from the App Connector by using the **ss** command.

In this example, the output shows that 10 is the number of UDP ports and 39 is the number of TCP ports in use.

Slide 29 - Slide 29

The screenshot shows a terminal window with a blue header bar. The terminal content is as follows:

```
root@zpa-connector:/home/admin
total used free shared buff/cache available
Mem: 1884308 307020 1399408 16912 177960 1411292
Swap: 0 0 0
[root@zpa-connector admin]# sudo df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sdal 8.0G 1.1G 7.0G 13% /
devtmpfs 902M 0 902M 0% /dev
tmpfs 921M 0 921M 0% /dev/shm
tmpfs 921M 17M 904M 2% /run
tmpfs 921M 0 921M 0% /sys/fs/cgroup
tmpfs 105M 0 105M 0% /run/user/1000
[root@zpa-connector admin]# ss -uln | wc -l && ss -tn state connected | wc -l
13
13
[root@zpa-connector admin]# sudo systemctl status zpa-connector -1
● zpa-connector.service - Zscaler Private Access Connector
  Loaded: loaded (/usr/lib/systemd/system/zpa-connector.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2020-08-21 10:38:34 PDT; 2h 29min ago
    Main PID: 1148 (zpa-connector)
   Group: /system.slice/zpa-connector.service
         ├─1148 /opt/zscaler/bin/zpa-connector
         └─1710 zpa-connector-child

Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Broker control connection, state fohh_connection_connected, [10.0.0.4]:45092>broker1.nyc3.prod.zpath.net:[165.225.221.253]:443
:1 uptime 2H:28M:57s, rtt: 10855 us
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Broker data connection, total 2, active 2, backed off connections 0
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Broker data transfer, to broker 8932139 bytes, from broker 156677 bytes
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Mtunnels(all|health-report-based|no-health-report-based), total 79|79|0, to broker 79|79|0, to private broker 0|0|0, unbound/et
rrored 0, current active 2|2|0, peak active 26
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 79, BindAck 79, AppRtDisc 31, DnsChk 46, MtunnelEnd 113 TagPause 0 TagResume 0 WinUpdate 246 Redirect
1 TX: BrkRqAct 0|0, BindReq 79|0, AppRReq 10922|0, HealthRp 4919|0 DnsChk 46
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Time skew: local time lags cloud time by 0.044780s
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: File descriptors(max|in-use): System 103415|1664, Process 102400|105
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: System Sockets: Created 221 TCP4 in-use 12, TCP4 time-wait 3, UDP4 in-use 9, TCP6 in-use 2, UDP6 in-use 5, Ports available per
interface 28232, IPv4 interfaces 2, IPv6 interfaces 2
Aug 21 13:07:44 zpa-connector zpa-connector-child[1710]: Broker data connection, [10.0.0.4]:34070>broker5.was1.prod.zpath.net:[165.225.9.253]:443:2, uptime 2H:20M:0S, rtt: 11451 us, a
ctive mtunnels 0, total mtunnels 25, to broker 20750 bytes, from broker 39384 bytes. Detail(rx 39384, peer_tx 39384, tx 20750, tx_drop 0, tx_limit 33575110, tx_limit_update 1598038626
474103, rx_rx 20670, rx_tx_limit 33593744, rx_wnd_update 1598038626474103, rx_wnd_update 1598038626470643, tx_blocked 0, emq 20750, deg 20750)
[root@zpa-connector admin]#
```

A callout box with a red border and white background is overlaid on the terminal window, containing the text:

Enter sudo systemctl status zpa-connector to check the status of the App Connector process

Slide notes

Use the **systemctl status** command to check the status of the App Connector process.

Make sure the status is shown as **Active**.



Slide 30 - Slide 30

```
root@zpa-connector:~# root@zpa-connector:~# 
Swap:          0      0      0
[root@zpa-connector admin]# sudo df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdal       8.0G  1.1G  7.0G  13% /
devtmpfs        902M   0  902M   0% /dev
tmpfs          921M   0  921M   0% /dev/shm
tmpfs          921M  17M  904M  2% /run
tmpfs          921M   0  921M   0% /sys/fs/cgroup
tmpfs          165M   0  165M   0% /run/user/1000
[root@zpa-connector admin]# ss -uIn | wc -l && ss -tn state connected | wc -l
13
13
[root@zpa-connector admin]# sudo systemctl status zpa-connector -l
● zpa-connector.service - Zscaler Private Access Connector
  Loaded: loaded (/usr/lib/systemd/system/zpa-connector.service; enabled; vendor preset: active)
  Active: active (running) since Fri 2020-08-21 10:38:34 PDT; 2h 29min ago
    Main PID: 1148 (zpa-connector)
   CGroup: /system.slice/zpa-connector.service
           └─1148 /opt/zscaler/bin/zpa-connector
             ├─1710 zpa-connector-child

Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Broker control connection, state fohh_connection_connected, [10.0.0.4]:45092:broker1.nyc3.prod.zpath.net:[165.225.221.253]:443
:1 uptime 2H:28M:57s, rtt: 10855 us
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Broker data connection, total 2, active 2, backed off connections 0
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Broker data transfer, to broker 8932139 bytes, from broker 156677 bytes
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Mtunnels(all|health-report-based|no-health-report-based), total 79|79|0, to broker 79|79|0, to private broker 0|0|0, unbound/errorred 0, current active 2|2|0, peak active 26
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 79, BindAck 79, AppRtDisc 31, DnsChk 46, MtunnelEnd 113 TagPause 0 TagResume 0 WinUpdate 246 Redirect 1 TX: BrkRqAck 0|0, BindReq 10922|0, HealthRp 4919|0 DnsChk 46
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Time skew: local time lags cloud time by 0.044780s
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: File descriptors(max|in-use): System 103415|1664, Process 102400|105
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: System Sockets: Created 221 TCP4 in-use 12, TCP4 time-wait 3, UDP4 in-use 9, TCP6 in-use 2, UDP6 in-use 5, Ports available per interface 28232, IPv4 interfaces 2, IPv6 interfaces 2
Aug 21 13:07:44 zpa-connector zpa-connector-child[1710]: Broker data connection, [10.0.0.4]:34070:broker5.was1.prod.zpath.net:[165.225.9.253]:443:2, uptime 2H:20M:08, rtt: 11451 us, active mtunnels 0, total mtunnels 25, to broker 20750 bytes, from broker 39384 bytes. Detail:[rx 39384, peer_tx 39384, tx 20750, tx_drop 0, tx_limit 33575110, tx_limit_update 1598038626474103, rx 20670, rx_tx_limit 33593744, tx_wnd_update 1598038626474103, rx_wnd_update 1598038626474103, tx_blocked 0, emg 20750, dem 20750]
[root@zpa-connector admin]# ls /opt/zscaler/var
cert.pem chain.pem cloud.pem config.json instance_id.crypt metadata provision key.crypt root.pem rsa key.pem rsa pub.pem updater.version version
[root@zpa-connector admin]#
```

Use **ls** to view the contents of a directory



Slide notes

You can use standard Linux commands, like **ls** to view the contents of a directory.

Slide 31 - Slide 31

```
root@zpa-connector:~# journalctl -u zpa-connector
-- Logs begin at Fri 2020-08-21 10:39:08 PDT, end at Fri 2020-08-21 13:08:37 PDT. --
Aug 21 10:38:34 zpa-connector systemd[1]: Started Zscaler Private Access Connector.
Aug 21 10:38:34 zpa-connector zpa-connector[1148]: Starting zscaler Private Access Connector...
Aug 21 10:38:34 zpa-connector zpa-connector[1148]: zpa-connector: starting, version 16.46.1
Aug 21 10:38:35 zpa-connector zpa-connector[1148]: zscaler-update: Zscaler software update: Currently installed version verified as 20.51.3
Aug 21 10:38:35 zpa-connector zpa-connector[1148]: zscaler-update: zpa-connector-child Started from /opt/zscaler/var/image.bin
Aug 21 10:38:35 zpa-connector zpa-connector[1148]: zscaler-update: zpa-connector-child Started from /opt/zscaler/var/image.bin
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: zpa-connector-child: starting, version 20.51.3
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: SSL version: OpenSSL 1.0.2o-fips 27 Mar 2018
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: libevent version: 2.1.8-stable
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: No modifications to thread pools present
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Connector version: 20.51.3
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Checking Enrollment
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Have valid certificate.
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Initialization assistant: 1441234
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: FOHH creating thread pool fohn
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: FOHH creating thread pool wally
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Waiting for connector to retrieve
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2b
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2b
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.249
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.253
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.254
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Log(event_log) successfully connected to zscaler Cloud: [10.0.0.4]:52552;broker4.wasi.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 10:38:36 zpa-connector zpa-connector-child[1710]: Get connector returned ZPN_RESULT_NOT_FOUND, please contact customer support, if this persists
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: FOHH creating thread pool control with threads 0->3
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Running with connector GID = 144123469846545379, name = NYC_HQ-1
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Initialization Complete
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Connector- waiting for time synchronization
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: _____ Connector Status: ID=144123469846545379;Name=NYC_HQ-1;Ver=20.51.3;Mem[System|Process]=18%@0%;Disk Avail=6.96GB;CPU=0%
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Certificate will expire in 371 days, 22 hours, 13 minutes, 13 seconds
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker config connection, state fohh_connection_connected, [10.0.0.4]:60534;broker2.wasi.prod.zpath.net:[165.225.9.250]:443;1
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Log(event_log) connection, state fohh_connection_connected, [10.0.0.4]:52552;broker4.wasi.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker control connection, state fohh_connection_unresolved, [uninitialized]:0;any.co2br.prod.zpath.net:[uninitialized]:0;1 up
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker data connection, total 0, active 0, backed off connections 0
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker data transfer, to broker 0 bytes, from broker 0 bytes
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Mtunnels(all|health-report-based|no-health-report-based), total 0|0|0, to broker 0|0|0, to private broker 0|0|0, unbound/error
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 0, BindAck 0, AppRtBdisc 0, OmsChk 0, MtunnelEnd 0 TagPause 0 TagResume 0 WinUpdate 0 Redirect 0 TX: Br
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Registered apps count 0, alive apps 0, apps with on-access health 0, apps with no health reporting 0, service count 0, target
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Time skew: local time lags cloud time by 0.000000s
lines 1-40
```

Use **journalctl -u zpa-connector** to view App Connector logs



Slide notes

Use the **journalctl** command to view App Connector logs.

Slide 32 - Slide 32



The screenshot shows a terminal window with the title 'root@zpa-connector:home/admin'. The window displays a log of events from the Zscaler Private Access Connector. The log includes messages about starting the connector, performing software updates, connecting to a cloud, and handling broker connections. The log ends with a message about time skew.

```
root@zpa-connector:home/admin
Aug 21 10:38:34 zpa-connector systemd[1]: Started Zscaler Private Access Connector.
Aug 21 10:38:34 zpa-connector systemd[1]: Starting zscaler Private Access Connector...
Aug 21 10:38:34 zpa-connector zpa-connector[1140]: zpa-connector: starting, version 16.46.1
Aug 21 10:38:35 zpa-connector zpa-connector[1140]: zscaler-update: Zscaler software update: Currently installed version verified as 20.51.3
Aug 21 10:38:35 zpa-connector zpa-connector[1140]: zscaler-update: zpa-connector-child Started from /opt/zscaler/var/image.bin
Aug 21 10:38:35 zpa-connector zpa-connector[11710]: zpa-connector-child: starting, version 20.51.3
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: SSL version: OpenSSL 1.0.2o-fips 27 Mar 2018
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Libevent version: 2.1.8-stable
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: No modifications to thread pools present
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Connector version: 20.51.3
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Checking Enrollment
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Have valid certificate.
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Initializing assistant: 144123469846545379, customer id: 144123469846544384 belonging to customer domain: patraining11.safemar
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: FOHH creating thread pool fohh_log with threads 0->3
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: FOHH creating thread pool wally with threads 0->3
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Waiting for connector to retrieve configuration
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.250
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.252
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.251
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.249
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.253
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.254
Aug 21 10:38:35 zpa-connector zpa-connector-child[11710]: Log(event_log) successfully connected to Zscaler Cloud: [10.0.0.4]:52552;broker4.wasl.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 10:38:36 zpa-connector zpa-connector-child[11710]: Get connector returned ZPN_RESULT_NOT_FOUND, please contact customer support, if this persists
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: FOHH creating thread pool control with threads 0->3
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Running with connector GID = 144123469846545379, name = NYC_HQ-1
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Initialization Complete
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Connector- waiting for time synchronization
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: ----- Connector Status:ID=144123469846545379:Name=NYC_HQ-1:Ver=20.51.3:Mem(System|Process)=18%8%:Disk Avail=6.96GB:CPU=0%
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Certificate will expire in 371 days, 22 hours, 13 minutes, 13 seconds
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Broker config connection, state fohh_connection_connected, [10.0.0.4]:60534;broker2.wasl.prod.zpath.net:[165.225.9.250]:443;1
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Log(event_log) connection, state fohh_connection_connected, [10.0.0.4]:52552;broker4.wasl.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Broker control connection, state fohh_connection_unresolved, [uninitialized]:0;any.co2br.prod.zpath.net:[uninitialized]:0;1 up
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Broker data connection, total 0, active 0, backed off connections 0
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Broker data transfer, to broker 0 bytes, from broker 0 bytes
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Mtunnels(all)health-report-based[no-health-report-based], total 0|0|0, to broker 0|0|0, to private broker 0|0|0, unbound/error
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: RPC Messages, RX: BrkRq 0, BindAck 0, AppRtDisc 0, DnsChk 0, MtunnelEnd 0 TagPause 0 WinUpdate 0 Redirect 0 TX: Br
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Registered apps count 0, alive apps 0, apps with on-access health 0, apps with no health reporting 0, service count 0, target
Aug 21 10:38:37 zpa-connector zpa-connector-child[11710]: Time skew: local time lags cloud time by 0.000000s
[root@zpa-connector admin]#
```



Slide notes

Slide 33 - Slide 33

```
root@zpa-connector:~# journalctl -n100 | grep target
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Waiting for connector to retrieve configuration
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.250
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.252
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.251
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.249
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.253
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.254
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Log(event_log) successfully connected to Zscaler Cloud: [10.0.0.4]:52552;broker4.was1.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 10:38:36 zpa-connector zpa-connector-child[1710]: Get connector returned ZPN_RESULT_NOT_FOUND, please contact customer support, if this persists
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: FOHH creating thread pool control with threads 0->3
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Running with connector GID = 144123469846545379, name = NYC_HQ-1
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Initialization Complete
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Connector- waiting for time synchronization
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: ----- Connector Status: ID=144123469846545379;Name=NYC_HQ-1;Ver=20.51.3;Mem(System|Process)=18%;Disk Avail=6.96GB;CPU=0%
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Certificate will expire in 371 days, 22 hours, 13 minutes, 13 seconds
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker config connection, state fohh connection connected, [10.0.0.41:60534:hrnker2.was1.nrrd.znath.net:[165.225.9.250]:443;1
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Log(event_log) connection, stat
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker control connection, stat
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker data connection, total 0
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker data transfer, to broker
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Mtunels(all)health-report-base
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 0, Bind
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Registered apps count 0, alive
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Time skew: local time lags clou
[redacted]
[root@zpa-connector admin]# journalctl -n100 | grep target
Aug 21 13:03:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
Aug 21 13:04:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
Aug 21 13:05:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
Aug 21 13:06:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
Aug 21 13:08:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target
count 27, target alive 26
[redacted]
[root@zpa-connector admin]#
```

Use journalctl -n100 | grep target to view information about applications that can be reached by the App Connector



Slide notes

The **grep** option allows you to filter the output.

In this example, the filtered output shows the number of applications that the App Connector is currently monitoring for reachability.

Slide 34 - Slide 34

```
root@zpa-connector:~# journalctl -n100 | grep target
Aug 21 13:03:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:04:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:05:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:06:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:08:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
[root@zpa-connector admin]# journalctl -n100 | grep target
Aug 21 13:03:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:04:37 zpa-connector zpa-connector-child[1710]: Certificate will expire in 6.96GB:CPU=0% 5.225.9.250):443;1
Aug 21 13:05:37 zpa-connector zpa-connector-child[1710]: Broker config connected 65.225.9.252):443;1
Aug 21 13:06:37 zpa-connector zpa-connector-child[1710]: Log(event_log) successfully connected to Zscaler Cloud: [10.0.0.4]:52552;broker4.was1.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Get connector returned ZPN_RESULT_NOT_FOUND, please contact customer support, if this persists
Aug 21 13:08:37 zpa-connector zpa-connector-child[1710]: FOMH creating thread pool control with threads 0->3
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Initialization completed
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Connector waiting for connection
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Broker control connected
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Broker data connected
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Broker data transferred
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Mtunneled(all)health-report-based[no-health-report-based], total 0|0|0, to broker 0|0|0, to private broker 0|0|0, unbond/error
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 0, Bindack 0, AppRtDisc 0, DnsChk 0, MtunnelEnd 0 TagPause 0 TagResume 0 WinUpdate 0 Redirect 0 TX: Br
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Registered apps count 0, alive apps 0, apps with on-access health 0, apps with no health reporting 0, service count 0, target count 0
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Time skew: local time lags cloud time by 0.000000s
[root@zpa-connector admin]#
```

Use journalctl -u zpa-connector > "filename" to save status logs to a file



Slide notes

You can also save the **journalctl** command output to a file which can then be viewed or copied off the App Connector and attached to a support ticket.

Slide 35 - Slide 35

```
root@zpa-connector:~# journalctl -n100 | grep target
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.251
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.249
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.253
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Adding name resolution for co2br.prod.zpath.net of 165.225.9.254
Aug 21 10:38:35 zpa-connector zpa-connector-child[1710]: Log(event log) successfully connected to Zscaler Cloud: [10.0.0.4]:52552;broker4.wasl.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 10:38:36 zpa-connector zpa-connector-child[1710]: Get connector returned ZEN_RESULT_NOT_FOUND, please contact customer support, if this persists
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: FOHH creating thread pool control with threads 0->3
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Running with connector GID = 144123469846545379, name = NYC_HQ-1
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Initialization Complete
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Connector- waiting for time synchronization
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: ----- Connector Status:ID=144123469846545379:Name=NYC_HQ-1:Ver=20.51.3:Mem(System|Process)=10%|0%:Disk Avail=6.96GB:CPU=0%
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Certificate will expire in 371 days, 22 hours, 13 minutes, 13 seconds
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker config connection, state fohh connection_connected, [10.0.0.4]:52552;broker4.wasl.prod.zpath.net:[165.225.9.252]:443;1
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker control connection, state fohh_connection_unresolved, [uninitialized]:0;any.co2br.prod.zpath.net:[uninitialized]:0;1 up
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker data connection, total 0, active 0, backed off connections 0
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Broker data transfer, to broker 0 bytes, from broker 0 bytes
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Mtnnels(all)health-report-based[no-health-report-based], total 0|0|0, to broker 0|0|0, to private broker 0|0|0, unbound/error
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 0, BindAck 0, AppRtDisc 0, DnsSchk 0, MtunnelEnd 0 TagPause 0 TagResume 0 WinUpdate 0 Redirect 0 TX: Br
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: Registered apps count 0, alive apps 0, apps with on-access health 0, apps with no health reporting 0, service count 0, target
Aug 21 10:38:37 zpa-connector zpa-connector-child[1710]: time skew: local time lags cloud time by 0.000000s

[root@zpa-connector admin]# journalctl -n100 | grep target
Aug 21 13:03:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, targe
count 27, target alive 26
Aug 21 13:04:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, targe
count 27, target alive 26
Aug 21 13:05:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, targe
count 27, target alive 26
Aug 21 13:06:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, targe
count 27, target alive 26
Aug 21 13:07:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, targe
count 27, target alive 26
Aug 21 13:08:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, targe
count 27, target alive 26
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, targe
count 27, target alive 26
[root@zpa-connector admin]# journalctl -u zpa-connector >journal.txt
[root@zpa-connector admin]# ls
journal.txt provision_key
[root@zpa-connector admin]#
```



Slide notes

Slide 36 - Slide 36

```
root@zpa-connector:~# 
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Certificate will expire in 371 days, 19 hours, 42 minutes, 13 seconds
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Broker config connection, state fohh_connection_connected, [10.0.0.4]:60534;broker2.was1.prod.zpath.net:[165.225.9.250]:443;1
uptime 2H:31M:28, rtt: 74216 us
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Log(event_log) connection, state fohh_connection_connected, [10.0.0.4]:52552;broker4.was1.prod.zpath.net:[165.225.9.252]:443;1
uptime 2H:31M:28, rtt: 19004 us
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Broker control connection, state fohh_connection_connected, [10.0.0.4]:45092;broker1.nyc3.prod.zpath.net:[165.225.221.253]:443
:1 uptime 2H:30M:57S, rtt: 19012 us
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Broker data connection, total 2, active 2, backed off connections 0
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Broker data transfer, to broker 8932216 bytes, from broker 156801 bytes
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Mtunnels(all)health-report-based[no-health-report-based], total 79[79]0, to broker 79[79]0, to private broker 0[0]0, unbound/errorred 0, current active 1[1]0, peak active 26
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 79, BindAck 79, AppRtDisc 32, DnsChk 46, MtunnelEnd 114 TagPause 0 TagResume 0 WinUpdate 248 Redirect 1 TX: BrkRqAck 0[0], BindReg 79[0], AppRtReg 1109010, HealthRp 501510 DnsChk 46
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: Time skew: local time lags cloud time by 0.046941s
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: File descriptors(max|in-use): System 103415[1664, Process 102400]105
Aug 21 13:09:37 zpa-connector zpa-connector-child[1710]: System Sockets: Created 221 TCP4 in-use 13, TCP4 time-wait 2, UDP4 in-use 8, TCP6 in-use 2, UDP6 in-use 5, Ports available per interface 28232, IPv4 interfaces 2, IPv6 interfaces 2
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: ----- Connector Status:ID=144123469046545379;Name=NYC_HQ-1;Ver=20.51.3;Mem(System|Process)=10%|0%;Disk Avail=6.96GB;CPU=0%
-----
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Certificate will expire in 371 days, 19 hours, 41 minutes, 13 seconds
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Broker config connection, state fohh_connection_connected, [10.0.0.4]:60534;broker2.was1.prod.zpath.net:[165.225.9.250]:443;1
uptime 2H:32M:28, rtt: 87470 us
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Log(event_log) connection, state fohh_connection_connected, [10.0.0.4]:52552;broker4.was1.prod.zpath.net:[165.225.9.252]:443;1
uptime 2H:32M:28, rtt: 4455 us
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Broker control connection, state fohh_connection_connected, [10.0.0.4]:45092;broker1.nyc3.prod.zpath.net:[165.225.221.253]:443
:1 uptime 2H:31M:57S, rtt: 10605 us
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Broker data connection, total 2, active 2, backed off connections 0
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Broker data transfer, to broker 8932216 bytes, from broker 156801 bytes
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Mtunnels(all)health-report-based[no-health-report-based], total 79[79]0, to broker 79[79]0, to private broker 0[0]0, unbound/errorred 0, current active 1[1]0, peak active 26
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: RPC Messages, RX: BrkRq 79, BindAck 79, AppRtDisc 32, DnsChk 46, MtunnelEnd 114 TagPause 0 TagResume 0 WinUpdate 248 Redirect 1 TX: BrkRqAck 0[0], BindReg 79[0], AppRtReg 1117510, HealthRp 506010 DnsChk 48
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Registered apps count 7, alive apps 7, apps with on-access health 5, apps with no health reporting 0, service count 11, target count 27, target alive 26
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: Time skew: local time lags cloud time by 0.048100s
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: File descriptors(max|in-use): System 103415[1664, Process 102400]104
Aug 21 13:10:37 zpa-connector zpa-connector-child[1710]: System Sockets: Created 220 TCP4 in-use 12, TCP4 time-wait 3, UDP4 in-use 8, TCP6 in-use 2, UDP6 in-use 5, Ports available per interface 28232, IPv4 interfaces 2, IPv6 interfaces 2
[root@zpa-connector admin]# 
```



Slide notes

Slide 37 - Troubleshooting Tools – App Connector CLI Commands

Troubleshooting Tools – App Connector CLI Commands

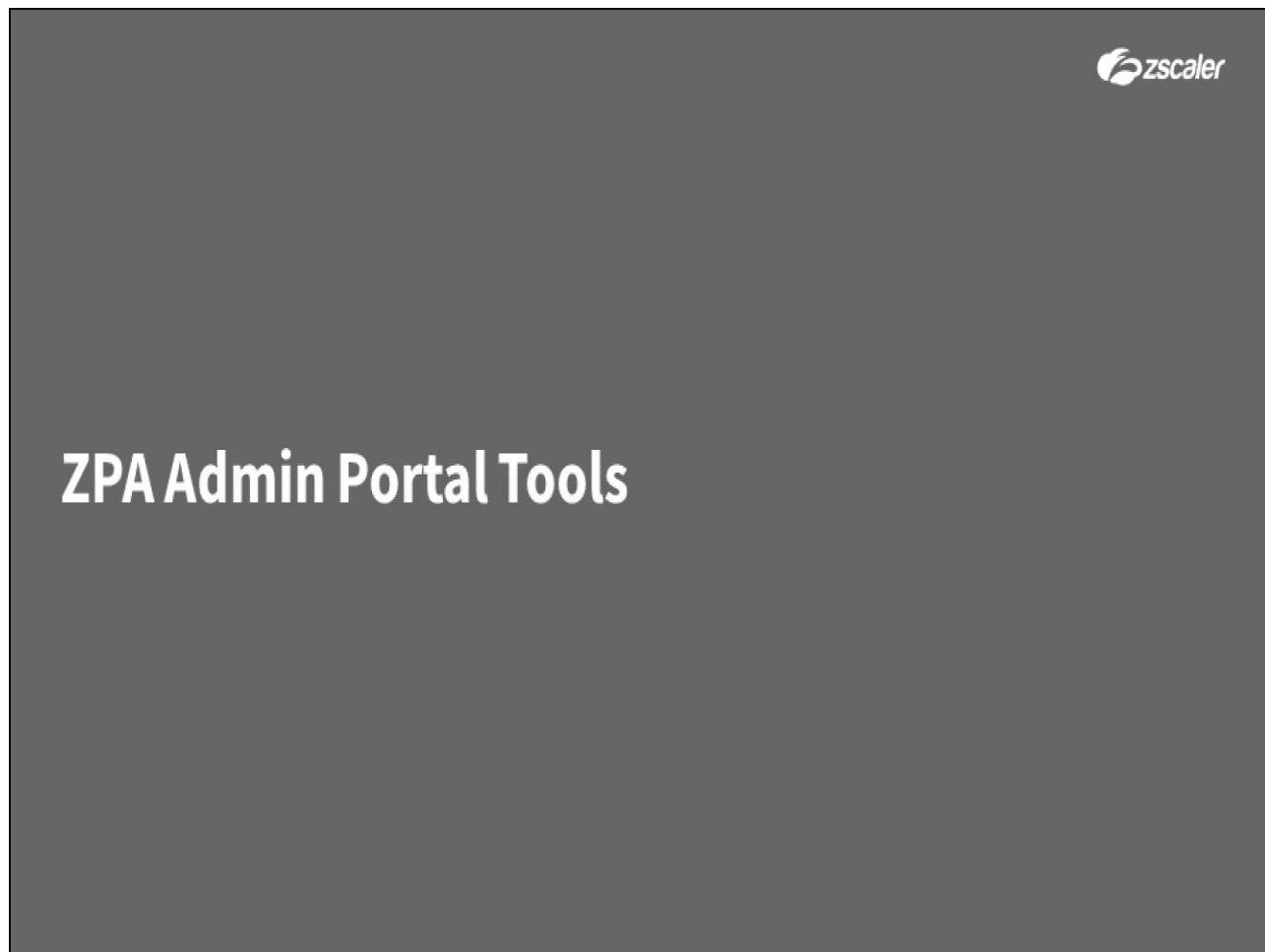
The screenshot shows a web browser window with the ZPA Admin Portal. The title bar says "Monitoring App Connector Performance". The content area discusses monitoring App Connectors and provides links to "App Connector Deployment Prerequisites" and "Networking Deployed App Connectors". It also mentions using the "App Connector Dashboard" and "Health Dashboard". A section titled "CPU Utilization" is expanded, explaining that peak utilization should be less than 75% and providing examples. Below this, another section discusses monitoring CPU utilization using "top" and "sysstat" commands, with a link to "https://help.zscaler.com/zpa/monitoring-connector-performance".

<https://help.zscaler.com/zpa/monitoring-connector-performance>

Slide notes

There are many more CLI commands available for Connector VMs. The Help portal URL listed here provides more detailed information about options to monitor and troubleshoot App Connectors.

Slide 38 - ZPA Admin Portal Tools

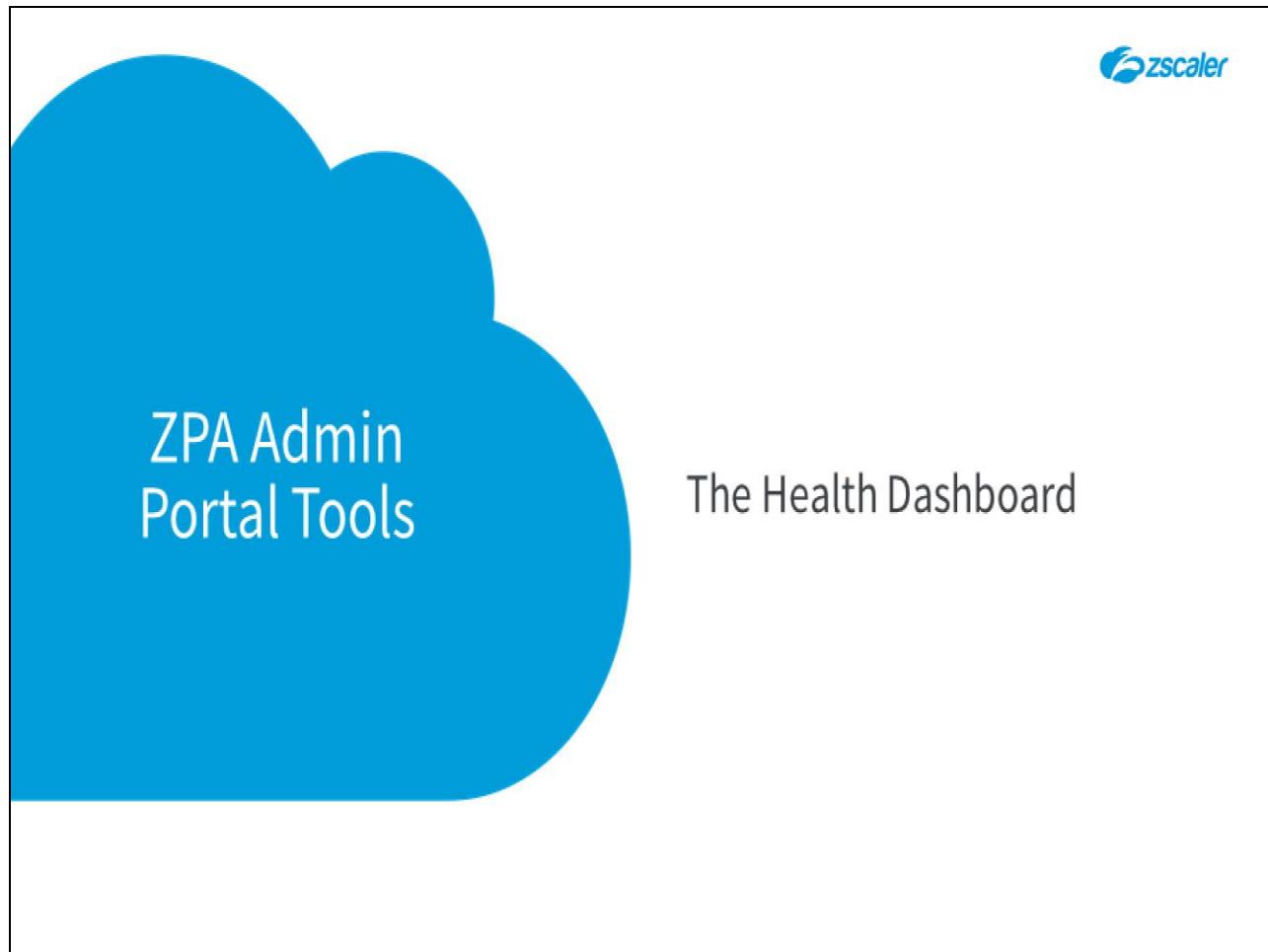


Slide notes

In the final section, we will look at some of the ZPA admin portal troubleshooting tools available, specifically the **Health** Dashboard, and the **Diagnostics** page.

This section has been created as an interactive demo to give you a feel for the navigation of the ZPA admin portal. You will be asked to select the appropriate menu options to navigate the UI. You may also use the **Play** control to proceed to the next step.

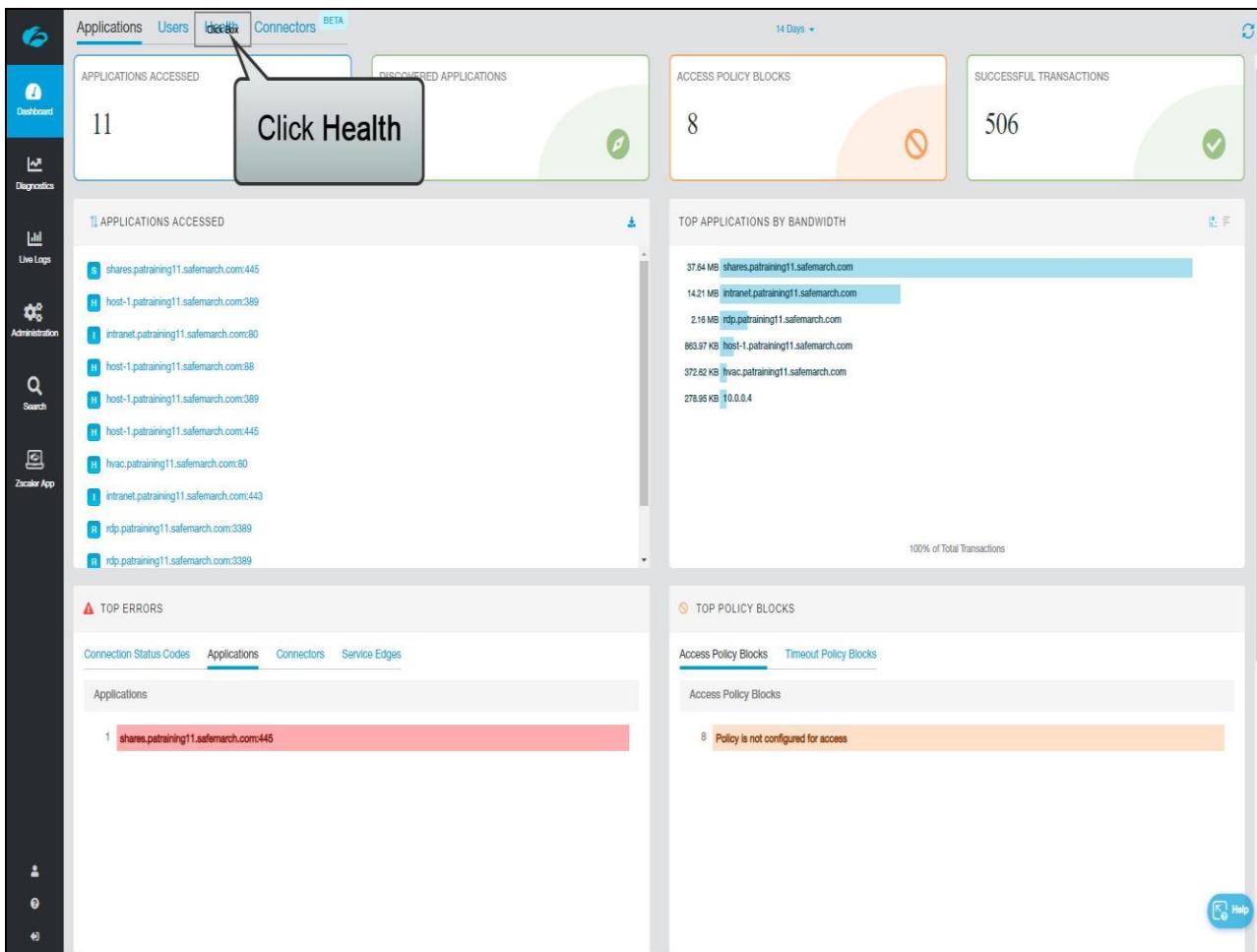
Slide 39 - ZPA Admin Portal Tools



Slide notes

The first ZPA admin portal tool that we will look at, is the **Health** Dashboard.

Slide 40 - Slide 40



Slide notes

Login to the ZPA admin portal and click **Health**.

Slide 41 - Slide 41

The screenshot shows the ZCTA-PA Health Dashboard interface. On the left, there is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and ZPA App. The main area has three tabs: Applications, Users, Health (selected), and Connectors (BETA). The Applications section displays 11+ applications with icons like S, H, R, and I, and names such as shares.patraining11.safemarch.com, host-1.patraining11.safemarch..., rdp.patraining11.safemarch.com, 10.0.0.4, host-1.patraining11.safemarch..., and 1.patraining11.safemarch... A search bar with the placeholder "Click Search" is overlaid on the top right of the Applications grid. The Connectors section displays 5+ connectors with icons showing network structures and names like Azure-East-1, Azure-East-3, LSS-1, LSS-2, and NYC_HQ-1. At the bottom right of the dashboard is a "Help" icon.

Slide notes

The **Health** Dashboard has three sections for; **APPLICATIONS**, **APP CONNECTORS**, and **ZPA PRIVATE SERVICE EDGES**. In this demonstration, we will focus on Applications and App Connectors.

At top right, there are **Search** and **Refresh** tools. To focus in on a specific application or connector, click **Search...**

Slide 42 - Slide 42

The screenshot shows the Zscaler Cloud Control Center interface. On the left, there is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for Applications, Users, Health, and Connectors, with 'Connectors' currently selected. The 'BETA' label is visible above the tabs.

APPLICATIONS section: Displays 11+ Applications (May vary over time). The applications listed are:

- shares.patraining11.safemarch.com (Status: S, Red)
- host-1.patraining11.safemarch.... (Status: H, Yellow)
- rdp.patraining11.safemarch.com (Status: R, Yellow)
- rdp.patraining11.safemarch.com (Status: R, Yellow)
- 10.0.0.4 (Status: 1, Green)
- host-1.patraining11.safemarch.... (Status: H, Yellow)
- host-1.patraining11.safemarch.... (Status: H, Yellow)
- host-1.patraining11.safemarch.... (Status: H, Yellow)
- hvac.patraining11.safemarch.com (Status: H, Green)
- intranet.patraining11.safemarch.com (Status: I, Green)
- intranet.patraining11.safemarch.com (Status: I, Green)
- shares.patraining11.safemarch.com (Status: S, Green)

CONNECTORS section: Displays 5+ Connectors (May vary over time). The connectors listed are:

- Azure-East-1
- Azure-East-3
- LSS-1
- LSS-2
- NYC_HQ-1

Slide notes

...and enter your search criteria.

Slide 43 - Slide 43

The screenshot shows the Zimbra Admin UI interface. The top navigation bar includes tabs for Applications, Users, Health, and Connectors (BETA). On the left, a sidebar lists various management sections: Dashboard, Diagnostics, Live Logs, Administration, Search, and Zimbra App. The main content area is titled "APPLICATIONS" and displays "2+ Applications (May vary over time)". Two application entries are visible, both labeled "rdp.patraining11.safemarch.com" and marked with a red question mark icon. A red rectangular box highlights these two entries. Below this is a "CONNECTORS" section with "0+ Connectors (May vary over time)". The bottom right corner features a "Help" button.

Slide notes

The dashboard now only shows items that match the search criteria.

Slide 44 - Slide 44

The screenshot shows the ZCTA-PA Troubleshooting Tools Dashboard. On the left, there is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zacker App. The main area has two sections: 'APPLICATIONS' and 'CONNECTORS'. The 'APPLICATIONS' section displays 11 applications with icons and names like 'shares.patraining11.safemarch.com', 'host-1.patraining11.safemarch...', 'rdp.patraining11.safemarch.com', etc. The 'CONNECTORS' section displays 5 connectors with icons and names like 'Azure-East-1', 'Azure-East-3', 'LSS-1', 'LSS-2', and 'NYC_HQ-1'. Both sections have a set of four status filters on the right side, each represented by a blue square with a white icon: a green circle with an upward arrow (Up), a red circle with a downward arrow (Down), a yellow circle with a question mark (Unhealthy), and a grey circle with a question mark (Unknown). The 'Up' filter is highlighted with a red border.

Slide notes

By default, the Dashboard shows all objects, regardless of their current status.

A set of status display filters on the right side allow you to choose the set of objects to view for each section independently. You can view objects in any combination of the statuses; **Up**, **Down**, **Unhealthy**, and **Unknown**.

Slide 45 - Health States

Health States



- Applications

 echo.mockcompany.com	Application is up No Health Check = Always Up!	 hp.mockcompany.com	Application is down
 portal.mockcompany.com	Application is unhealthy	 intranet.mockcompany.com	Application status unknown

Slide notes

For Applications the health states are as follows:

- **Up:** The application is up and functioning as expected. Note also that if an application has Health Check disabled, the Connector always reports the health status as up.
- **Down:** The application is down and not accessible to users. This is most likely because a server that hosts the application is down or unhealthy.
- **Unhealthy:** The application is unhealthy but still accessible to users. An application may have multiple servers that host it, and at least one of those servers is unhealthy or down, but because there's at least one server for the application that is up, users can still access the application.

- **Unknown:** The application health is unknown. This status is shown only for applications configured with ‘On Access’ health reporting. It indicates that ZPA has stopped reporting the health of this application because it has been more than 30 minutes since a user has accessed it. ZPA reports the health status as soon as a user accesses the application again.

Slide 46 - Health States

Health States

The diagram illustrates various health states for applications and servers. It uses colored boxes (green for up, orange for unhealthy, red for down) and question marks to indicate unknown status.

- Applications:**
 - echo.mockcompany.com (E): Application is up (Green)
 - hp.mockcompany.com (H): Application is down (Red)
 - portal.mockcompany.com (P): Application is unhealthy (Orange)
 - intranet.mockcompany.com (I): Application status unknown (Black)
- Servers:**
 - Portal Server 2, Oregon: Server is up (Green)
 - Portal Server 1, Oregon: Server is down (Red)
 - Portal Server 2, Oregon: Server is unhealthy (Orange)
 - 104.80.88.15: Server status unknown (Black)

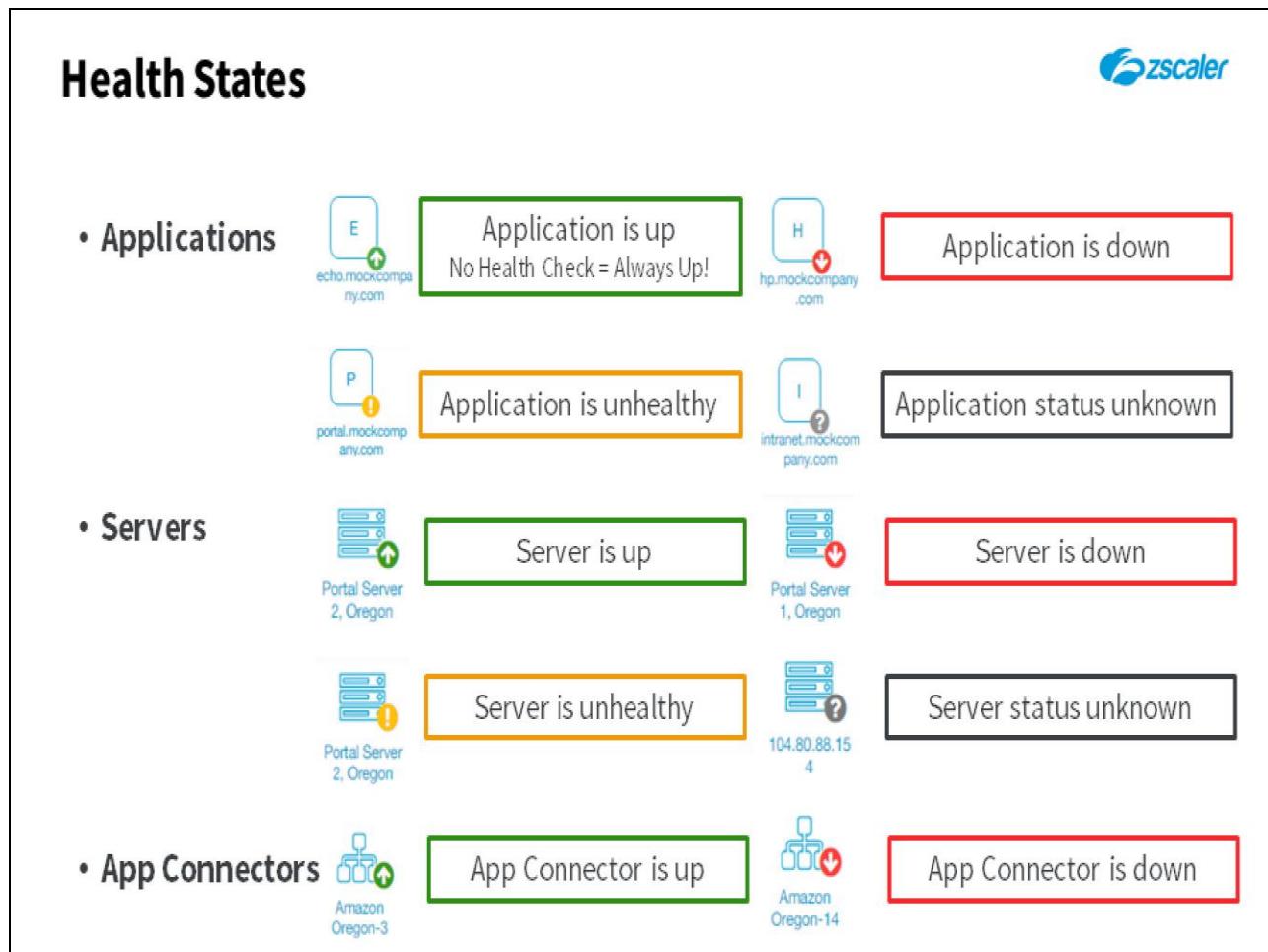
Slide notes

For Servers the health states are as follows:

- **Up:** The server is up and functioning as expected.
- **Down:** The server is down and not functional.
- **Unhealthy:** The server is unhealthy because of one or more of the following reasons: On the server, at least one port used for an application is functioning, but there is also at least one port for an application that is not functioning; At least one of the Connectors that has access to this server is down.

- **Unknown:** Server health is unknown. This status is shown only for servers that have been dynamically discovered. It indicates that ZPA has stopped reporting the health of this server because it has been more than 30 minutes since a user has accessed it. ZPA will begin monitoring the health of the server again as soon as a user accesses an application hosted by this server.

Slide 47 - Health States



Slide notes

For Connectors the health states are as follows:

- **Up:** The Connector is up and functioning as expected.
- **Down:** The Connector is down and not functional.

Slide 48 - Slide 48

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zacker App. The main area has tabs for Applications, Users, Health, and Connectors (BETA). The Applications section displays 11+ applications with various status icons (S, H, R, 1) and names like shares.patraining11.safemarch.com, host-1.patraining11.safemarch..., and rdp.patraining11.safemarch.com. The Connectors section shows 5+ connectors with icons like Azure-East-1, Azure-East-3, LSS-1, LSS-2, and NYC_HQ-1. A callout box with the text "Unselect Up filter" points to the "Up" filter button in the Applications section's filter toolbar.

Slide notes

To view **APPLICATIONS** in the Down, Unhealthy and Unknown **state**, click to unselect the **Up** filter...

Slide 49 - Slide 49

The screenshot shows the Zscaler Cloud Control Center interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for Applications, Users, Health, and Connectors, with 'Connectors' currently selected. A 'BETA' label is visible above the connectors section.

APPLICATIONS (11+ Applications, May vary over time):

- shares.patraining11.safemarch.com (Status: Down, icon with red dot)
- host-1.patraining11.safemarch.... (Status: Unhealthy, icon with yellow question mark)
- rdp.patraining11.safemarch.com (Status: Up, icon with green checkmark)
- rdp.patraining11.safemarch.com (Status: Up, icon with green checkmark)

CONNECTORS (5+ Connectors, May vary over time):

- Azure-East-1
- Azure-East-3
- LSS-1
- LSS-2
- NYC_HQ-1

Slide notes

...and the display will be limited to applications that are not in the **Up** status. Toggle the filters in each section to display the objects and statuses of interest to you. Applications that are in the Down, or Unhealthy status are the ones that you probably need to focus your troubleshooting efforts on.

Slide 50 - Slide 50

The screenshot shows the Zscaler Cloud Control Center interface. On the left, a sidebar contains icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for Applications, Users, Health, and Connectors, with the Connectors tab currently selected (labeled 'BETA').

APPLICATIONS section: Displays 11+ Applications (May vary over time). Items include: shares.patraining11.safemarch.com (highlighted with a red box), host-1.patraining11.safemarch..., rdp.patraining11.safemarch..., rdp.patraining11.safemarch... 10.0.0.4, host-1.patraining11.safemarch..., host-1.patraining11.safemarch..., host-1.patraining11.safemarch..., and hvac.patraining11.safemarch.com.

CONNECTORS section: Displays 5+ Connectors (May vary over time). Items include: Azure-East-1 (highlighted with a red box), Azure-East-3, LSS-1, LSS-2, and NYC_HQ-1.

A tooltip in the bottom-left corner of the Applications section says: "Mouseover an item to view details".

Slide notes

If you mouseover an item in this Dashboard, a pop-up tool tip will display additional information about it.

Slide 51 - Slide 51

The screenshot shows the Zscaler Cloud interface with the 'Connectors' tab selected. The left sidebar includes links for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App.

APPLICATIONS (11+ Applications):

- shares.patraining11.safemarch.com (Port: 139, Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- rdp.patraining11.safemarch.com (Protocol Type: RDP, Last Updated: Aug 21st, 16:56 PM (EDT))
- 10.0.0.4 (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- host-1.patraining11.safemarch... (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- host-1.patraining11.safemarch... (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- host-1.patraining11.safemarch... (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- hvac.patraining11.safemarch.com (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- intranet.patraining11.safemarch.com (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- intranet.patraining11.safemarch.com (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))
- shares.patraining11.safemarch.com (Protocol Type: TCP, Last Updated: Aug 21st, 16:56 PM (EDT))

CONNECTORS (5+ Connectors):

- Azure-East-1
- Azure-East-3
- LSS-1
- LSS-2
- NYC_HQ-1

Slide notes

For Applications, you can see the application **Name**, the **Port**, the **Protocol Type**, and the **Last Updated** date and time.

Slide 52 - Slide 52

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zacker App. The main area has tabs for Applications, Users, Health, and Connectors (BETA). The Applications section displays 11+ applications with icons like S, H, R, 1, and 10.0.0.4, and hostnames such as shares.patraining11.safemarch.com, host-1.patraining11.safemarch.com, rdp.patraining11.safemarch.com, 10.0.0.4, host-1.patraining11.safemarch.com, host-1.patraining11.safemarch.com, host-1.patraining11.safemarch.com, and hvac.patraining11.safemarch.com. The Connectors section displays 5+ connectors with icons for Azure-East-1, SS-1, LSS-2, and NYC_HQ-1. A detailed info box for Azure-East-1 shows the following data:

Name: Azure-East-1
Last Updated: Aug 21st, 16:56 PM (EDT)
Public IP: 168.62.37.56
Private IP: 10.0.0.7
CPU Utilization: 1%
Memory Utilization: 11%
Up Time: 1 day(s) 2 hrs 44 mins
Active Apps: 2

Slide notes

For **Connectors** you can see; the Connector **Name**, the **Last Updated** date and time, the **Public IP** address (if available), the **Private IP** address (if available), the **CPU Utilization**, the **Memory Utilization**, the **Uptime**, and the **number of active apps**.

Slide 53 - Slide 53

The screenshot shows the Zscaler Cloud Control Center interface. On the left, a vertical sidebar contains icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for Applications, Users, Health, and Connectors, with 'Connectors' currently selected (labeled 'BETA').

APPLICATIONS section: Displays 11+ Applications (May vary over time). One item, 'Click Box' (shales.patraining11.safemarch.com), is highlighted with a red circle and a callout box containing the text 'Click on an item to drill down'. Other items include 'host-1.patraining11.safemarch.com', 'rdp.patraining11.safemarch.com', '10.0.0.4', 'host-1.patraining11.safemarch.com', 'host-1.patraining11.safemarch.com', and 'hvac.patraining11.safemarch.com'.

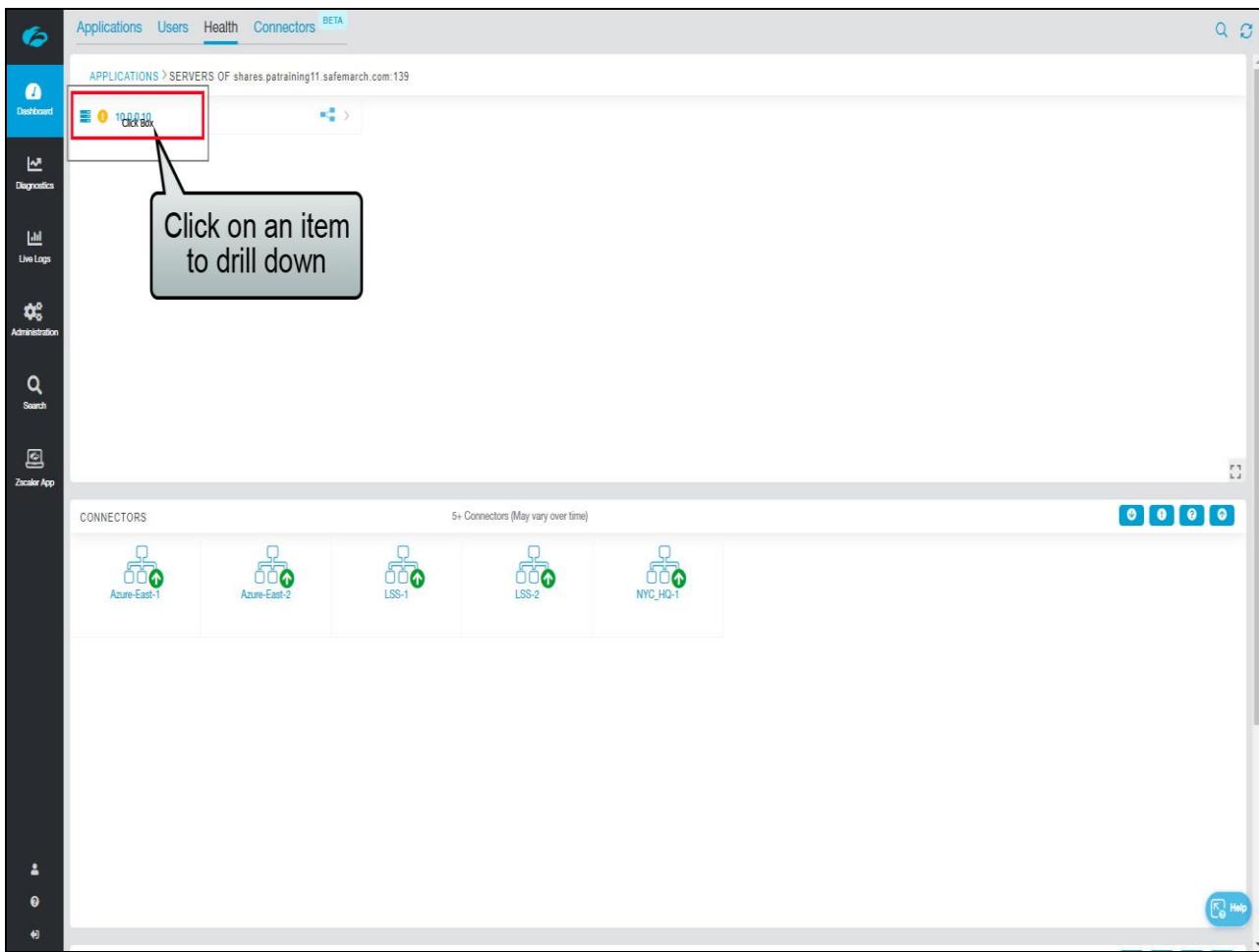
CONNECTORS section: Displays 5+ Connectors (May vary over time). Items listed are 'Azure-East-1', 'Azure-East-3', 'LSS-1', 'LSS-2', and 'NYC_HQ-1'.

Slide notes

For each object on the Dashboard, you can drill down to see related objects. For example, if you click on an **Application**,

...

Slide 54 - Slide 54



Slide notes

...you will see the related **Server**, and its status. If you click on that **Server**, ...

Slide 55 - Slide 55

The screenshot shows the Zimbra Admin interface with the 'Connectors' tab selected. The left sidebar includes links for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zimbra App. The main content area displays a list of connectors under the heading 'CONNECTORS'. It shows five connectors: Azure-East-1, Azure-East-3, LSS-1, LSS-2, and NYC_HQ-1. Each connector is represented by a small icon showing a tree structure with green arrows indicating status. A red box highlights the 'NYC_HQ-1' connector. The top navigation bar shows the path: APPLICATIONS > SERVERS OF shares.patraining11.safemarch.com:139 > CONNECTORS OF 10.0.0.10.

Slide notes

...you will see the related **Connectors**, and their status.

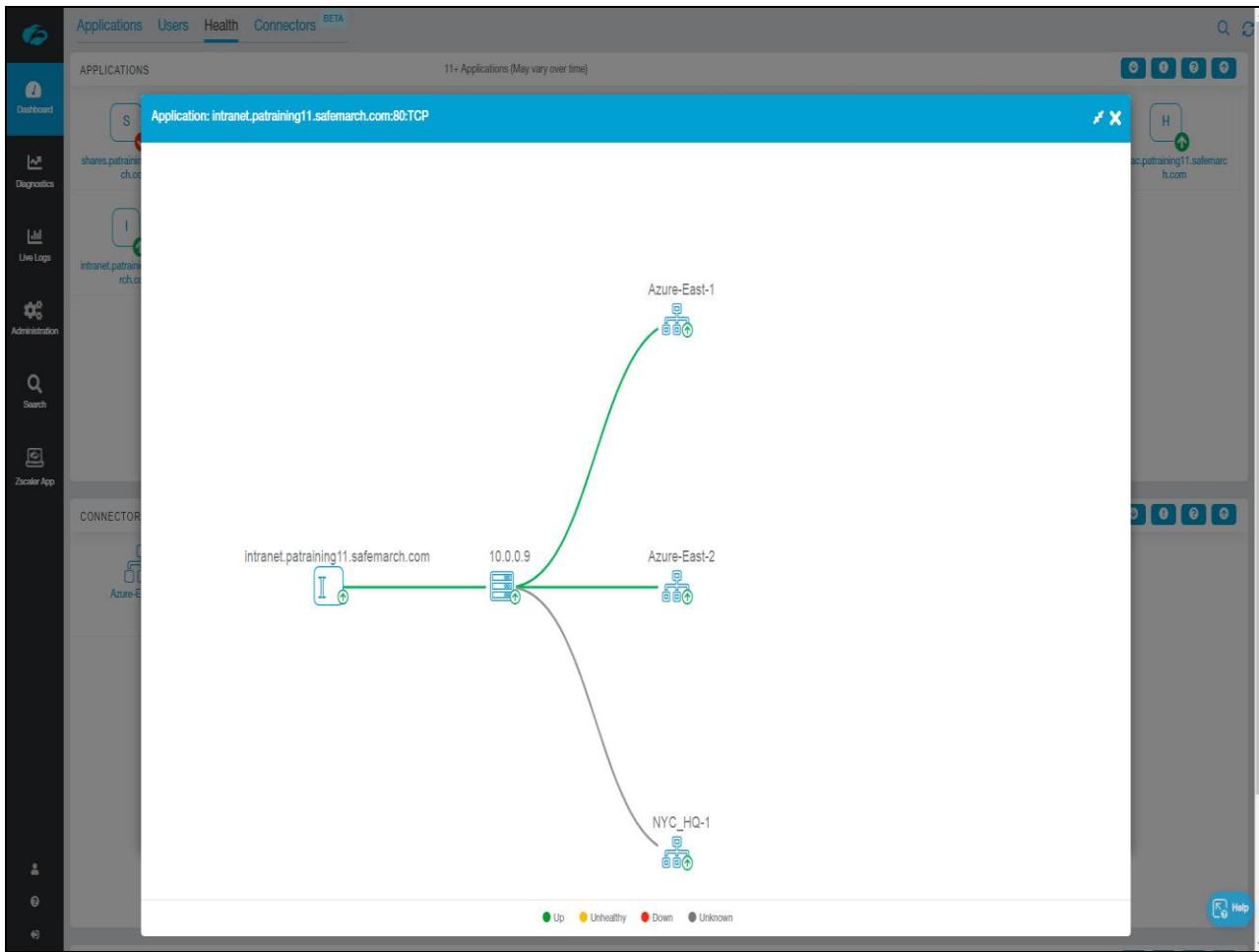
Slide 56 - Slide 56



Slide notes

If you mouseover an object, you have the option to click to view the connectivity map for that object, ...

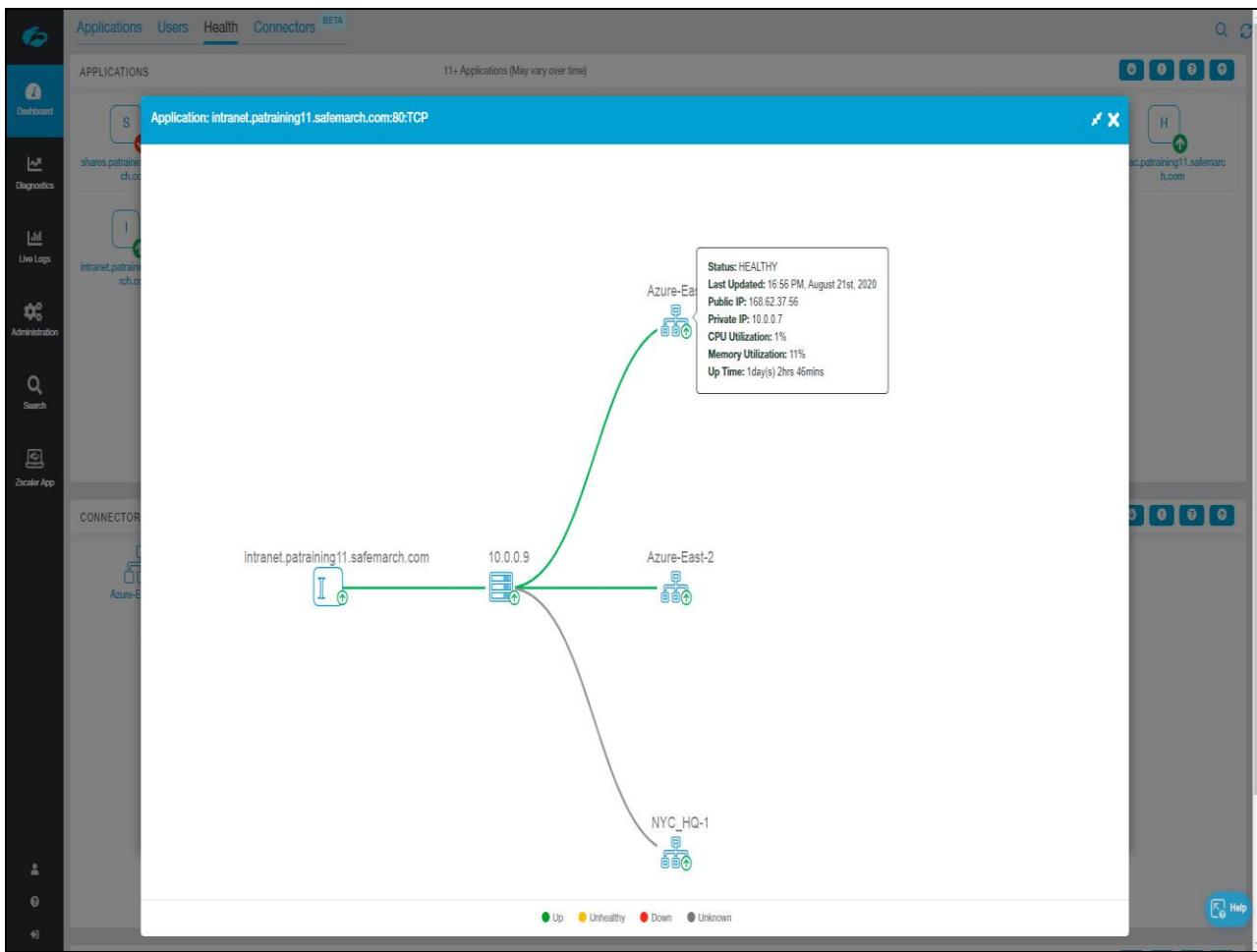
Slide 57 - Slide 57



Slide notes

...which indicates in a graphical form the relationship between this object and the related objects. In this example, we can see a one-to-one relationship between the **Application** and **Server**, but a one-to-many relationship between the **Server** and **Connectors**.

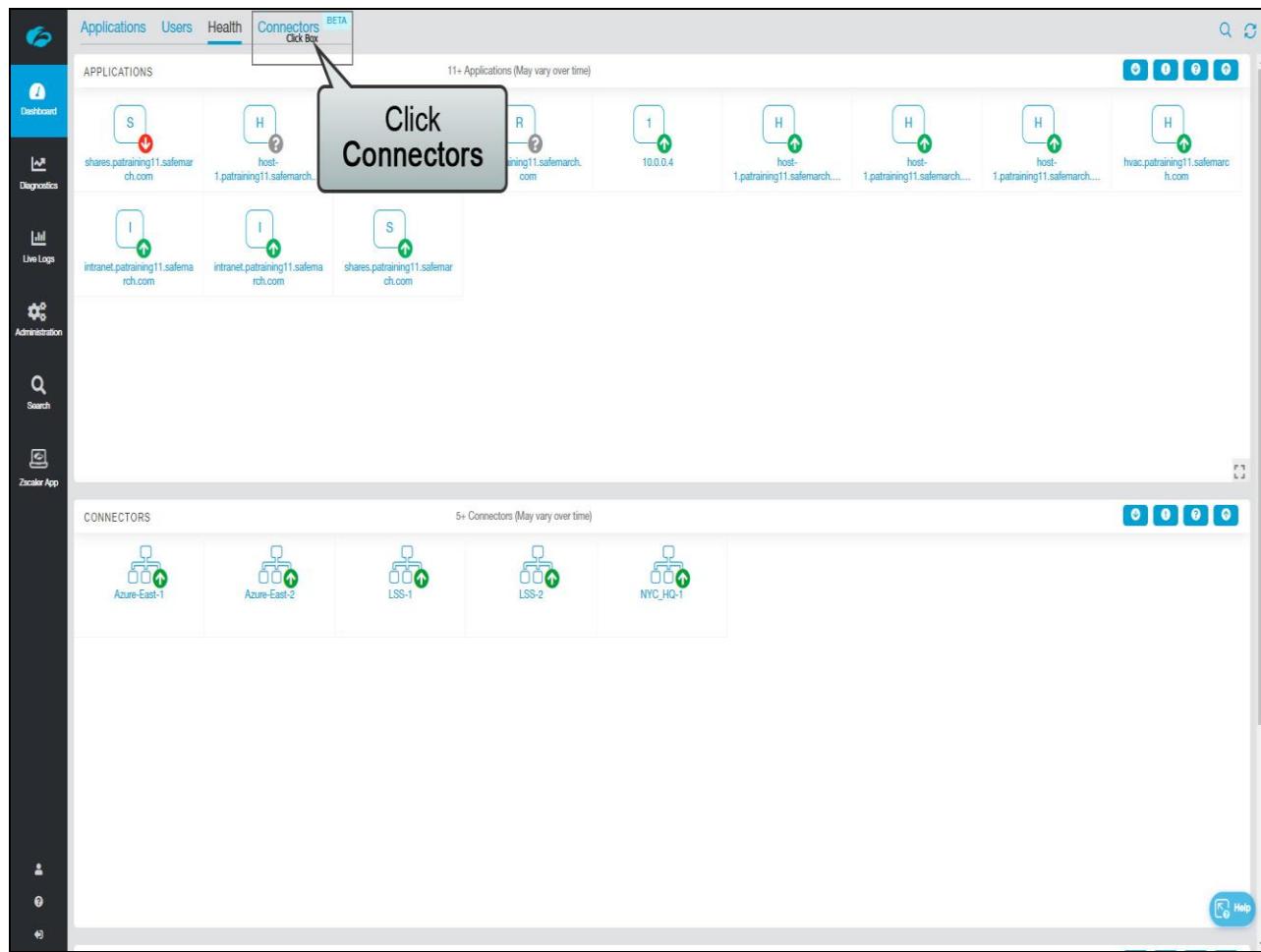
Slide 58 - Slide 58



Slide notes

As before, you can mouseover an object to view more details.

Slide 59 - Slide 59



Slide notes

Next, click **Connectors**.

Slide 60 - Slide 60

The screenshot shows the Zscaler Connectors dashboard with a sidebar containing links for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has four widgets:

- CPU UTILIZATION**: Shows connector names, group names, locations, and CPU usage. A red box highlights the table.
- MEMORY UTILIZATION**: Shows connector names, group names, locations, and memory usage. A red box highlights the table.
- BYTES (RECEIVED AND TRANSMITTED)**: Shows connector names, group names, locations, and byte counts. A red box highlights the table.
- NEW APPLICATION TUNNELS**: Shows connector names, group names, locations, and tunnel counts. A red box highlights the table.

A red box highlights the "Time period" dropdown at the top right, which is set to "30 Mins". A callout bubble points to this dropdown with the text "Time period".

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	1 %	
Azure-East-1	Azure-East	New York, US	1 %	
Azure-East-2	Azure-East	New York, US	1 %	
LSS-1	LSS	New York, US	1 %	
LSS-2	LSS	New York, US	1 %	

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	18 %	
Azure-East-1	Azure-East	New York, US	11 %	
Azure-East-2	Azure-East	New York, US	11 %	
LSS-1	LSS	New York, US	11 %	
LSS-2	LSS	New York, US	11 %	

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	11.74 MB	
Azure-East-2	Azure-East	New York, US	2.99 MB	
LSS-1	LSS	New York, US	2.87 MB	
Azure-East-1	Azure-East	New York, US	2.49 MB	
LSS-2	LSS	New York, US	2.29 MB	

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	13	
Azure-East-2	Azure-East	New York, US	8	
Azure-East-1	Azure-East	New York, US	7	
LSS-1	LSS	New York, US	1	

Slide notes

The **Connectors** dashboard provides information about the App Connectors for your organization. The display can be filtered for periods between 30 mins. to 24 Hours, or you can select a Custom Range.

Then there are four widgets:

- The **CPU Utilization** table displays up to 100 App Connectors that use the most CPU at a point in the selected time frame.
- The **Memory Utilization** table displays up to 100 App Connectors that use the most memory at a point in the selected time frame.

- The **Bytes Received and Transmitted** table displays up to 100 App Connectors that use the most bytes while receiving and transmitting data, across all interfaces of the App Connector, in the selected time frame.
- And the **New Application tunnels** table displays up to 100 App Connectors that have the largest number of Microtunnels (M-Tunnels) connecting to it compared to the previous time interval, which is 5 minutes. This count reflects the number of application connections served by the App Connector.

Slide 61 - Slide 61

The screenshot shows the Zscaler App Connector Dashboard with the following sections:

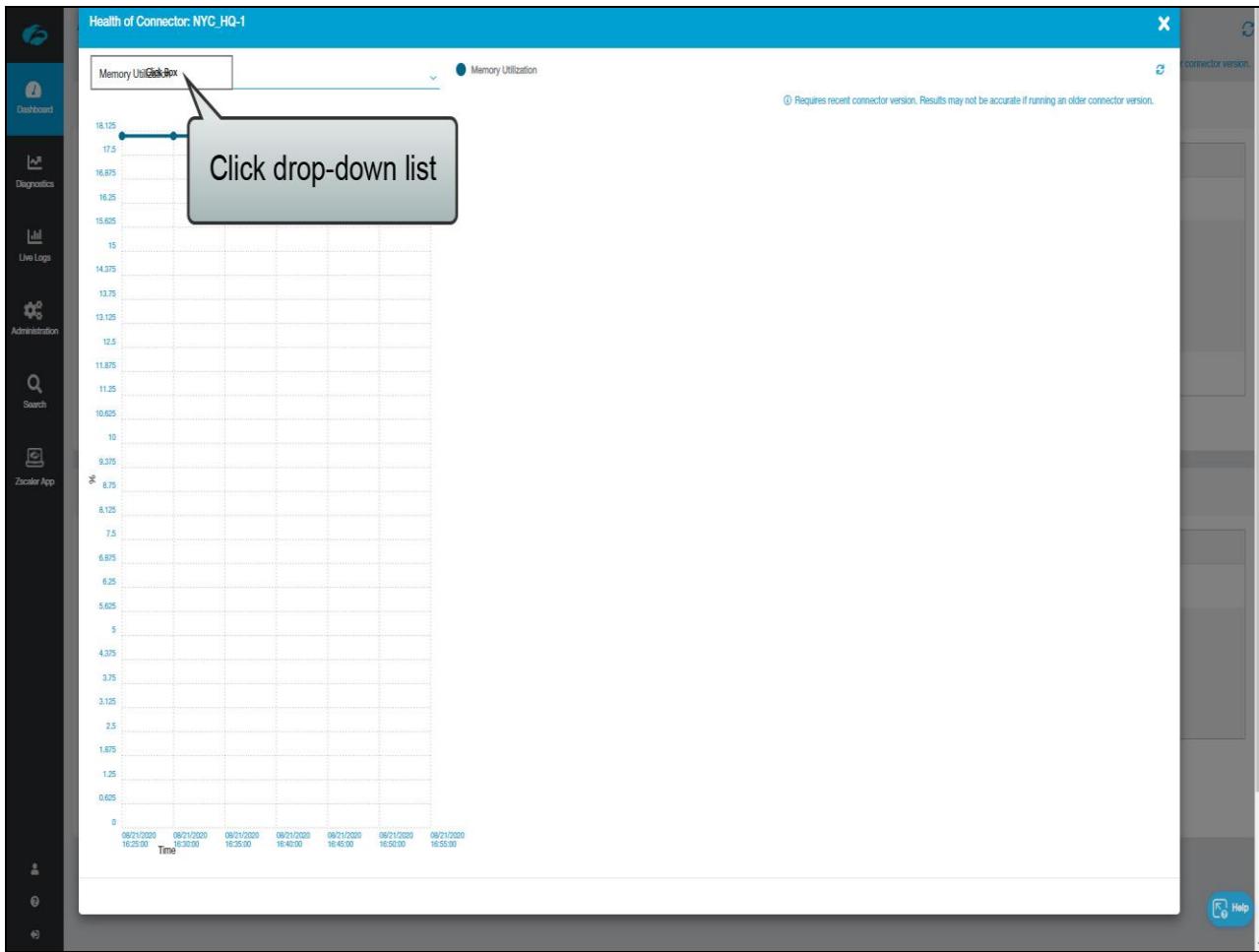
- CPU UTILIZATION:** Shows connector names (NYC_HQ-1, Azure-East-1, Azure-East-2, LSS-1, LSS-2) grouped by connector group (NYC_HQ, Azure-East, LSS). All show 1% value.
- MEMORY UTILIZATION:** Shows connector names (NYC_HQ-1, Azure-East-1, Azure-East-2, LSS-1, LSS-2) grouped by connector group (NYC_HQ, Azure-East, LSS). Values are 18%, 11%, 10%, 10%, and 10% respectively. A callout bubble points to the "Click to view Health Charts" button next to the first row.
- BYTES (RECEIVED AND TRANSMITTED):** Shows connector names (NYC_HQ-1, Azure-East-2, LSS-1, Azure-East-1, LSS-2) grouped by connector group (NYC_HQ, Azure-East, LSS). Values range from 11.74 MB to 2.29 MB.
- NEW APPLICATION TUNNELS:** Shows connector names (NYC_HQ-1, Azure-East-2, Azure-East-1, LSS-1) grouped by connector group (NYC_HQ, Azure-East, LSS). Values range from 13 to 1.

A callout bubble with the text "Click to view Health Charts" points to the "Click to view Health Charts" button in the Memory Utilization section.

Slide notes

From any table in the dashboard, you can click on the **Health Chart** icon for an App Connector to see how it performed for that area of the App Connector's health.

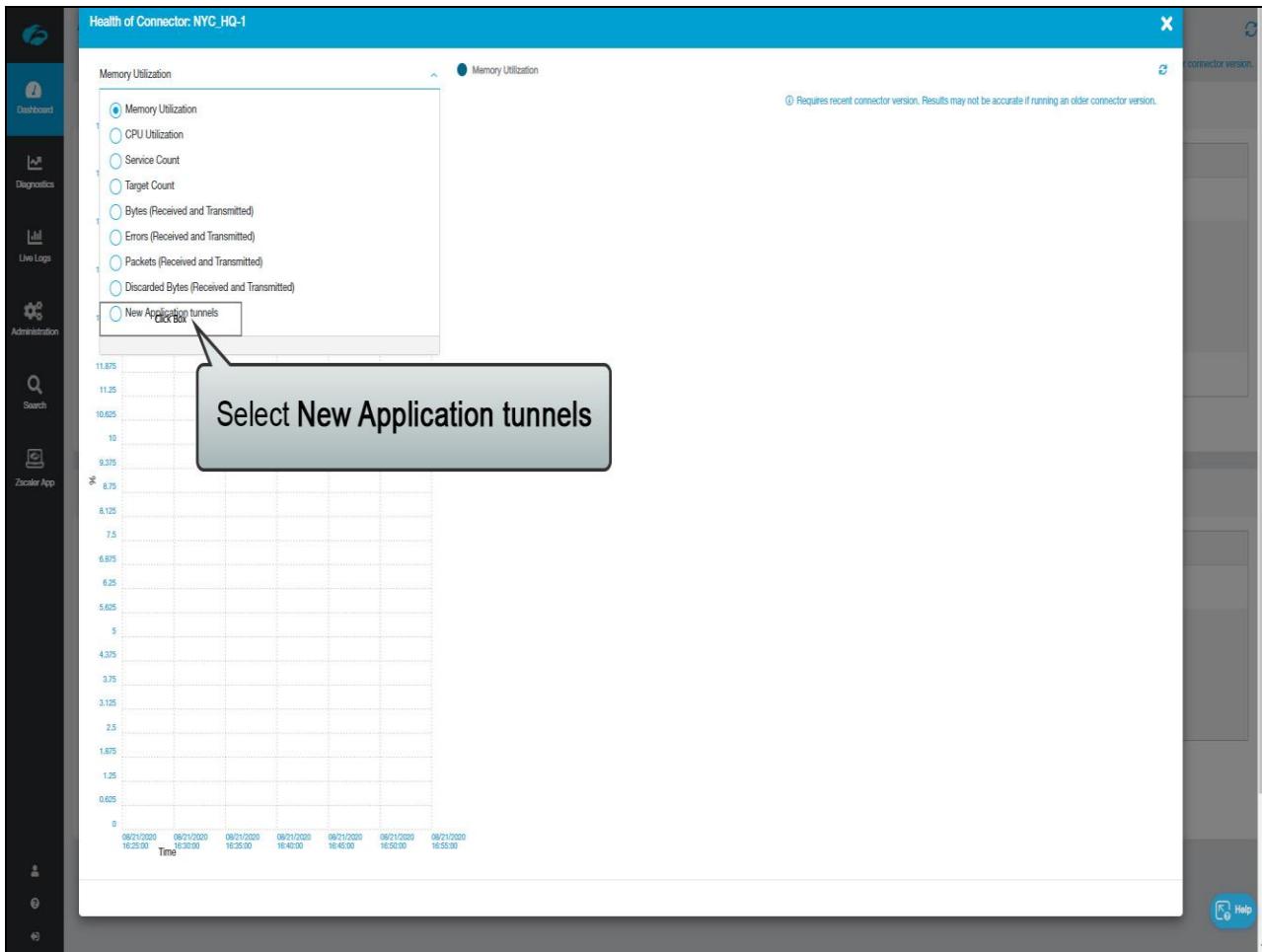
Slide 62 - Slide 62



Slide notes

The drop-down list at the top allows you to select a number of graphs.

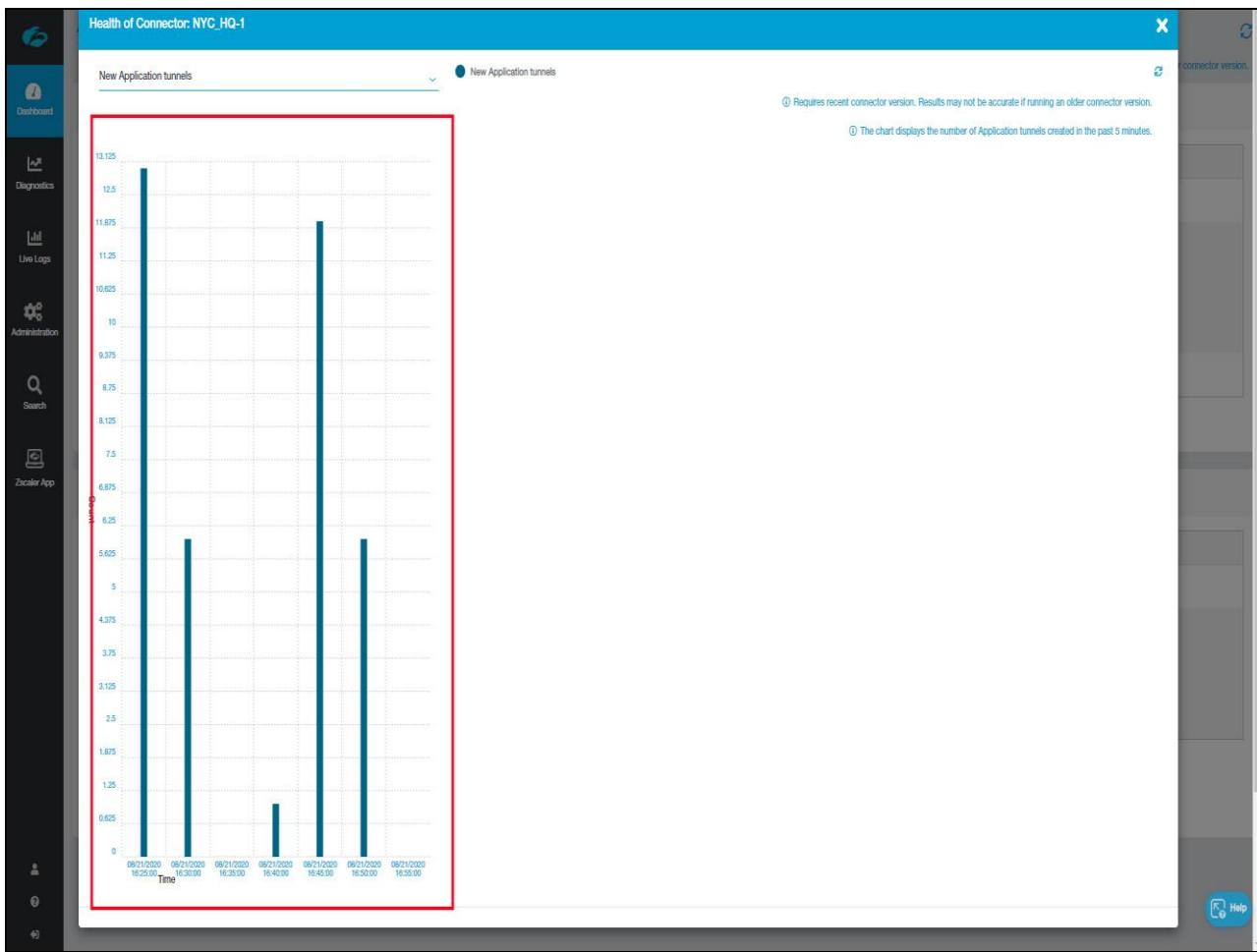
Slide 63 - Slide 63



Slide notes

For example, select **New Application tunnels...**

Slide 64 - Slide 64



Slide notes

...to display the number of Microtunnels for this App Connector over time.

Slide 65 - Slide 65

The screenshot shows the ZCTA-PA Troubleshooting Tools interface with the following sections:

- CPU UTILIZATION:** Shows connector utilization by location. Data table:

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	1 %	Edit Delete
Azure-East-1	Azure-East	New York, US	1 %	Edit Delete
Azure-East-2	Azure-East	New York, US	1 %	Edit Delete
LSS-1	LSS	New York, US	1 %	Edit Delete
LSS-2	LSS	New York, US	1 %	Edit Delete

- MEMORY UTILIZATION:** Shows connector memory utilization by location. Data table:

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	18 %	Edit Delete
Azure-East-1	Azure-East	New York, US	11 %	Edit Delete
Azure-East-2	Azure-East	New York, US	11 %	Edit Delete
LSS-1	LSS	New York, US	11 %	Edit Delete
LSS-2	LSS	New York, US	11 %	Edit Delete

- BYTES (RECEIVED AND TRANSMITTED):** Shows connector byte usage by location. Data table:

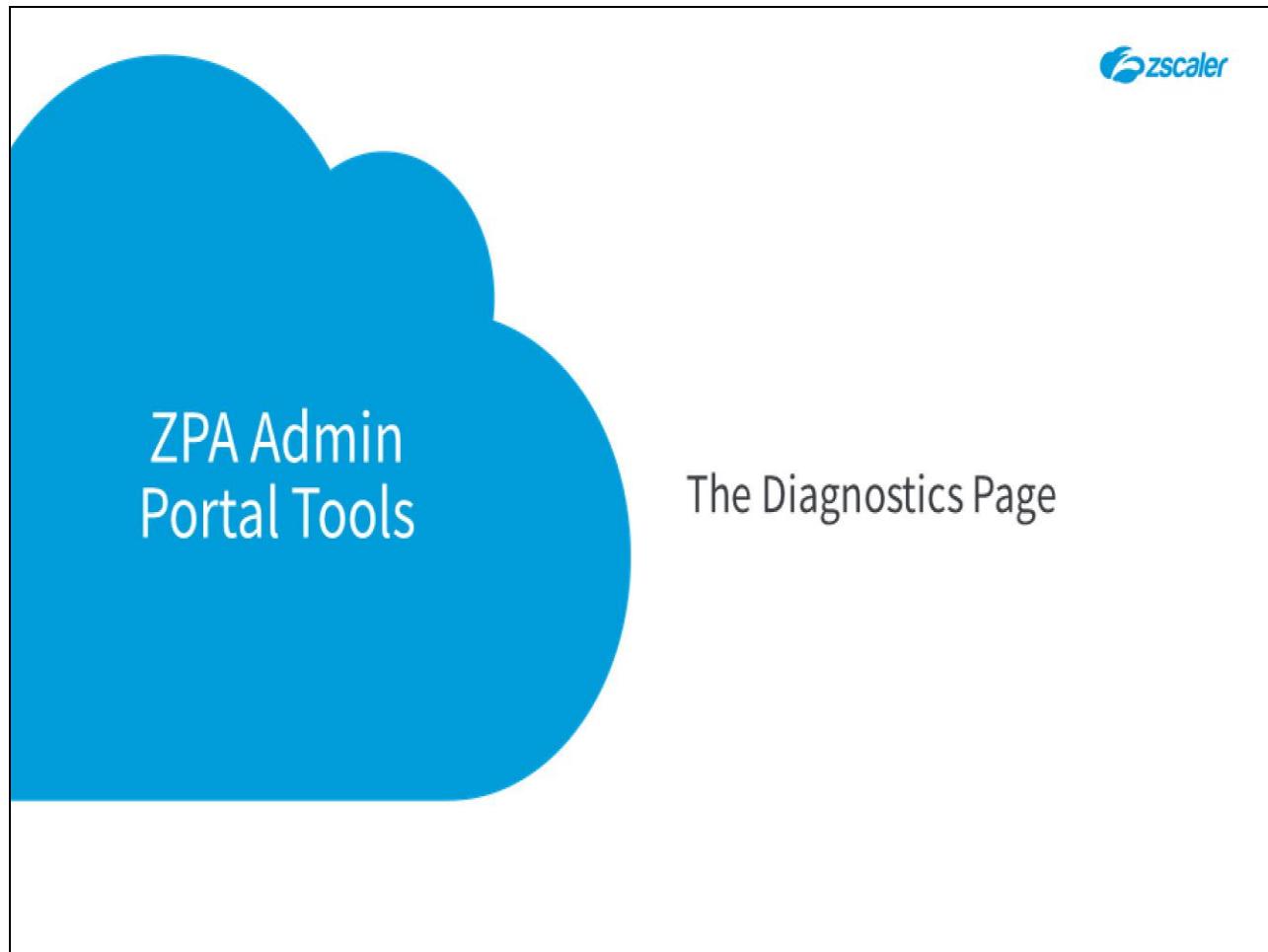
Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	11.74 MB	Edit Delete
Azure-East-2	Azure-East	New York, US	2.99 MB	Edit Delete
LSS-1	LSS	New York, US	2.67 MB	Edit Delete
Azure-East-1	Azure-East	New York, US	2.49 MB	Edit Delete
LSS-2	LSS	New York, US	2.29 MB	Edit Delete

- NEW APPLICATION TUNNELS:** Shows connector tunnel counts by location. Data table:

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	13	Edit Delete
Azure-East-2	Azure-East	New York, US	8	Edit Delete
Azure-East-1	Azure-East	New York, US	7	Edit Delete
LSS-1	LSS	New York, US	1	Edit Delete

Slide notes

Slide 66 - ZPA Admin Portal Tools



Slide notes

Finally, will have a look at the **Diagnostics** capabilities available within the admin portal.

Slide 67 - Slide 67

The screenshot shows the ZPA Diagnostics interface with several sections:

- CPU UTILIZATION:** Shows connector utilization by group and location.
- MEMORY UTILIZATION:** Shows connector utilization by group and location.
- BYTES (RECEIVED AND TRANSMITTED):** Shows byte utilization by connector and group.
- NEW APPLICATION TUNNELS:** Shows the number of tunnels per connector group.

A large callout box highlights the "Diagnostics" link in the left sidebar, with the text "Click Diagnostics" overlaid.

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	1 %	Edit Details
NYC_East-1	NYC_East	New York, US	1 %	Edit Details
NYC_East-2	NYC_East	New York, US	1 %	Edit Details
LSS-1	LSS	New York, US	1 %	Edit Details
LSS-2	LSS	New York, US	1 %	Edit Details

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	18 %	Edit Details
Azure-East-1	Azure-East	New York, US	11 %	Edit Details
Azure-East-2	Azure-East	New York, US	11 %	Edit Details
LSS-1	LSS	New York, US	11 %	Edit Details
LSS-2	LSS	New York, US	11 %	Edit Details

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	11.74 MB	Edit Details
Azure-East-2	Azure-East	New York, US	2.99 MB	Edit Details
LSS-1	LSS	New York, US	2.87 MB	Edit Details
Azure-East-1	Azure-East	New York, US	2.49 MB	Edit Details
LSS-2	LSS	New York, US	2.29 MB	Edit Details

Connector Name	Connector Group Name	Connector Location	Value	Actions
NYC_HQ-1	NYC_HQ	New York, US	13	Edit Details
Azure-East-2	Azure-East	New York, US	8	Edit Details
Azure-East-1	Azure-East	New York, US	7	Edit Details
LSS-1	LSS	New York, US	1	Edit Details

Slide notes

To access the ZPA diagnostics interface, click **Diagnostics**.

Slide 68 - Slide 68

The screenshot shows the Zscaler Diagnostics interface. At the top, there are four main log counters: TOTAL 532, ERRORS 1, ACCESS POLICY BLOCKS 8, and TIMEOUT POLICY BLOCKS 0. Below these, a date range selector shows "Aug 11, 2020 17:00:36 EDT - Aug 21, 2020 17:00:36 EDT". A callout box points to this date range selector with the text "Click to set a custom date range". To the left of the date range, it says "Data on the Dashboard page may be more recent than the data presented below". Below the counters, a section titled "Log counters, and timeframe selector" contains a "No filters have been applied" message and "Apply", "Clear All", and "Add Filters" buttons. The main table lists application logs with columns: Connection (timestamp), UTC, Policy, User, Service Edge, Connector, and Application. The table shows numerous entries for "Allow CorpSSO" and "Allow Access to SAP Portal" policies. A "Hub" button is located at the bottom right of the table.

Connection	UTC	Policy	User	Service Edge	Connector	Application
> Aug 21st, 16:51:57.723 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
> Aug 21st, 16:51:57.083 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
> Aug 21st, 16:51:56.443 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
> Aug 21st, 16:51:55.799 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
> Aug 21st, 16:49:47.201 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :88 TCP
> Aug 21st, 16:49:47.180 EDT		Allow LSS on SSH	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	shares.patraining11.safemar... :445 TCP
> Aug 21st, 16:49:37.656 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
> Aug 21st, 16:49:37.657 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
> Aug 21st, 16:49:37.657 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
> Aug 21st, 16:49:37.656 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
> Aug 21st, 16:49:37.656 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
> Aug 21st, 16:49:37.560 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
> Aug 21st, 16:47:46.053 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
> Aug 21st, 16:46:28.895 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 TCP

Slide notes

The **Diagnostics** page displays counters at the top to indicate the **TOTAL** number of messages, the number of **ERRORS**, **ACCESS** and **TIMEOUT POLICY BLOCKS**, and **SUCCESS** messages.

Informational messages represent the total number of application connections that terminated because the user or App Connector abruptly ended the session for some reason or the application's connection timed out.

There is also a drop-down list to select different types of logs.

To set a custom date range for the log messages, click the date range indication at the top right of the page, ...

Slide 69 - Slide 69

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area displays a summary of log types: TOTAL 532, ERRORS 1, ACCESS POLICY BLOCKS 8, TIMEOUT POLICY BLOCKS 0, SUCCESSFUL 511, and INFO 12. Below this is a table of log entries with columns for Connection, UTC, Policy, User, Service Edge, and Connection. A modal window titled "Select Custom Range" is overlaid on the table, with a tooltip pointing to it. The modal has fields for "From" (set to "Aug 11, 2020 17:00:36 EDT") and "To" (set to "Aug 21, 2020 17:00:36 EDT"), and a "OK" button.

Connection	UTC	Policy	User	Service Edge	Connection
Aug 21st, 16:51:57.723 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:51:57.083 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:51:56.443 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:51:55.799 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:49:47.201 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:49:47.180 EDT		Allow LSS on SSH	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:49:37.656 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2
Aug 21st, 16:49:37.657 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2
Aug 21st, 16:49:37.657 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2
Aug 21st, 16:49:37.656 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2
Aug 21st, 16:49:37.656 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2
Aug 21st, 16:49:37.560 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:47:46.053 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1
Aug 21st, 16:46:28.895 EDT		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1

Slide notes

and select **Custom Range...**

Slide 70 - Slide 70

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zacker App. The main area has a 'Log Type' dropdown set to 'User Activity'. It displays a summary with 'TOTAL 532' and 'ERRORS 1'. Below this, a message says 'No filters have been applied' with buttons for 'Apply', 'Clear All', and 'Add Filters'. A large table lists log entries from Aug 21st, 2020, at 16:51:37.723 EDT. The table columns are 'Connection', 'UTC', 'Policy', and 'Details'. A tooltip 'Select the required start and stop dates' points to a 'Choose Custom Date Range' modal window. This modal has two date pickers: 'Start Date' (Aug 12, 2020) and 'End Date' (Aug 21, 2020). Both pickers show the month of August 2020 with days numbered 1 through 31. A 'Save' button is highlighted with a callout 'Click Save'.

Slide notes

...and set a custom time range within the last 14 days to include up to 14 days of logs and click **Save**.

Slide 71 - Slide 71

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zacker App. The main area has a header with 'Log Type' set to 'User Activity' and a date range from 'Aug 12, 2020 17:00:36 EDT - Aug 21, 2020 17:00:36 EDT'. Below this is a summary section with counts for TOTAL (532), ERRORS (1), ACCESS POLICY BLOCKS (8), TIMEOUT POLICY BLOCKS (0), SUCCESSFUL (511), and INFO (12). A note says 'Data on the Dashboard page might be more recent than the data presented below'. Underneath is a search bar with a dropdown showing 'No filters have been applied', buttons for 'Apply', 'Clear All', and 'Add Filter', and a placeholder 'Click Box'. A callout box with the text 'Click Add Filters' points to the 'Add Filter' button. Below the search bar is a table titled 'Connection' with columns: Connection, User, Service Edge, Connector, and Application. The table lists 15 rows of connection logs, each with a timestamp, action (e.g., 'Allow CorpSSO', 'Allow LSS on SSH'), user (smadmin@patraining11.safemarch.com), service edge (US-VA-9420), connector (NYC_HQ-1 or Azure-East-2), and application (host-1.patraining11.safemar... or shares.patraining11.safemar...). A 'Hub' icon is located in the bottom right corner of the main content area.

Slide notes

To apply filters and drilldown further into the log data, click **Add Filters**....

Slide 72 - Slide 72

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area is titled "User Activity". At the top, there are five summary boxes: TOTAL 532, ERRORS 1, ACCESS POLICY BLOCKS 8, TIMEOUT POLICY BLOCKS 0, SUCCESSFUL 511, and INFO 12. Below these are two tabs: "No filters have been applied" and "Add Filters". A dropdown menu is open, showing options like Application: Domain, Application: Double Encryption, Application: Protocol, Application: Segment Name, Application: Server IP Address, Application: Server Port, Connection: Connection ID, Connection: Setup Time, Connection: Status, and several entries starting with "Allow CorpSSO". A callout box with the text "Click to scroll down..." points to the scroll-down arrow at the bottom of this list.

Connection	User	Service Edge	Connector	Application
Aug 21st, 16:51:57.723	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:57.083	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:56.443	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:55.795	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:49:47.201 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :88 TCP
Aug 21st, 16:49:47.180 EDT	Allow CorpSSO	US-VA-9420	NYC_HQ-1	shares.patraining11.safemar... :445 TCP
Aug 21st, 16:49:37.656 EDT	Allow LSS on SSH	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.656 EDT	Allow Access to SAP Portal	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.657 EDT	Allow Access to SAP Portal	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.657 EDT	Allow Access to SAP Portal	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.656 EDT	Allow Access to SAP Portal	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.560 EDT	Allow Access to SAP Portal	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:47:46.053 EDT	Allow CorpSSO	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:46:28.895 EDT	Allow CorpSSO	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 TCP

Slide notes

...and select from the list of available filter options. In this example, scroll down...

Slide 73 - Slide 73

The screenshot shows a dashboard with various metrics: TOTAL 532, ERRORS 1, ACCESS POLICY BLOCKS 8, TIMEOUT POLICY BLOCKS 0, SUCCESSFUL 511, and INFO 12. Below this, a table lists log entries. A callout bubble points to a dropdown menu labeled "Username" with the text "... and select Username".

Connection	User	Service Edge	Connector	Application
Aug 21st, 16:51:57.723	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:57.083	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:56.442	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:55.795	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:49:47.201 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :88 TCP
Aug 21st, 16:49:47.180 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	shares.patraining11.safemar... :445 TCP
Aug 21st, 16:49:37.656 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.657 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.657 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.656 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.656 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:49:37.560 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safema... :80 TCP
Aug 21st, 16:47:46.053 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:46:28.895 EDT	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 TCP

Slide notes

...and select **Username**.

Slide 74 - Slide 74

The screenshot shows a network monitoring interface with a sidebar containing navigation links: Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area displays a summary of log types: TOTAL 532, ERRORS 1, ACCESS POLICY BLOCKS 8, TIMEOUT POLICY BLOCKS 0, SUCCESSFUL 511, and INFO 12. Below this, a search bar is highlighted with the text "Search for and select a User...". The main content area shows a table of log entries with columns: Date, Action, User, Service Edge, Connector, and Application. The table lists various log entries for users like hvac@patraining11.safemarch.com and smadmin@patraining11.safemarch.com across different service edges and connectors.

Date	Action	User	Service Edge	Connector	Application
Aug 21st, 16:51:56.443 EDT	Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:55.799 EDT	Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:49:47.201 EDT	Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:49:47.180 EDT	Allow LSS on SSH	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 TCP
Aug 21st, 16:49:37.658 EDT	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.657 EDT	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.657 EDT	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.656 EDT	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.656 EDT	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP

Slide notes

Search for and select a User...

Slide 75 - Slide 75

The screenshot shows the ZCTA-PA Troubleshooting Tools dashboard. The left sidebar includes links for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area displays a summary of log types: TOTAL 532, ERRORS 1, ACCESS POLICY BLOCKS 8, TIMEOUT POLICY BLOCKS 0, SUCCESSFUL 511, and INFO 12. Below this is a search interface with a dropdown for Log Type set to 'User Activity'. The search results table has columns for Connection, UTC, Policy, User, Service Edge, Connector, and Application. A search filter for 'hvac' is applied, and a callout box points to the 'Done' button in the search interface.

Connection	UTC	Policy	User	Service Edge	Connector	Application
Aug 21st		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st		Allow CorpSSO	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st		Allow LSS on SSH	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :389 UDP
Aug 21st, 16:51:35.799 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :80 TCP
Aug 21st, 16:49:47.201 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	host-1.patraining11.safemar... :80 TCP
Aug 21st, 16:49:47.180 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	NYC_HQ-1	shares.patraining11.safemar... :445 TCP
Aug 21st, 16:49:37.658 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.657 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.657 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.656 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP
Aug 21st, 16:49:37.560 EDT		Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.safemar... :80 TCP

Slide notes

Click Done...

Slide 76 - Slide 76

The screenshot shows the ZCTA-PA Troubleshooting Tools dashboard with the following details:

- Log Type:** User Activity
- Date Range:** Aug 12, 2020 17:00:36 EDT - Aug 21, 2020 17:00:36 EDT
- Metrics:**
 - TOTAL: 532
 - ERRORS: 1
 - ACCESS POLICY BLOCKS: 8
 - TIMEOUT POLICY BLOCKS: 0
 - SUCCESSFUL: 511
 - INFO: 12
- Filter Bar:**
 - No filters have been applied.
 - USERNAME: Equals hvac0@patraining11.safemarch.com
 - Buttons: Add Filter, Clear All, Add Filters
- Table:** A large table titled "Connections" showing log entries. The columns are:
 - Timestamp
 - Action
 - User
 - Service Edge
 - Connector
 - Application
- Actions:** Buttons for "Expand All" and "Hub".

A callout box points to the "Add Filter" button in the filter bar, with the text "Click Apply" inside it.

Slide notes

...and click **Apply**.

Slide 77 - Slide 77

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header with 'Log Type' set to 'User Activity' and a date range from 'Aug 12, 2020 17:00:36 EDT - Aug 21, 2020 17:00:36 EDT'. Below the header are six summary boxes: TOTAL 3, ERRORS 0, ACCESS POLICY BLOCKS 0, TIMEOUT POLICY BLOCKS 0, SUCCESSFUL 3, and INFO 0. Underneath these are filter options for 'USERNAME' set to 'hvac@patraining11.safemarch.com'. A large red box highlights a table of log entries. The table columns are Connection (UTC), Policy, User, Service Edge, Connector, and Application. The data is as follows:

Connection (UTC)	Policy	User	Service Edge	Connector	Application
Aug 21st, 13:11:44.234 EDT	Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9414	NYC_HQ-1	hvac.patraining11.safemarch...:80 TCP
10th, 13:11:44.234 EDT	Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch...:80 TCP
	BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch...:80 TCP

A callout box with the text 'Click to reveal details' points to the first row of the table.

Slide notes

The display is updated to only include user activity log data for this one user. For each of the log entries, you have the option to reveal full details by clicking on the chevron.

Slide 78 - Slide 78

The screenshot shows the ZCP User Activity dashboard. At the top, there are summary counts for TOTAL (3), ERRORS (0), ACCESS POLICY BLOCKS (0), TIMEOUT POLICY BLOCKS (0), SUCCESSFUL (3), and INFO (0). Below this, a search bar filters logs for the user hvac@patraining11.safemarch.com. The main table displays detailed connection information for a specific session:

Connection	UTC	Policy	User	Service Edge	Connector	Application
START TIME Aug 21st, 16:39:51.874 EDT		ACCESS POLICY NAME Allow BrowserAccess to HVAC	USERNAME hvac@patraining11.safemarch.com	NAME US-OH-9414	NAME NYC_HQ-1	APPLICATION PORT & PROTOCOL hvac.patraining11.safemarch....:80 TCP
END TIME Aug 21st, 16:43:06.672 EDT		ACTION ALLOW	IP 184.10.224.172	LOCATION Cleveland, US	IP-PORT & PROTOCOL 10.0.0.4:39826 TCP	APPLICATION SEGMENT HVAC
STATUS CODE SE: Connection closed by Service...		POLICY ID 14412346984654396	LOCATION Sterling, US	POLICY PROCESSING 446.57 ms	LOCATION New York, US	SERVICE IP PORT & PROTOCOL 10.0.0.12:80 TCP
INTERNAL STATUS CODE BRK_MT_TERMINATED		TIMEOUT POLICY NAME Default_Rule	CLIENT TYPE Web Browser	RX FROM CLIENT 6.88 KB	CONNECTOR ID 14412346984654397	APPLICATION ID 14412346984654395
STATUS Closed Connection		ACTION ALLOW	USER METADATA	TX TO CONNECTOR 6.88 KB	CONNECTION SETUP TIME 896.65 ms	SERVICE ID Unavailable
DURATION 3m 14s 998ms		TIMEOUT POLICY ID 14412346984654394		RX FROM CONNECTOR 48.694 KB	CONNECTOR GROUP NAME NYC_HQ	DOUBLE ENCRYPTION Disabled
TOTAL BYTES 55.574 KB				TX TO CLIENT 48.694 KB	CONNECTOR GROUP ID 14412346984654398	
CONNECTION ID vUMBxLx0vMhppk2MGA.bcyX5...						
CONNECTION STATUS LOG Click to download the log file						

A callout box points to the "Click to download the log file" link at the bottom of the table.

Slide notes

This provides detailed information about the connection, incl. which policy was applied, which ZPA Public Service Edge and which Connector were involved, what application was accessed and more.

You can also download the complete details of the connection status log...

Slide 79 - Slide 79

The screenshot shows the ZCTA-PA Troubleshooting Tools dashboard. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header "Log Type User Activity". Below it, there are three summary boxes: "TOTAL 3", "ERRORS 0", and "ACCESS POLICY BLOCKS 0". A search bar filters results for "Username Equals hvac@patraining11.safemarch.com". The main table lists connection details:

Connection	UTC	Policy	User
START TIME Aug 21st, 16:39:51.874 EDT		ACCESS POLICY NAME Allow BrowserAccess to HVAC	USERNAME hvac@patraining11.safemarch.com
END TIME Aug 21st, 16:43:06.872 EDT		ACTION Allow	IP 184.170.224.172
STATUS CODE SE: Connection closed by Service...		POLICY ID 14412346984654396	LOCATION Sterling,US
INTERNAL STATUS CODE BRK_MT_TERMINATED		TIMEOUT POLICY NAME Default_Rule	CLIENT TYPE Web Browser
STATUS Closed Connection		ACTION Allow	USER METADATA
DURATION 3m 14s 998ms		TIMEOUT POLICY ID 14412346984654396	
TOTAL BYTES 55,574 KB			
CONNECTION ID vUMlxLx0vuMhppKzMGA,bcyX...			
CONNECTION STATUS LOG			
Aug 20th, 13:11:44.234 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com
Aug 20th, 13:11:42.609 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com

To the right, a Notepad window displays a JSON log entry with a red border:

```

{
  "status": "BRK_MT_TERMINATED",
  "connectionId": "vUMlxLx0vuMhppKzMGA,bcyX5bFskowwlkry",
  "connEndTime": "1598042586872623",
  "duration": "194998386",
  "connectionStatus": "close",
  "doubleEncrypt": "0",
  "reAuthPolicyName_id": "144123469846544394",
  "reAuthPolicyName": "Default_Rule",
  "policyAction": "ALLOW",
  "policyType": "AccessPolicy",
  "connToServerLat": "896653",
  "origConnStartTime": "1598842391874237",
  "domain": "hvac.patraining11.safemarch.com",
  "sentBytes": "49863",
  "protocol": "TCP",
  "protocol_id": "6",
  "clientPublicIp": "184.170.224.172",
  "userLocation": "Sterling,US",
  "serverIp": "10.0.0.12",
  "brokerToBisplat": "446571",
  "idpName": "Azure",
  "idpName_id": "144123469846545366",
  "clientLat": "39",
  "connStartTime": "1598042391874237",
  "astReceivedBytes": "49863",
  "serverPort": "80",
  "policyName": "Allow BrowserAccess to HVAC",
  "policyName_id": "144123469846545396",
  "connectorPort": "39826",
  "connectorGroupName_id": "144123469846545378",
  "connectorName_id": "144123469846545376"
}

```

Slide notes

... and attach that file to a support ticket, if needed.

Slide 80 - Slide 80

The screenshot shows the Zscaler Diagnostics interface. On the left, there's a sidebar with icons for Dashboard, Diagnostics (which is selected), Live Logs, Administration, and Search. The main area has a header "Log Type User Activity" with dropdown menus for "TOTAL" (set to 3), "ERRORS" (0), and "ACCESS POLICY BLOCKS" (0). Below this, there are filters for "USERNAME" set to "hvac@patraining11.safemarch.com". A red box highlights the "Status Code" field, which shows "SE: Connection closed by Service". The main table lists session details like start time, policy name, user, and duration. A red box highlights the "INTERNAL STATUS CODE" column. The bottom part of the interface shows a list of log entries with columns for Connection, UTC, Policy, User, and Duration.

A modal window titled "About ZPA Session Status Codes" is open in the center. It displays a table of session status codes with columns for Session Status, Internal Reason, Description, and Resolution. The table includes rows for "Connector: Connection closed successfully" (Reason: AST_MT_TERMINATED, Description: "The connection to the App Connector was terminated without issue.", Resolution: "No action required."), "Request was successful" (Reason: OPEN_OR_ACTIVE_CONNECTION, Description: "The connection is active and working.", Resolution: "No action required."), and "SE: Connection closed successfully" (Reason: MT_CLOSED_TERMINATED, Description: "The connection to the ZPA Public Service Edge (formerly Zscaler Enforcement Node or ZEN) was terminated.", Resolution: "No action required."). The modal also contains a note about finding a list of ZPA session status codes in the Diagnostics pages.

Slide notes

Some items in the log entry are shown in blue and represent hyperlinks. For example, clicking the **Status Code** will bring up a complete list of status codes. Also, clicking the filter icon applies this item as a new filter to the Diagnostics display.

Slide 81 - Slide 81

Connection	UTC	Policy	User	Service Edge	Connector	Application
START TIME Click to conceal details	21st, 16:39:51.874 EDT	ACCESS POLICY NAME Allow BrowserAccess to HVAC	USERNAME hvac@patraining11.safemarch.com	NAME US-OH-9414	NAME NYC_HQ-1	APPLICATION PORT & PROTOCOL hvac.patraining11.safemarch... :80 TCP
END TIME Aug 21, 16:39:51.874 EDT		ACTION ID 469846945396	IP 184.170.224.172	LOCATION Cleveland, US	IP/PORT & PROTOCOL 10.0.4.39826 TCP	APPLICATION SEGMENT HVAC
STATISTICS		T POLICY NAME Rule	LOCATION Sterling, US	POLICY PROCESSING 446.57 ms	LOCATION New York, US	SERVICE IP/PORT & PROTOCOL 10.0.0.12:80 TCP
INTERVAL BRK			CLIENT TYPE Web Browser	RX FROM CLIENT 6.88 KB	CONNECTOR ID 144123469846945379	APPLICATION ID 144123469846945395
STATUS Closed Connection		ACTION Allow		TX TO CONNECTOR 6.88 KB	CONNECTION SETUP TIME 896.65 ms	SERVICE ID Unavailable
DURATION 3m 14s 998ms		TIMEOUT POLICY ID 14412346984694394		RX FROM CONNECTOR 48.694 KB	CONNECTOR GROUP NAME NYC_HQ	DOUBLE ENCRYPTION Disabled
TOTAL BYTES 55.574 KB				TX TO CLIENT 48.694 KB	CONNECTOR GROUP ID 144123469846945378	
CONNECTION ID vUMBxLx0vMhIppKzMGAbcyX...						
CONNECTION STATUS LOG						
Aug 20th, 13:11:44.234 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP
Aug 20th, 13:11:42.609 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP

Slide notes

Click once again to conceal the details.

Slide 82 - Slide 82

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header with 'Log Type' and 'User Activity' dropdowns, a date range from 'Aug 12, 2020 17:00:36 EDT - Aug 21, 2020 17:00:36 EDT', and a note about data being more recent than the dashboard page. Below this are four summary boxes: 'TOTAL 3' (highlighted with a callout 'Click Log Type drop-down list'), 'ACCESS POLICY BLOCKS 0', 'TIMEOUT POLICY BLOCKS 0', and 'INFO 0'. A 'SUCCESSFUL' box shows '3'. Underneath are filter options for 'USERNAME Equals hvac@patraining11.safemarch.com' and buttons for 'Apply', 'Clear All', and 'Add Filters'. At the bottom is a table of 'Live Logs' with columns: Connection, UTC, Policy, User, Service Edge, Connector, and Application. Three rows are listed:

Connection	UTC	Policy	User	Service Edge	Connector	Application
Aug 21st, 16:39:51.874 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9414	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP
Aug 20th, 13:11:44.234 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP
Aug 20th, 13:11:42.609 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP

Slide notes

Let's have a quick look at other log types. Click the drop-down list...

Slide 83 - Slide 83

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a title bar "Log Type User Activity" and a date range "Aug 12, 2020 17:00:36 EDT - Aug 21, 2020 17:00:36 EDT". It features four summary boxes: ACCESS POLICY BLOCKS (0), TIMEOUT POLICY BLOCKS (0), SUCCESSFUL (3), and INFO (0). A callout box highlights the "User Status" dropdown menu under "Log Type". Below this, there's a search bar with the filter "[Username Equals hvac@patraining11.safemarch.com]" and an "Apply" button. The main content area displays a table of log entries:

Connection	UTC	Policy	User	Service Edge	Connector	Application
Aug 21st, 16:39:51.874 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9414	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP
Aug 20th, 13:11:44.234 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP
Aug 20th, 13:11:42.609 EDT		Allow BrowserAccess to HVAC	hvac@patraining11.safemarch.com	US-OH-9408	NYC_HQ-1	hvac.patraining11.safemarch... :80 TCP

Slide notes

...and select **User Status**.

Slide 84 - Slide 84

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zacker App. The main area has a header with 'Log Type' and 'User Status' dropdowns, a date range from 'Aug 20, 2020 17:03:34 EDT - Aug 21, 2020 17:03:34 EDT', and a note about data being more recent than the dashboard page. It displays 'TOTAL 12' sessions, '0' errors, and '12' successful sessions. A table below lists session details: Session (Auth Log Timestamp, UTC Authentication Time, Disconnect Time), Client (Email address), and Service Edge (Location). One row in the table is highlighted with a red border.

Session	Auth Log Timestamp	UTC Authentication Time	Disconnect Time	Client	Service Edge
Authenticated	Aug 21st, 17:01:12.621 EDT	Aug 21st, 16:45:02.000 EDT		smadmin@patraining11.safemarch.com	US-VA-9420
Disconnected	Aug 21st, 16:48:12.484 EDT	Aug 21st, 16:39:51.000 EDT	Aug 21st, 16:48:12.484 EDT	hvac@patraining11.safemarch.com	US-OH-9414
Authenticated	Aug 21st, 16:45:02.542 EDT	Aug 21st, 16:45:02.000 EDT		smadmin@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 16:42:51.922 EDT	Aug 21st, 15:47:21.000 EDT	Aug 21st, 16:42:51.922 EDT	studentl@patraining11.safemarch.com	US-VA-9422
Disconnected	Aug 21st, 15:47:21.734 EDT	Aug 21st, 15:47:21.000 EDT	Aug 21st, 15:47:21.734 EDT	studentl@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 15:46:33.423 EDT	Aug 21st, 12:35:36.000 EDT	Aug 21st, 15:46:33.423 EDT	smadmin@patraining11.safemarch.com	US-VA-9421
Disconnected	Aug 21st, 10:20:53.884 EDT	Aug 21st, 10:20:53.000 EDT	Aug 21st, 10:20:53.884 EDT	smadmin@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 10:19:30.877 EDT	Aug 21st, 09:56:25.000 EDT	Aug 21st, 10:19:30.877 EDT	studentl@patraining11.safemarch.com	US-VA-9422
Authenticated	Aug 21st, 09:56:25.644 EDT	Aug 21st, 09:56:25.000 EDT		studentl@patraining11.safemarch.com	US-OR-8311
Disconnected	Aug 20th, 18:28:08.369 EDT	Aug 20th, 16:42:17.000 EDT	Aug 20th, 18:28:08.369 EDT	studentl@patraining11.safemarch.com	US-VA-9420
Authenticated	Aug 20th, 18:27:51.347 EDT	Aug 20th, 18:23:41.000 EDT		smadmin@patraining11.safemarch.com	AM-CA-8734
Disconnected	Aug 20th, 18:23:39.503 EDT	Aug 20th, 18:23:39.000 EDT	Aug 20th, 18:23:39.503 EDT	smadmin@patraining11.safemarch.com	US-OR-8310

Slide notes

This shows details about active and disconnected sessions for users. As previously shown, you can apply filters, limit the reporting time period and expand each log entry to view more details.

Slide 85 - Slide 85

The screenshot shows the ZCTA-PA Troubleshooting Tools Dashboard. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header with 'Log Type' and 'User Status Click Box' dropdowns, a date range from 'Aug 20, 2020 17:03:34 EDT - Aug 21, 2020 17:03:34 EDT', and a note about data being more recent than the page. It displays three summary boxes: 'TOTAL 12' (blue), 'ERRORS 0' (red), and 'SUCCESSFUL 12' (green). Below these are buttons for 'Apply', 'Clear All', and 'Add Filters'. A large callout box points to the 'Log Type' dropdown with the text 'Click Log Type drop-down list'. The main content area is a table of session logs with columns: Session, Auth Log Timestamp (UTC), Authentication Time, Disconnect Time, Client, and Service Edge. Each row shows a session status (Authenticating, Disconnected, etc.), timestamp, and client information. The table includes an 'Expand All' button at the top right. A 'Help' icon is located in the bottom right corner.

Session	Auth Log Timestamp (UTC)	Authentication Time	Disconnect Time	Client	Service Edge
Authenticated	Aug 21st, 17:01:12.621 EDT	Aug 21st, 16:45:02.000 EDT		smadmin@patraining11.safemarch.com	US-VA-9420
Disconnected	Aug 21st, 16:48:12.484 EDT	Aug 21st, 16:39:51.000 EDT	Aug 21st, 16:48:12.484 EDT	hvac@patraining11.safemarch.com	US-OH-9414
Authenticated	Aug 21st, 16:45:02.542 EDT	Aug 21st, 16:45:02.000 EDT		smadmin@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 16:42:51.922 EDT	Aug 21st, 15:47:21.000 EDT	Aug 21st, 16:42:51.922 EDT	student@patraining11.safemarch.com	US-VA-9422
Disconnected	Aug 21st, 15:47:21.734 EDT	Aug 21st, 15:47:21.000 EDT	Aug 21st, 15:47:21.734 EDT	student@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 15:46:33.423 EDT	Aug 21st, 12:35:36.000 EDT	Aug 21st, 15:46:33.423 EDT	smadmin@patraining11.safemarch.com	US-VA-9421
Disconnected	Aug 21st, 10:20:53.884 EDT	Aug 21st, 10:20:53.000 EDT	Aug 21st, 10:20:53.884 EDT	smadmin@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 10:19:30.877 EDT	Aug 21st, 09:56:25.000 EDT	Aug 21st, 10:19:30.877 EDT	student@patraining11.safemarch.com	US-VA-9422
Authenticated	Aug 21st, 09:56:25.644 EDT	Aug 21st, 09:56:25.000 EDT		student@patraining11.safemarch.com	US-OR-8311
Disconnected	Aug 20th, 18:28:08.369 EDT	Aug 20th, 16:42:17.000 EDT	Aug 20th, 18:28:08.369 EDT	student@patraining11.safemarch.com	US-VA-9420
Authenticated	Aug 20th, 18:27:51.347 EDT	Aug 20th, 18:23:41.000 EDT		smadmin@patraining11.safemarch.com	AM-CA-8734
Disconnected	Aug 20th, 18:23:39.503 EDT	Aug 20th, 18:23:39.000 EDT	Aug 20th, 18:23:39.503 EDT	smadmin@patraining11.safemarch.com	US-OR-8310

Slide notes

Click the **Log Type** dropdown list again...

Slide 86 - Slide 86

The screenshot shows the ZCTA-PA Troubleshooting Tools dashboard. On the left, there's a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header with 'Log Type' (set to 'User Status'), a date range ('Aug 20, 2020 17:03:34 EDT - Aug 21, 2020 17:03:34 EDT'), and a note about data being more recent than the page. It displays 'TOTAL 12' and 'ERRORS 0'. A large button on the right says 'SUCCESSFUL 12'. Below this is a table of session logs with columns: Session, Auth Log Timestamp (UTC), Authentication Time, Disconnect Time, Client, and Service Edge. The table lists 12 rows of session data. At the bottom right is a 'Help' icon.

Session	Auth Log Timestamp (UTC)	Authentication Time	Disconnect Time	Client	Service Edge
Authenticated	Aug 21st, 17:01:12.621 EDT	Aug 21st, 16:45:02.000 EDT		smadmin@patraining11.safemarch.com	US-VA-9420
Disconnected	Aug 21st, 16:48:12.484 EDT	Aug 21st, 16:39:51.000 EDT	Aug 21st, 16:48:12.484 EDT	hvac@patraining11.safemarch.com	US-OH-9414
Authenticated	Aug 21st, 16:45:02.542 EDT	Aug 21st, 16:45:02.000 EDT		smadmin@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 16:42:51.922 EDT	Aug 21st, 15:47:21.000 EDT	Aug 21st, 16:42:51.922 EDT	student@patraining11.safemarch.com	US-VA-9422
Disconnected	Aug 21st, 15:47:21.734 EDT	Aug 21st, 15:47:21.000 EDT	Aug 21st, 15:47:21.734 EDT	student@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 15:46:33.423 EDT	Aug 21st, 12:35:36.000 EDT	Aug 21st, 15:46:33.423 EDT	smadmin@patraining11.safemarch.com	US-VA-9421
Disconnected	Aug 21st, 10:20:53.884 EDT	Aug 21st, 10:20:53.000 EDT	Aug 21st, 10:20:53.884 EDT	smadmin@patraining11.safemarch.com	US-OR-8310
Disconnected	Aug 21st, 10:19:30.877 EDT	Aug 21st, 09:56:25.000 EDT	Aug 21st, 10:19:30.877 EDT	student@patraining11.safemarch.com	US-VA-9422
Authenticated	Aug 21st, 09:56:25.644 EDT	Aug 21st, 09:56:25.000 EDT		student@patraining11.safemarch.com	US-OR-8311
Disconnected	Aug 20th, 18:28:08.369 EDT	Aug 20th, 18:42:17.000 EDT	Aug 20th, 18:28:08.369 EDT	student@patraining11.safemarch.com	US-VA-9420
Authenticated	Aug 20th, 18:27:51.347 EDT	Aug 20th, 18:23:41.000 EDT		smadmin@patraining11.safemarch.com	AM-CA-8734
Disconnected	Aug 20th, 18:23:39.503 EDT	Aug 20th, 18:23:39.000 EDT	Aug 20th, 18:23:39.503 EDT	smadmin@patraining11.safemarch.com	US-OR-8310

Slide notes

...and select **Connector Status**.

Slide 87 - Slide 87

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area displays session logs with columns for Session, Application Time, Disconnect Time, Name, and Service Edge. A callout box points to the 'Add Filters' button in the toolbar.

Session	Application Time	Disconnect Time	Name	Service Edge
> Authenticated ↔	Aug 21st, 17:03:26.667 EDT	Aug 20th, 15:47:29.616 EDT	Azure-East-1	US-VA-9422
> Authenticated ↔	Aug 21st, 17:03:26.667 EDT	Aug 20th, 14:59:26.667 EDT	Azure-East-2	US-VA-9419
> Authenticated ↔	Aug 21st, 17:03:06.508 EDT	Aug 20th, 15:03:06.507 EDT	LSS-1	US-VA-9419
> Authenticated ↔	Aug 21st, 17:02:47.868 EDT	Aug 20th, 15:54:47.869 EDT	LSS-2	US-CA-8172
> Authenticated ↔	Aug 21st, 17:02:47.272 EDT	Aug 21st, 13:26:47.271 EDT	LSS-2	US-VA-9421
> Authenticated ↔	Aug 21st, 17:02:30.667 EDT	Aug 20th, 16:42:30.668 EDT	Azure-East-2	US-VA-9420
> Authenticated ↔	Aug 21st, 17:02:26.482 EDT	Aug 20th, 16:42:26.482 EDT	LSS-2	US-CA-8171
> Authenticated ↔	Aug 21st, 17:02:19.337 EDT	Aug 20th, 14:34:19.337 EDT	LSS-1	US-CA-9390
> Authenticated →	Aug 21st, 17:02:18.186 EDT	Aug 20th, 14:14:18.368 EDT	LSS-1	US-NY-9567
> Authenticated ↔	Aug 21st, 17:02:07.942 EDT	Aug 20th, 14:34:07.941 EDT	LSS-1	US-CA-8173
> Authenticated ↔	Aug 21st, 17:02:07.396 EDT	Aug 20th, 14:34:07.396 EDT	LSS-1	US-CA-8172
> Authenticated →	Aug 21st, 17:02:05.714 EDT	Aug 20th, 14:10:05.881 EDT	Azure-East-2	US-NY-9565
> Authenticated ↔	Aug 21st, 17:02:05.083 EDT	Aug 20th, 15:38:05.083 EDT	Azure-East-1	US-VA-9419
> Authenticated ↔	Aug 21st, 17:02:00.244 EDT	Aug 20th, 14:34:00.244 EDT	LSS-2	US-CA-9390

Slide notes

Click Add Filters...

Slide 88 - Slide 88

The screenshot shows the Zscaler Admin UI interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header with 'Log Type' and 'Connector Status' dropdowns, and a date range from 'Aug 21, 2020 16:33:57 EDT - Aug 21, 2020 17:03:57 EDT'. Below this is a summary bar with 'TOTAL 193', 'ERRORS 0', and 'SUCCESSFUL 194'. A message says 'Data on the Dashboard page might be more recent than the data presented below'. The main content is a table of session logs with columns: Session, Connector Name, UTC, Authentication Time, Disconnect Time, Name, and Service Edge. A tooltip 'Select Connector: Private IP Address' is overlaid on the 'Connector: Private IP Address' filter dropdown in the top navigation bar.

Session	Connector Name	UTC	Authentication Time	Disconnect Time	Name	Service Edge
> Authenticated ↔	Connector: Click Box Address	EDT	Aug 21st, 15:47:29.616 EDT		Azure-East-1	US-VA-9422
> Authenticated ↔	Connector: Public IP Address					US-VA-9419
> Authenticated ↔	Service Edge: Name (Public/Private)				LSS-2	US-CA-8172
> Authenticated ↔		Aug 21st, 17:03:01 EDT				US-VA-9419
> Authenticated ↔		Aug 21st, 17:02:41 EDT				US-CA-8172
> Authenticated ↔		Aug 21st, 17:02:47.272 EDT	Aug 21st, 13:26:47.271 EDT		LSS-2	US-VA-9421
> Authenticated ↔		Aug 21st, 17:02:30.667 EDT	Aug 20th, 16:42:30.668 EDT		Azure-East-2	US-VA-9420
> Authenticated ↔		Aug 21st, 17:02:26.482 EDT	Aug 20th, 16:42:26.482 EDT		LSS-2	US-CA-8171
> Authenticated ↔		Aug 21st, 17:02:19.337 EDT	Aug 20th, 14:34:19.337 EDT		LSS-1	US-CA-9390
> Authenticated →		Aug 21st, 17:02:18.186 EDT	Aug 20th, 14:14:18.368 EDT		LSS-1	US-NY-9567
> Authenticated ↔		Aug 21st, 17:02:07.942 EDT	Aug 20th, 14:34:07.941 EDT		LSS-1	US-CA-8173
> Authenticated ↔		Aug 21st, 17:02:07.396 EDT	Aug 20th, 14:34:07.396 EDT		LSS-1	US-CA-8172
> Authenticated →		Aug 21st, 17:02:05.714 EDT	Aug 20th, 14:10:05.881 EDT		Azure-East-2	US-NY-9565
> Authenticated ↔		Aug 21st, 17:02:05.083 EDT	Aug 20th, 15:38:05.083 EDT		Azure-East-1	US-VA-9419
> Authenticated ↔		Aug 21st, 17:02:00.244 EDT	Aug 20th, 14:34:00.244 EDT		LSS-2	US-CA-9390

Slide notes

...and home in on a specific App Connector by using its private IP address.

Slide 89 - Slide 89

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header with 'Log Type' and 'Connector Status' dropdowns, a date range from 'Aug 21, 2020 16:33:57 EDT - Aug 21, 2020 17:03:57 EDT', and a note about data being more recent than the dashboard page. It displays three summary boxes: 'TOTAL 193', 'ERRORS 0', and 'SUCCESSFUL 194'. Below this is a filter bar with 'No filters have been applied', a connector filter for 'CONNECTOR: PRIVATE IP ADDRESS Equals', and buttons for 'Apply', 'Clear All', and 'Add Filters'. A large callout box with the text 'Click Apply' points to the 'Apply' button. The main table lists session details with columns: Session ID, Timestamp, UTC, Authentication Time, Disconnect Time, Name, and Service Edge. The table contains 19 rows of session data.

Session ID	Timestamp	UTC	Authentication Time	Disconnect Time	Name	Service Edge
> A	Aug 21st, 13:29:616 EDT		Aug 21st, 15:47:29.616 EDT		Azure-East-1	US-VA-9422
> Authenticated ↔	Aug 21st, 17:03:26.667 EDT		Aug 20th, 14:59:26.667 EDT		Azure-East-2	US-VA-9419
> Authenticated ↔	Aug 21st, 17:03:06.508 EDT		Aug 20th, 15:03:06.507 EDT		LSS-1	US-VA-9419
> Authenticated ↔	Aug 21st, 17:02:47.868 EDT		Aug 20th, 15:54:47.869 EDT		LSS-2	US-CA-8172
> Authenticated ↔	Aug 21st, 17:02:47.272 EDT		Aug 21st, 13:26:47.271 EDT		LSS-2	US-VA-9421
> Authenticated ↔	Aug 21st, 17:02:30.667 EDT		Aug 20th, 16:42:30.668 EDT		Azure-East-2	US-VA-9420
> Authenticated ↔	Aug 21st, 17:02:26.482 EDT		Aug 20th, 16:42:26.482 EDT		LSS-2	US-CA-8171
> Authenticated ↔	Aug 21st, 17:02:19.337 EDT		Aug 20th, 14:34:19.337 EDT		LSS-1	US-CA-9390
> Authenticated →	Aug 21st, 17:02:18.186 EDT		Aug 20th, 14:14:18.368 EDT		LSS-1	US-NY-9567
> Authenticated ↔	Aug 21st, 17:02:07.942 EDT		Aug 20th, 14:34:07.941 EDT		LSS-1	US-CA-8173
> Authenticated ↔	Aug 21st, 17:02:07.356 EDT		Aug 20th, 14:34:07.356 EDT		LSS-1	US-CA-8172
> Authenticated →	Aug 21st, 17:02:05.714 EDT		Aug 20th, 14:10:05.881 EDT		Azure-East-2	US-NY-9565

Slide notes

Enter the IP address, then click **Apply**.

Slide 90 - Slide 90

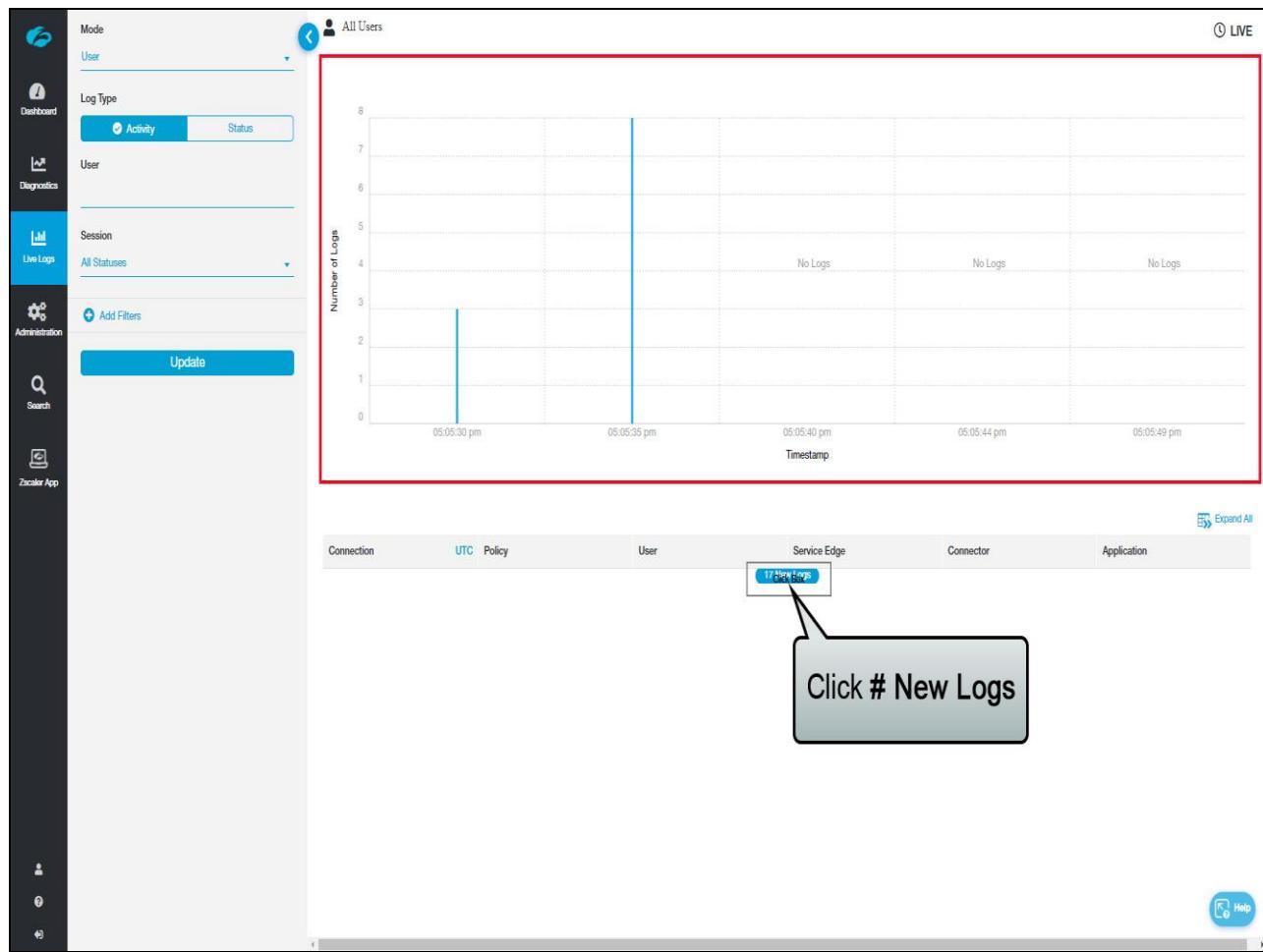
The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left, there's a vertical navigation bar with icons for Dashboard, Diagnostics, Live Logs (which is selected), and Administration. Below the navigation bar, a search bar contains the text "Click Live Logs". The main area displays a dashboard with three large boxes: "TOTAL 42", "ERRORS 0", and "SUCCESSFUL 42". Below the dashboard, there's a search filter for "Connector: Private IP Address Equals 10.0.0.13" and a dropdown menu set to "Equals". A table titled "Session" lists 12 rows of log entries. The columns include Session, Auth Log Timestamp, UTC, Authentication Time, Disconnect Time, Name, and Service Edge. Each row shows an "Authenticated" event with various timestamp variations and names like LSS-1, US-CA-8171, etc. At the bottom right of the table, there's a "Hub" icon.

Session	Auth Log Timestamp	UTC	Authentication Time	Disconnect Time	Name	Service Edge
> Authenticated ↔	Aug 21st, 17:03:54.317 EDT		Aug 21st, 16:39:54.317 EDT		LSS-1	US-CA-8171
> Authenticated ↔	Aug 21st, 17:03:06.508 EDT		Aug 20th, 15:03:06.507 EDT		LSS-1	US-VA-9419
> Authenticated ↔	Aug 21st, 17:02:19.337 EDT		Aug 20th, 14:34:19.337 EDT		LSS-1	US-CA-9390
> Authenticated →	Aug 21st, 17:02:18.186 EDT		Aug 20th, 14:14:18.368 EDT		LSS-1	US-NY-9567
> Authenticated ↔	Aug 21st, 17:02:07.942 EDT		Aug 20th, 14:34:07.941 EDT		LSS-1	US-CA-8173
> Authenticated ↔	Aug 21st, 17:02:07.356 EDT		Aug 20th, 14:34:07.356 EDT		LSS-1	US-CA-8172
> Authenticated ↔	Aug 21st, 16:59:54.317 EDT		Aug 21st, 16:39:54.317 EDT		LSS-1	US-CA-8171
> Authenticated ↔	Aug 21st, 16:59:06.508 EDT		Aug 20th, 15:03:06.507 EDT		LSS-1	US-VA-9419
> Authenticated ↔	Aug 21st, 16:58:19.337 EDT		Aug 20th, 14:34:19.337 EDT		LSS-1	US-CA-9390
> Authenticated →	Aug 21st, 16:58:18.186 EDT		Aug 20th, 14:14:18.368 EDT		LSS-1	US-NY-9567
> Authenticated ↔	Aug 21st, 16:58:07.941 EDT		Aug 20th, 14:34:07.941 EDT		LSS-1	US-CA-8173
> Authenticated ↔	Aug 21st, 16:58:07.355 EDT		Aug 20th, 14:34:07.356 EDT		LSS-1	US-CA-8172

Slide notes

To view events as they occur, click **Live Logs**.

Slide 91 - Slide 91



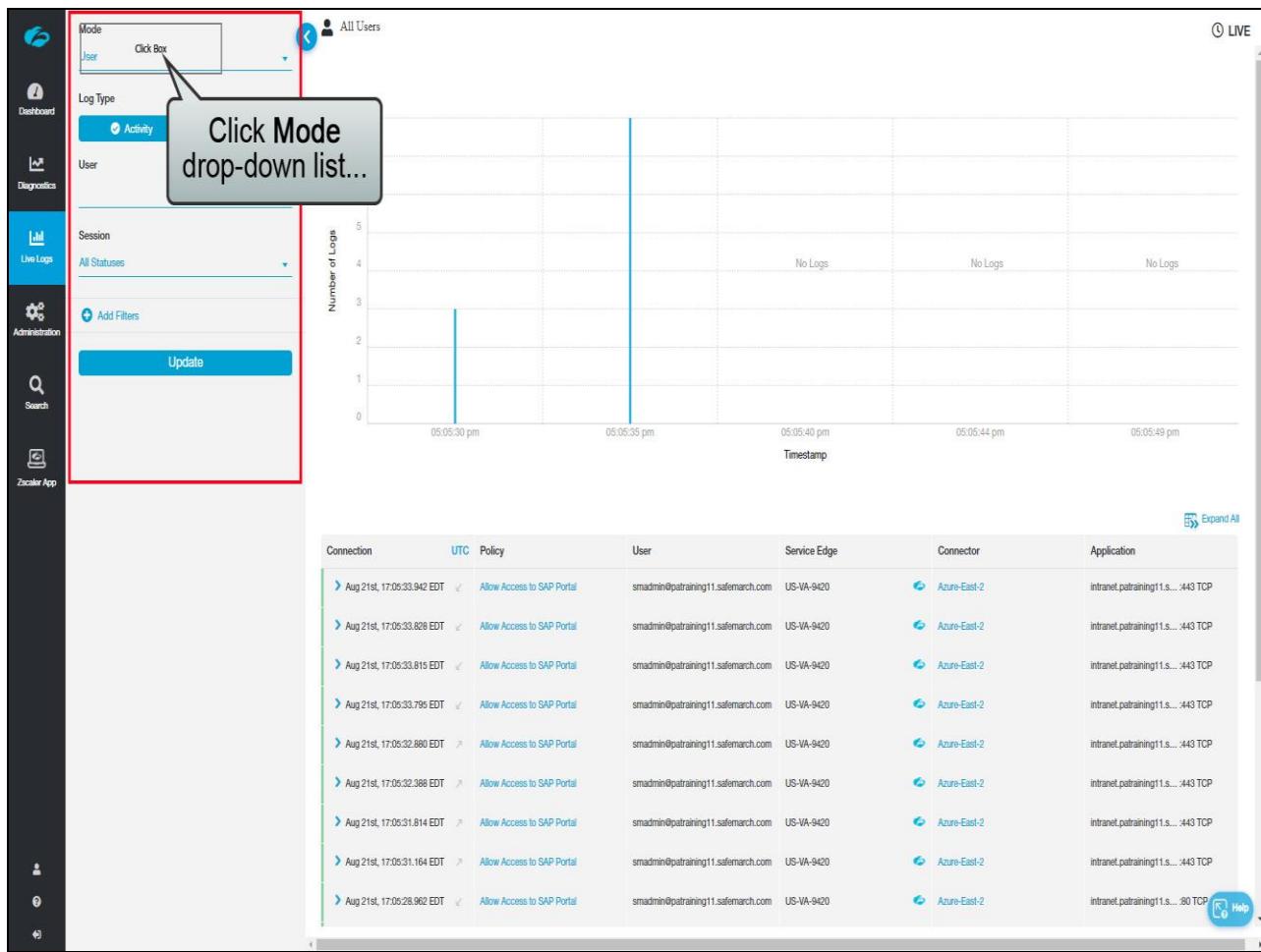
Slide notes

The log display will start to stream events as they happen and display them on a graph showing the last 75s in 5s time-slices.

An event is indicated by a blue line on the graph, and the new logs are displayed in the table below.

Click the **# New Logs** button to refresh the table and view the latest logs.

Slide 92 - Slide 92



Slide notes

For example, for **User** mode, you have the option to specify whether to view **Activity** logs (to view application access activity), or **Status** logs (to review session status).

Click the **Mode** drop-down list...

Slide 93 - Slide 93

Connection	UTC	Policy	User	Service Edge	Connector	Application
Aug 21st, 17:05:33.942 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:33.828 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:33.815 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:33.795 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:32.880 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:32.888 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:31.814 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:31.164 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:443 TCP
Aug 21st, 17:05:28.962 EDT	<input checked="" type="checkbox"/>	Allow Access to SAP Portal	smadmin@patraining11.safermarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP

Slide notes

...and select Application.

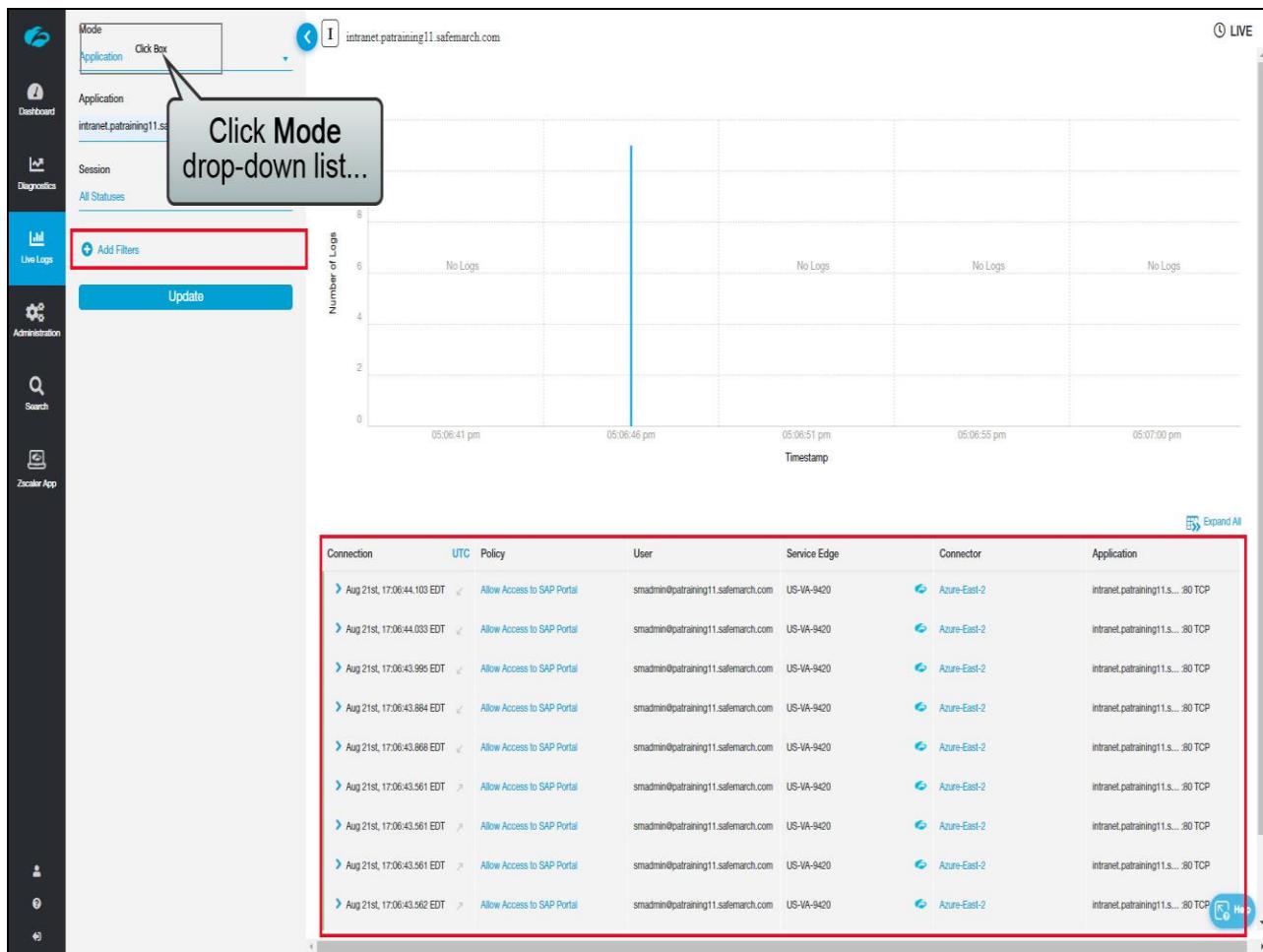
Slide 94 - Slide 94

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs (which is selected and highlighted in blue), Administration, Search, and Zscaler App. The main area has a header with 'Mode Application' and a URL 'intranet.patraining11.safemarch.com'. A red box highlights the 'Application' dropdown in the top navigation bar. Below it, a grey callout box with the text 'Click Update' points to a blue button labeled 'Update' in the 'Live Logs' section. The 'Live Logs' section includes a search bar, filter options ('All Statuses', 'Add Filters'), and a table with columns: Connection, UTC, Policy, User, Service Edge, Connector, and Application. The table shows 'No Items Found'. At the bottom right of the main area is a 'Help' icon.

Slide notes

Specify an application and click **Update**.

Slide 95 - Slide 95



Slide notes

As with the **User** logs, these logs can be viewed in real-time, or as a historic list. Filters are available to be applied to the **Application** logs as well, both standard filters and an additional list of filters that are specific to applications.

Click **Mode** drop-down list again...

Slide 96 - Slide 96

The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs (selected), Administration, Search, and Zscaler App. The main area has a header with 'intranet.patraining11.safemarch.com' and a 'LIVE' button. A modal window titled 'Select Connector Status' is open over a log table. The modal contains a 'Click Box' input field and a 'Private Service Edge Status' dropdown menu with options like 'All Statuses', 'Up', 'Down', and 'Unknown'. The log table below has columns for Connection, UTC, Policy, User, Service Edge, Connector, and Application. It lists 10 entries from Aug 21st at 17:06:44 to 17:06:43.562 EDT, all with the policy 'Allow Access to SAP Portal' and user 'smadmin@patraining11.safemarch.com'. The connector column shows 'Azure-East-2' and the application column shows 'intranet.patraining11.s...:80 TCP'. A 'Hub' button is visible in the bottom right corner of the log table.

Connection	UTC	Policy	User	Service Edge	Connector	Application
Aug 21st, 17:06:44.103 EDT	✓	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:44.033 EDT	✓	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:43.995 EDT	✓	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:43.884 EDT	✓	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:43.866 EDT	✓	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:43.561 EDT	✓	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:43.561 EDT	✗	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:43.561 EDT	✗	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP
Aug 21st, 17:06:43.562 EDT	✗	Allow Access to SAP Portal	smadmin@patraining11.safemarch.com	US-VA-9420	Azure-East-2	intranet.patraining11.s...:80 TCP

Slide notes

...and select **Connector Status**.

Slide 97 - Slide 97

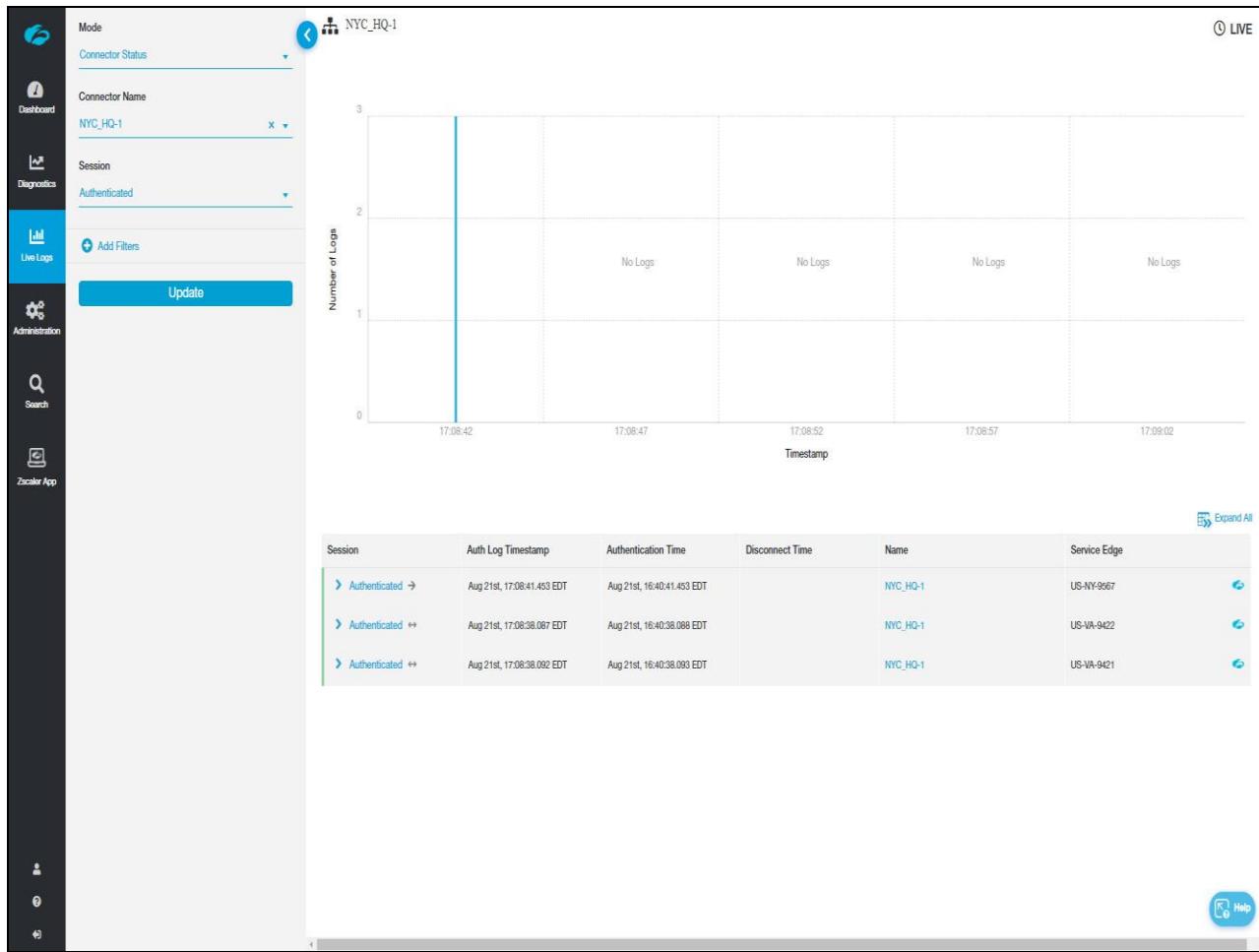
The screenshot shows the ZCTA-PA Troubleshooting Tools interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs (which is selected), Administration, Search, and Zscaler App. The main area shows a connector named 'NYC_HQ-1'. The 'Live Logs' section has a 'Connector Status' dropdown set to 'NYC_HQ-1' and a 'Session' dropdown set to 'All Statuses'. A blue button labeled 'Update' is highlighted with a callout box containing the text 'Click Update'. Below the button is a chart titled 'Number of Logs' showing three data series: 'No Logs' at 17:07:22, 'No Logs' at 17:07:27, and 'No Logs' at 17:07:32. At the bottom is a table with columns: Session, Auth Log Timestamp, Authentication Time, Disconnect Time, Name, and Service Edge. The table shows 'No Items Found'. There is also a 'Expand All' button.

Slide notes

As before, real-time and historic views are available, and filters can be applied to the Connector logs as well, both standard filters and an additional list of filters that can be added. In this example, we specified one particular App Connector.

Having added and configured the filters you need, don't forget to **Update** the log view.

Slide 98 - Slide 98



Slide notes

Slide 99 - Thank you & Quiz



Thank you & Quiz

Slide notes

Thank you for following this training module on ZPA troubleshooting tools, 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.