\*\*Login for Labs 1-7 lasts for 3 weeks\*\*

1. Navigating the ZDX Admin Portal

**Content**

* View the ZDX Dashboard
* View Applications Overview page
* View User Overview page
* View Automated Root Cause Analysis Data
* View Call Quality Dashboards
* View Inventory Dashboards
* View Deep Tracing Results and Alerts

1.1: View ZDX Dashboard

To view widgets and graphs available on the Performance Overview page, follow these steps:

1. At the top of the ZDX Dashboard, select **24 Hours**from the dropdown list.
2. To zoom in/out on the map, use the **+** and **–** controls.
3. Click **Draw Fence** and then use your mouse to draw a rectangle around a geographic area.
4. Click **Filter Selection**
5. Scroll through the graphs for the selected area.
6. Click on any point in a graph to get more details.
7. Below the ZDX Score graph, click **Add Another Application** to select one from the dropdown list
8. Click **Reset**.
9. At the top of the ZDX Dashboard, click **Geolocations**and select a location from the dropdown list.
10. Click **Apply**.
11. View the Performance Overview reports for the location.
12. Click **Reset**.
13. To view widgets and graphs available on the Incidents Overview page, follow these steps:
    1. Go to **Dashboard > Incidents Overview**
    2. Review the information for the various incident areas
    3. Scroll down to Incidents by Epicenters map, click on a marker; select one of the incidents
    4. Click the **View incidents Details**link and review the collected metrics.
14. To view widgets and graphs available on the Self-Service Overview page, follow these steps:
    1. Go to **Dashboard > Self Service Overview**
    2. Explore the summary graphs about notifications in the selected timeframe
    3. Click to review the details for a specific notification.

**Note:** Review current notification configuration under **Administration** > **Self Service Settings**.

**Optional:** Explore the System Generated reports, QBR reports and ZDX Snapshots available from the **Analytics** tab.

1.2: View Applications Overview Dashboard

In this task, you will browse information about monitored predefined and custom applications. To access the Applications Overview Dashboard, follow these steps:

1. From the main menu on the left, select **Applications**.
2. In the Applications Overview:
   1. Sort the applications table based on **ZDX Score Trend**.
   2. Click the application with the lowest ZDX Score
   3. In the **ZDX Score Over Time** graph, drag your mouse to zoom in on a time period with a significant change.

Note: You may have to change the reporting timeframe to see meaningful data.

* 1. Click **Zoom out**.
  2. Scroll down to view the **Page Fetch Time** graph and most impacted **Departments**, **Regions**and **Zscaler Locations**
  3. View information about the application's configured probes.

1.3: View User Overview Dashboard

In this task, you will browse available user overview reports. To access the User Overview Dashboard and view user-specific metrics, follow these steps:

1. From the main menu on the left, select Users.
2. Select an application from the dropdown list, and then click Apply
3. Under **ZDX Score User Distribution**, toggle between **Poor**, **Okay**and **Good**to update the user table.
4. Select a user with either Poor or Okay performance.
5. Review the user’s device information, e.g. OS type and IP address information.
6. Click **View More Device Details**
7. View the details under the **Hardware**, **Network**and **Software**tabs. Then click **Done**.
8. View the selected application’s **ZDX Score Over Time** graph for that user.
9. To review Web Probe Metrics:
   1. Scroll down to the **Web Probe Metrics** graphs.
   2. Clickto select/unselect web probe graphs as needed.
   3. Click anywhere on a graph to get more details about spikes in Page Fetch Time, Server Response Time, etc
10. To review Cloud Path Metrics:
    1. Scroll down to the Cloud Path Probe Metrics graphs.
    2. View the Cloud Path graph for **Latency**and **Packet Loss**.
    3. Select/unselect any of the Cloud Path legs, as needed.
    4. Scroll down to the **Hop View** and expand the view for the leg with the highest differential latency (shown in Orange)
    5. Mouse-over a hop to get more information
    6. Click the **Command Line View** and identify hops with high packet loss and/or latency
11. To review Device Health Metrics:
    1. Scroll down to the **Device Health** section and customize the set of graphs, e.g. unselect **Disk**.
    2. View the various graphs.
    3. Click on a graph to display more details, e.g. **CPU Usage** and **Most Impacted Processes**
    4. Under **User Device Events**, mouse-over a circle on one of the timelines to view the event details

1.4: View Automated Root Cause Analysis Data

In this task, you will search for a specific user that reported problems with an application and use the ZDX Y-Engine to analyze possible root causes by following these steps:

1. Search for the user in the ZDX Admin Portal:
   1. From the main menu on the left, select **Search**.
   2. Start typing the user name, e.g. **Curtis Hardwick** and press **Enter**.
   3. Click on the user's name in the search results
   4. Select an application from the drop-down list and click **Apply**
2. In the **ZDX Score Over Time**graph, click on a graph point with **poor**ZDX score.
   1. Click **Analyze Score**.
   2. Review the results of the automated root cause analysis
   3. Scroll through the Web Probe Metrics, Cloud Path view and Device Health information, and confirm the root cause analysis was correct
   4. Scroll back up to the ZDX Score Over Time graph.
   5. Drag the slider to select a time range
   6. Click **Analyze Range**
   7. Review the results of the automated root cause analysis for the selected time range
   8. Use the  buttons to provide feedback.
   9. Scroll back up to the ZDX Score Over Time graph.
   10. Click **Compare to**and select **Same time 1 day ago**
   11. Scroll through the side-by-side comparison graphs
   12. Identify key differences between the two points in terms of web metrics, cloud path details and device metrics

1.5: View Call Quality Dashboards

In this task, you will view the details for a recent Microsoft Teams meeting. To view Call Quality metrics, follow these steps:

1. From the main menu on the left, select **Applications > Microsoft Teams Call Quality**.
   1. Scroll through the Overview reports, e.g. ZDX Score Over Time
   2. At the top of the page, click the **Meetings**tab and view the list of recent meetings
2. To review details for a meeting, follow these steps:
   1. Either click the **meeting name** or click theicon
   2. Review the Meeting Details and the overview of meeting participants.
   3. Click theicon to view details for one user.
3. To view Call Quality metrics for a specific user, follow these steps:
   1. In the **Sessions and User Devices** list, click the name of a user.
   2. Scroll down to the **Meeting Monitoring Metrics** for that user
   3. Click on a point in any of the graphs and review the details.
   4. Scroll down further to the **Cloud Path**section and review the details of hops along the data path between end user and the Microsoft Teams Transport Relay URL
   5. Scroll down further and review **Device Health** metrics and **User Device Events**

1.6: View Inventory Dashboards

In this task, you will browse software and hardware inventory reports. To view Software Inventory information, follow these steps:

1. From the main menu on the left, select **Inventory > Software Overview**.
   1. View the current count for installed software, vendors, and the total users.
   2. Mouse over an application tile. A tooltip displays the total number of installations for application, as well as the total number of versions for the application.
   3. Click any tile, e.g. **Microsoft Edge**.
   4. Review the details for the selected application.
   5. Click an application name to drill down further.
   6. Review the list of devices and users of that application
   7. Click the **eye**icon for a device to review the version history details.
   8. Click a username to drill down further and view their installed software
2. **Optionally**: Go to **Inventory > Process Overview** and explore software processes that may be impacting the performance of user devices.
3. To view your organization's devices and their associated users, follow these steps:
   1. From the main menu on the left, select **Inventory > Device Overview**.
   2. View the current device count and total active users.
   3. Mouse over and click any tile.
   4. Click a **devicename**and review its hardware, network and software details

1.7: View Deep Tracing Results

In this task, you will view the details for a recent Deep Tracing session. To view Deep Tracing results, follow these steps:

1. From the main menu on the left, select **Diagnostics > Deep Tracing**.
2. In the **History**table, click theicon for a previously captured Deep Tracing session.
   1. Scroll through the report data
   2. Click on an unusual spike or drop in any of the graphs to see more details, including a list of the most impacted software processes.
   3. Close the Deep Tracing session results window.

1.8: View Alerts

In this task, you will view the details for ongoing and historic alerts. To view alerts, follow these steps:

1. From the main menu on the left, select **Alerts**.
2. Review the number of alerts, as well as number of impacted devices, geolocations and applications.
   1. With the **Ongoing Alerts** tab selected, click the icon to view an ongoing alert.
   2. Scroll through the alert details
   3. Return to the **Alerts Overview**page.
   4. Click the **Alert History** tab and view the details for an alert that has ended.

2. Troubleshooting Poor Wifi

**Problem Statement**

A user is reporting poor user experience involving frequent disconnections, slow internet speeds and difficulty in completing work tasks. This issue is impacting the user's productivity and causing frustration. Initial indications are that the issues may be caused by poor Wi-Fi, but the details are vague.

User: **Curtis Hardwick** Device: **PC-Curtis-WiFi** Time Range: **Last 48 Hours**

Highlights: **Poor Wifi Signal**, **SSID Changing**, **Y-Engine Comparison**

In this section, you will troubleshoot to pinpoint the exact root cause by:

* Filtering to display *ZDX Score* and application performance data for the user for the time period of the incident.
* Using the ZDX Y-engine *Analyze Score* feature to find the factors that might have impacted ZDX score.
* Comparing *Cloud Path* data before and after a degradation of ZDX score to pinpoint root causes.
* Viewing *Device Events* associated with ZDX score changes.
* Identifying device event details that impact user experience.

2.1: View User ZDX Score for an Application

In this task, you will search to see ZDX score data for a user for an application covering the time period that they have been having issues. To view the user ZDX score for an application, follow these steps:

1. Search for the user in the ZDX Admin Portal:
   1. Click **User Search**.
   2. Start typing the username in the search box. (**Curtis Hardwick**).
   3. Click on the user's name in the search results
2. View the ZDX score for an application for the period of the incident.
   1. Select the time period for the incident (e.g., **48 Hours**).
   2. Select an application (e.g., **Salesforce Lightning**).
   3. View the **ZDX Score Over Time** graph
   4. Observe that the ZDX score is fluctuating often between **Good**and **Poor**

2.2: Analyze Poor ZDX Score Interval

In this task, you will zoom in on the data to focus on a time when the ZDX score fluctuated from Good to Poor. You will use the *Analyze Score* capability of the ZDX Y-Engine to identify factors that might have impacted the ZDX score. To analyze a poor ZDX score interval, follow these steps:

**Note**: **Your results will differ from the screenshots shown here** - feel free to explore! Traffic in the lab is simulated, so what you see will depend on the traffic and the data points you select. Repeat steps as necessary against different data points to see how the changing conditions affect the analysis.

**Use these examples as a guide to help you navigate and choose data to analyze.**

1. Zoom in to analyze the details for an application with a fluctuating score.
   1. In the **ZDX Score Over Time** graph identify a time period when the ZDX Score is **Poor**. **Click**and **drag**to zoom in on that time period.

**Note**: For best results, ensure that the selection includes time **before and after** the Poor score period.

* 1. **Click**to set the cursor on a **point on the graph with a Poor score**.
  2. View the **ZDX Score** displayed for that sample.
  3. Click **Analyze Score**. Analysis will take a few seconds to complete.
  4. View the analysis results table titled *The following factors that might have impacted the ZDX score*

In this example, the score of 10/100 most likely came from a Low Wifi Signal, and the Suboptimal Wifi degraded user performance after connecting to the 3Com\_Wifi SSID.

2.3: Compare Poor ZDX Score to Last Known Good Score

In this task, you will use the ZDX comparison tool to highlight the important differences between a sample with a poor score to the last known good score. To compare a poor ZDX score to the last known good score, follow these steps:

1. Click **Compare to** for the selected point on the ZDX Score Over Time graph.
2. Select **Last known good score.**
3. Examine the data for the **Analyzed Point** and note the differences shown for the **Comparison Point**, particularly in terms of:
   1. ZDX Score.
   2. WiFi identifier
   3. Client-Egress Latency

2.4: Isolate High Latency Hop

In this task, you will examine Cloud Path Hop View to pinpoint the high latency. To isolate the high latency hop, follow these steps:

1. Click the **<- Compare ZDX Scores** link at the top of the page to return to the user report.
2. **Zoom in** again on a period containing a Poor ZDX Score in the ZDX Score Over Time graph.
3. Scroll down to view the **Cloud Path** graph and latency values at the selected data point.

Results will vary, but you most likely see low latency at the beginning of the selected time period for when the ZDX score was Good, and it will likely change to **high latency** when the score drops to Poor.

1. Examine the **Hop View** visualization below the graph. It will display a breakdown of each of the detected hops between the client and the server for the selected application, and the latency measured for each hop.

**Note**: If the network connection was lost there will be no data available to report on, and the Hop View will not be able to be displayed. Pick a different point in time where data is showing in the graph to analyze.

In this example, the Hop View isolates the slow end-to-end latency to the first hop between the user's device and their local gateway (319ms of the overall 339ms).

2.5: View User Device Events Associated With ZDX Score Changes

In this task, you will examine User Device Events and view the details that were recorded when the ZDX score dropped.

To, view User Device Events associated with ZDX score changes, follow these steps:

1. Scroll down to the bottom of the page to view the **User Device Events** timeline plots.
2. **Mouse-over** the **dot**on the Network timeline at the time corresponding to when the ZDX Score transitioned to Poor. You will see a pop-up showing details of the **Network Interface** data recorded at that sample.
3. **Scroll**through the Network Interface data to identify the type of event that changed at that point (indicated by a value recorded in the **New Value** field).

In this example, the **SSID Change** from the **Google\_Nest** to the **3Com\_Wifi** SSID is associated with the **Poor** score transition

1. **Mouse-over** the **dot**corresponding to when the ZDX Score transitioned back to **Good**.

In this example, switching back to the **Google\_Nest** SSID is associated with a **Good** score.

Summary: ZDX Troubleshooting Poor Wifi

In this example, ZDX Score data confirmed the user report of sporadic poor performance. By zooming in to a specific period of poor performance and using the ZDX Y-Engine, the issue was quickly isolated to a poor Wifi signal. Comparing a sample showing poor performance against the last known sample showing good performance zeroed in quickly on the switch to the 3Com\_Wifi SSID as the root cause. This enables immediate action to resolve the issue by addressing the problem with the specific Wifi device that is performing poorly.

3. Troubleshooting End User Device Root Causes - High CPU

**Problem Statement**

A user is sometimes experiencing slow device performance and slow application access. They indicate that the problem is sporadic, with periods of poor performance followed by good response for a short time. They have reported the issue to the service desk, and it has been escalated to your team for immediate attention to determine what is causing the periodic slowdowns so the issue can be resolved.

User: **Barry Bogdown** Device: **Barry-PC** Time Range: **Last 48 Hours**

Highlights: **CPU Peaks, Offending Process (e.g. Adobe Premier)**

In this lab, you will troubleshoot to pinpoint the exact root cause by:

* Filtering to display *ZDX Score*and application performance data for the user for the time period of the incident.
* Viewing the quantitative data that confirms the poor user experience.
* Using the ZDX Y-engine *Analyze Score* feature to find the factors that might have impacted ZDX score.
* Viewing *Device Events* associated with ZDX score changes.

Task 3.1: View User ZDX Score for an Application

In this task, you will search to see ZDX score data for a user for an application covering the time period that they have been having issues. To view the user ZDX score for an application, follow these steps:

1. Find the user and the affected device:
   1. User: **Barry Bogdown**.
   2. Device: **Barry-PC**.
   3. Select the time period for the incident (e.g. **48 Hours**).
2. Analyze the user's ZDX Score over the period.

In this example, the repeating pattern of periods of poor and then good performance confirm the symptoms reported by the user.

Task 3.2: Analyze Poor ZDX Score Interval

In this task, you will zoom in on the data to focus on a time when the ZDX score fluctuated from Good to Poor. You will use the *Analyze Score* AI capability to identify factors that might have impacted the ZDX score. To analyze a poor ZDX score interval, follow these steps:

1. View the ZDX score for a Poor Score interval.
   1. Select an interactive user application. (e.g. **Microsoft Teams Web App**).
   2. **Zoom**in on a **Poor**score period.
2. Analyze the ZDX score when it drops from Good to Poor.
   1. **Click**on the point on the ZDX score where it first drops to **Poor**.
   2. Click **Analyze Score**.
   3. Examine the table listing *The following factors might have impacted the ZDX score*.

In this example, the top factor listed is **Device CPU High**.

Task 3.3: View Quantitative User Experience Metrics

In this task, you will look at Web Probe Metrics data collected at the time of the ZDX Score dropped to Poor. To view quantitative user experience metrics, follow these steps:

1. Scroll down to the **Web Probe Metrics**section.
2. Examine the **Page Fetch Time** graph.

In this example, Page Fetch Time (PFT) was **5633ms** at the time sample selected, compared to the PFT Baseline of **701ms**. This metric confirms that the user was experiencing an **8x slower** response time.

Task 3.4: View Device Health - CPU Usage Data

In this task, you will look at the device health data that was collected at the time of the ZDX Score drop to Poor. To, view device health - CPU usage data, follow these steps:

1. Analyze the CPU Usage data collected at the time of the ZDX Score drop to Poor:
   1. Scroll down to the **Device Health** section of the report.
   2. View the **CPU Usage** value collected. (e.g. 100%).

**Note**: A cursor line is displayed on each graph at the sample time point selected to analyze. Read the values shown in the popup when the mouse pointer is moved over the line.

1. **Click**on the **cursor line** to see the details of the **Most Impacted Processes**.

In this example, the escalation would be resolved by reporting back to the Service Desk that the periods of poor performance were most likely being caused by Adobe Premier Pro.exe activity spiking to bog down the CPU. This level of detail enables Service Desk to work with Barry Bogdown to confirm that this is the root cause of the periodic slowdowns and resolve the issue.

1. Scroll down to the Top Processes by CPU Incidents graph and confirm the application with the highest CPU usage

Summary: ZDX Troubleshooting End User Device Root Causes - High CPU

In this example, ZDX Score data confirmed the user's report of periodic poor performance. Analysis of a period of poor performance by the ZDX Y-Engine identified the most likely cause as being high CPU usage on the user's device. Examining Page Fetch Time data from the Web Probe metrics showed the sudden spike in latency, and the associate Device Health data showed the 100% CPU Usage as the root of the issue. Details from the software inventory further isolated Adobe Premiere Pro.exe as the process using 97% of the CPU.

4. Troubleshooting Slow DNS Response

**Problem Statement**

A user reports to the service desk that they are having a consistently poor experience when accessing SaaS apps. Zoom calls are fine once connected, but anything web based is very slow.

User: **Linda Lucas**Device: **Linda-PC-Route5**  Time Range: **Last 48 Hours**

Highlights: **Poor App Experience**, **Slow DNS Response Times**, **Y-Engine**

In this lab, you will troubleshoot to pinpoint the exact root cause by:

* Viewing the user's overall ZDX score over the time period of the incident.
* Analyzing the high page fetch times for overall latency issues.
* Using the ZDX Y-Engine to determine the root cause.

Task 4.1: View User ZDX Score Over Time

In this task you view the overall ZDX score for all monitored applications covering the time period that the user has been having issues. To view the user ZDX score over time, follow these steps:

1. Find the user and the affected device:
   1. User: **Linda Lucas**.
   2. Device: **LINDA-PC-ROUTE5**.
2. View the ZDX score for the period of the incident.
   1. Select the time period for the incident (e.g. **48 Hours**).
   2. View the **ZDX Score Over Time** graph

Observe that in this example:

* ZDX score is consistently Poor over the entire interval.
* Score for every application is poor (13/100 or lower).

Task 4.2: Analyze High Page Fetch Time

In this task, you will analyze the web probe metrics for the user to look for patterns that can help to isolate the cause of the user's poor ZDX score. To analyze high page fetch time, follow these steps:

1. Scroll down to view the **Web Probe Metrics** section of the report section.
2. Analyze the **Page Fetch Time** Graph Note the range of values over the period. In this example it varies from ~1000ms to ~3000ms.
3. Analyze a specific web probe sample:
   1. **Click**on a point on the Page Fetch Time graph.
   2. Note the difference between the **PFT Baseline** and the **Page Fetch Time** value at the selected point.

In this example, we see the Page Fetch Time of 1790ms which indicates quite overall high latency for each page request. It is much longer than the PFT Baseline of 516ms.

* 1. Note the relative breakdown of the Page Fetch Time between the measurements for **Server Response Time** and **DNS Resolve Time**.

In this example, note:

* High fluctuations in the DNS Resolve Time.
* DNS Resolve Time accounts for most of the overall Page Fetch Time latency.

Task 4.3: Use ZDX Y-Engine to Determine Root Cause

In this task, you will use the ZDX Y-Engine to confirm your analysis of the likely cause of the high Page Fetch Time. To use the ZDX Y-Engine to determine root cause, follow these steps:

1. Scroll back up to the **ZDX Score Over Time** graph.
2. Click **Analyze Score** and note the factor listed in *The following factors might have impacted the ZDX score* table.

In this example, High DNS is the most likely root cause of the poor performance. Confidence Level is shown as 100%. Note that details needed to isolate this further to the specific DNS Server are recorded in the User Devices at the top of the page. DNS Server for LINDA-PC\_ROUTE5 is 10.0.1.53

Summary: Troubleshooting Slow DNS Response

In this example, viewing the ZDX score over a 48 hour period showed consistently poor ZDX scores for all applications, and the Page Fetch Times showed an ongoing problem of high latency for all transactions. Examining the breakdown between DNS Resolve Time and Server Response Time isolated the issue to DNS, which was confirmed by the ZDX Y-Engine analysis.

5. Troubleshooting Slow Network Router (Hop)

**Problem Statement**

The user reports very poor experience when they are accessing SaaS apps. They commented that the problem seems to show up randomly and sometimes seems to get resolved on its own.

User: **Quincy Martin**   PC: **QUINCY-PC**  Time Range: **Last 48 Hours**

Highlights: **Poor App Experience**, **SLOW Network Response Times**, **Y-Engine**

In this lab, you will troubleshoot to pinpoint the exact root cause by:

* Confirming sporadic SaaS Application Performance.
* Analyzing high page fetch times.
* Identify the high latency link in the path to the cloud.
* Analyze the point of highest hop latency.
* Comparing Cloud Path data before and after a degradation of ZDX score to pinpoint root causes.

Task 5.1: Confirm Sporadic SaaS Application Performance

In this task, you view the overall ZDX score for a specific SaaS application covering the time period that the user has been having issues to confirm the sporadic drops in ZDX Score. To confirm sporadic SaaS application performance, follow these steps:

1. Search for the user:
   1. Click **User Search**.
   2. Start typing the user name in the search box. (**Quincy Martin**).
   3. Click on the user's name in the search results.
2. View the ZDX score for the period of the incident.
   1. Select the time period for the incident (e.g. **48 Hours** for the most recent data, or pick a **Custom**time interval covering 48 hours that includes the time of the user complaint.).
   2. Select a SaaS application (e.g. **ServiceNow**).
   3. View the **ZDX Score Over Time** graph.

Observe that the ZDX score is fluctuating often between Good and Poor over the report period. This confirms the user's report of the sporadic poor performance.

Task 5.2: Analyze High Page Fetch Time

In this task, you will analyze the metrics collected by the Web Probe for the user to look for patterns that can help to isolate the cause of the user's poor ZDX score. To analyze high page fetch time, follow these steps:

1. Scroll down to view the **Web Probe Metrics** section of the report section.
2. Analyze the **Page Fetch Time** Graph. Look for patterns in the page fetch times.

In this example, Page Fetch Time will be below the PFT Baseline (indicated by the green horizontal line) for a period and then it suddenly increases for a few hours, and then decreases again. Increased Page Fetch Times correspond to times when the ZDX Score drops to Poor.

1. Note the relative breakdown of the Page Fetch Time between the measurements for **Server Response Time** and **DNS Resolve Time**.

In this example, note that both DNS Resolve Time and Server Response Time increase when Page Fetch Time increases. This likely points to an overall increase in end-to-end latency, rather than a separate issue with either DNS or the server.

Task 5.3: Identify High Latency Cloud Path Link

In this task, you will analyze the metrics collected by the Cloud Path Probe for the user to isolate the cause of the user's poor ZDX score. To identify the high latency cloud path link, follow these steps:

1. Scroll down to the **Cloud Path**section of the user report.
2. Select a point on the graph when the End-End latency is high. Examine the latency metrics to determine which hop is contributing the most to the End-End latency.

In this example, the Client-Egress contributes 496ms to the overall End-End 551ms latency.

Task 5.4: Analyze High Hop Latency

In this task, you will drill in to analyze the details of the high latency cloud patch link. To analyze the high hop latency, follow these steps:

1. Scroll to the **Hop View**.
2. Locate the high latency link.

In this example, the Client-Egress latency (496ms) is noted on the hop between the client Gateway and their Egress point to the Internet.

1. Click the **magnifying glass** icon to expand the view of the link, and note the specifics of where the high latency was detected.

In this example, the high latency is isolated to be between the Client Gateway at 10.1.2.1 and the next hop to the router at 10.0.0.254.

Task 5.5: Confirm Key Differences with ZDX Score Comparison

In this task, you will use the ZDX comparison tool to highlight the important differences between a sample with a poor score to the last known good score. To confirm key differences with ZDX Score Comparison, follow these steps:

1. Scroll back up to the **ZDX Score Over Time** graph.
2. **Click**to select a time when the score was **Poor**.
3. Select **Last known good score**
4. Examine the Key Differences table for the **Analyzed Point** and note the differences shown for the **Comparison Point**.

**Note**: In this example, the much higher Client-Egress Latency is one of the key differences listed. This confirms the previous analysis done to identify this manually by examining the cloud path data

1. Click **View Detailed Cloud Path** to see a direct comparison of the Hop View for the Analyzed Point to the Comparison Point.
2. Click **Close**to return back to the comparison view.
3. Click **<- Compare ZDX Scores** to return to the User report.

Summary: Troubleshooting Slow Network Router (Hop)

In this example, sporadic drops in SaaS application performance were confirmed by drops in the ZDX Score, supported by the high Page Fetch Times measured by the Web Probes. Simultaneous high latency for both the DNS Resolve Time and the Server Response indicated that latency somewhere on the path. Cloud Path data enabled further isolation to the hops between the Client device and their Internet Egress point, and zooming in on the hop details isolated the issue to the IP address of the router having issues. ZDX score comparison enabled quick confirmation of the location and IP address of the router at the source of the issue.

6. Analyzing Call Quality

**Problem Statement**

A user is reporting poor call quality and overall meeting experience when on Teams meetings, the issue is sporadic, so it is difficult for the servicedesk to troubleshoot.

User: **Grady Archie**  Device: **GRADY-PC**  Time Range: **Last 48 Hours**

Highlights: **Poor Call Quality**, **MOS Score**, **Cloud Path Slow Hop**

In this lab, you will troubleshoot to pinpoint the exact root cause by:

* Viewing the Microsoft Teams Call Quality trend.
* Examining meeting metrics.
* Locating meeting issues.

Task 6.1: View Microsoft Teams Call Quality Trend

In this task, you will view the trend for Microsoft Teams Call Quality over the past 48 hours. To view the Microsoft Teams call quality trend, follow these steps:

1. Click **Applications**and note the ZDX Score Trend for Microsoft Teams Call Quality.

In this example, the ZDX Score Trend shows a poor score for Microsoft Teams Call Quality (22/100).

Task 6.2: Examine Meeting Metrics

In this task, you will drill into the details of a meeting to see detailed measurements of the call quality. To, examine meeting metrics, follow these steps:

1. Click the **Meetings**tab.

Since call quality metrics are only collected while calls are active, the metrics show gaps in the displayed data for periods where there were no active calls.

1. Zoom in to analyze the details for a specific meeting. **Click**and **drag**to zoom in on that time period.
2. Click on a Meeting ID to see meeting details.
3. Click on one of the listed users to drill into the details for their devices.

In this example, the meeting includes sessions for two users (Irwin Syyers and Grady Archie). Both meetings participants were connected for about 1 hour, with an overall Poor ZDX Score for each.

1. Check each of the devices listed under User Devices to show the one that includes Microsoft Teams Call Quality in the list of Applications.

In this example, Gradiy Archie has two different user devices connected, and it is the second device on the list that shows metrics for Microsoft Teams Call Quality.

Task 6.3: Locate Meeting Issues

In this task, you will view the metrics collected to monitor the meeting to locate where to look for more details on why the ZDX Score is Poor. To locate meeting issues, follow these steps:

1. Scroll down to the **Meeting Monitoring Metrics** section of the report.
2. **Click**on one of the **data points**to see the pop-ups showing the metric values. Examine the charts for measurements help to locate where to look further. In particular examine:
   1. **Audio MOS Score**
   2. **Audio latency in/out**

In this example, an Audio MOS scores of 2.06 (in) and 2 (out) indicate the audio part of the call as a major factor in the overall poor meeting quality. A related Audio Latency of 640ms both in and out highlights that high latency is driving poor audio quality.

Task 6.4: Locate Source of Audio Latency

In this task, you will examine the Cloud Probe metrics to locate where the calls are encountering high latency. To locate the source of audio latency, follow these steps:

1. **Scroll**down to the **Cloud Path** section of the report.
2. Examine the **Hop View** to locate the hop that is contributing the most to the overall latency.

In this example, the hop between the GRADY-PC device and the local Gateway at 10.1.2.1 accounts for 569ms of the overall 640ms end-end latency, pinpointing the root cause of the poor user experience on Teams meetings.

Summary: Analyzing Call Quality

In this example, the poor ZDX score for the Microsoft Teams Call Monitoring confirmed the user's report of poor call quality. Drilling down to see the details for a call and into the specifics collected for one of the users further confirmed low Audio MOS scores, and highlighted audio latency as the driver for poor quality. This led further to the quick isolation to the root cause of high latency between the user's PC and their local gateway.

7. Troubleshooting Device Startup and Software Reliability Issues with Microsoft Intune Integration

**Problem Statement**

A user reports that they are frustrated with the overall user experience with their PC. They also comment that Chrome crashes frequently, and when they try a restart to clean things up it is sometimes slow to get going.

User: **Joni Sherman**  Device: **ZPM-JONI-SHERMA**  Time Range: **Last 48 Hours**

Highlights: **Endpoint Analytics Score**, **Health Status**, **Boot Time**, **Software Crash**

In this lab, you will troubleshoot to view data gathered via Intune to locate the source of the poor user experience by

* Analyzing high CPU usage to see what processes are impacting performance.
* Filtering to display user device details for the time period of the incident.
* Viewing the health status of the device.
* Examining the boot history collected for the device.
* Reviewing the software reliability events over the last 14 days.

Task 7.1: Analyze CPU Usage

In this task, you will look at the device health data that was collected at the time of the Poor ZDX Score. To, view device health - CPU usage data, follow these steps:

1. Search for the user:
   1. Click **User Search**.
   2. Start typing the user name in the search box. (**Joni Sherman**).
   3. Click on the user's name in the search results.
2. Scroll down to the **Device Health** section of the report.
3. Click on a point of high **CPU Usage** to see the list of **Most Impacted Processes**.

In this example, chrome.exe is using 94% of the CPU. This would have a negative impact on the overall machine performance user experience.

Task 7.2: View Endpoint Analytics

In this task you will drill down to see the analytics collected on the endpoint device by Microsoft Intune for the user who has been having issues. To view endpoint analytics, follow these steps:

1. Scroll back up to the **User Devices**section.
2. Click **View Endpoint Analytics**.
3. Examine the **Startup Performance** and **Software Reliability** category scores.

In this example, the Startup Performance of 96/100 looks ok, but the Software Reliability score of 46/100 is low.

Task 7.4: Review Software Reliability Events

In this task, you will review the software reliability data collected on the endpoint. To review software reliability events, follow these steps:

1. Click the **Software Reliability**tab.
2. Note the frequency of startup events shown in the bar chart for **Software Events Over Last 14 days**.
3. Review the details of each item recorded in the **Software Events** table.

In this example, we see from the graph that there are a large number of software events recorded in the first 3 days in particular. From the events listed it looks like Chrome and Edge were crashing frequently.

Summary: Troubleshooting Device Startup and Software Reliability Issues with Microsoft Intune Integration

In this example, we saw poor performance was caused by Chrome hogging the CPU. Data collected from Microsoft Intune on the endpoint device showed a number of App crash software events as well as a fairly long startup at one point. Quick access to this data for the past 14 days through ZDX enables rapid isolation of the root cause of the performance issue as well as a detailed history of processes that are crashing.

**Note**: Make sure, you **log out** of the ZDX Read-Only Tenant.

8. Configuring Cloud Applications Monitoring

**Problem Statement**

Consider the scenario where your organization (Safemarch) has identified an initial set of business-critical cloud applications that need to be configured in ZDX. In this lab, you will:

* Log into a simulated end user device and verify that Internet traffic is being forwarded to Zscaler via the Client Connector
* Enable predefined cloud applications for monitoring, and
* Create a custom application and probes for monitoring.

Task 8.1: Verify Traffic Forwarding to Zscaler

In this task, you will check that traffic is being forwarded from the Client PC to the Zscaler cloud. You will authenticate to the ZIA service as a user in the Finance department. To check the traffic forwarding, follow these steps:

1. On the **Client PC VM**, sign in to the Zscaler Service as a test user:
   1. From the Windows Status Bar, click to **Show hidden icons**, then click on the **Zscaler Client Connector** icon and select **Open Zscaler**.
   2. When the Zscaler Client Connector user interface opens, enter the **Student Username** and click **Login**.
   3. At the *Pick an account* dialog, click **Use another account**.
   4. Enter your **Student Username**and**Password**again and click **Sign in**.
   5. At the *Stay signed in? dialog*, click **No**.
   6. Open Zscaler Client Connector again and click on the **Digital Experience** tab.
   7. Verify that the **Service Status** is **ON**.
   8. Verify that the **Authentication Status** is **Authenticated**.
2. Verify that Internet access is now via the Zscaler Cloud.
   1. Open a web browser tab and go to **ip.zscaler.com**.
3. Verify that **You are accessing the Internet via Zscaler Cloud**is displayed.
   1. Verify that your username is: **student@zsxxxx.safemarch.com** (scroll down on the ip.zscaler.com page to view).

Task 8.2: Enable Predefined Applications

**Note**: Predefined Applications will either be pre-configured and require *Enabling*, or, will be Un-Configured, and need *Onboarding*. In this lab, you will use the **onboard**option, which is a one-time, one-button click process.

In this task, you will enable/onboard predefined application templates for common cloud applications. To enable a predefined application, follow these steps:

1. In a new browser tab, go to **https://admin.zdxcloud.net** and log in to your ZDX Full Access Tenant, with **ZDX Admin Username** and **ZDX Admin Password**.
2. From the main menu on the left, select **Configuration**.
3. Onboard a Predefined Application:
   1. Click to expand the **Box**application.
   2. Click **Go**.

**Note**: The application will onboard automatically, and you will see the probes associated with Box.

* 1. From the main menu, select **Activation**and then click **Activate**.
  2. Expand **Box**to verify that the application and its associated probes are now **Enabled**.

1. Repeat the steps to enable one additional Predefined Application: **Outlook Online**.
   1. Click to expand Outlook.
   2. Click **Go**.
   3. From the main menu, select **Activation**and then click **Activate**.
   4. Verify that Outlook Online is now shown as **Enabled**.

Task 8.3: Configure a Custom Application

In this task, you will configure a custom application. To configure and enable a custom application, follow these steps:

1. From the main menu on the left, select **Configuration**.
2. Select **Add New Custom Application**.
3. Enter a name, e.g. **Safemarch\_CustomApp**  and click **Save**.

Task 8.4: Create a Custom Probe

In this task, you will configure a probe for the custom application you created in the previous task. To configure a probe, follow these steps:

1. At the top of the Configuration screen, select **Probes** and click **Add New Probe**.
2. At the **Configure Probe**step of the wizard:
   1. Enter a name, e.g. **Safemarch\_Web**
   2. From the **Application**dropdown list, select **Safemarch\_CustomApp**
   3. From the **Probe Type** dropdown list, select **Web**
   4. Leave the **Probing Criteria** and **Exclusion Criteria** sections unchanged
   5. Click **Next**.
3. At the **Additional Parameters**step of the wizard:
   1. In the **Destination**URL field, enter **https://portal.azure.com**
   2. Click **Next**.
4. Review the configuration settings, then click **Submit**.

**Optional**: Add a Cloud Path probe for the custom application and explore its configuration options.

1. From the main menu, select **Activation**and then click **Activate**.
2. Verify that the custom application is now enabled:
   1. At the top of the screen, click **Applications**.
   2. Verify that the new custom application is listed as **Enabled**. If needed, enable the application.
3. Wait at least 5-10 minutes, then click **ZDX Dashboard**on the main menu and verify that the predefined and custom applications are now shown.

9. Configuring Alerts & Deep Tracing

**Problem Statement**

Consider the scenario where your organization has configured a set of business-critical cloud applications for monitoring in ZDX. You now need to establish thresholds for acceptable application performance and ensure that helpdesk staff is alerted whenever any of these thresholds are exceeded. You also need to familiarize yourself with the steps required to configure and start a Deep Tracing session for a specific user.

Task 9.1: Create an Alert Rule

In this task, you will create a new alert rule for an application. To add an alert rule, follow these steps:

1. From the main menu on the left, select **Alerts**.
2. Click **Rules**and select **Add New Alert Rule**.
3. At the **Configure Rule**step of the wizard, enter:
   1. Name: **Outlook\_Online**
   2. Severity: **High**
   3. Type: **Application**.
4. Click **Next**.
5. At the **Filters**step of the wizard, select:
   1. Application: **Outlook Online**
   2. Web Probe: **Outlook Online Login Page Probe**.
6. Click **Next**.
7. At the **Criteria**step of the wizard, select:
   1. Page Fetch Time: **>=200 ms**.
   2. **ZDX Score Drops** and Sensitivity **Medium**
8. Click **Next**.
9. At the **Action**step of the wizard, select:
   1. Alert Only if Repeated: **3**
   2. Minimum Devices Impacted: **Number 1**
   3. Alert Delivery Method: **Email**
   4. Alert Recipient: **helpdesk@training.safemarch.com**.
10. Click **Email Preview** and view an example alert email.
11. Click **X** to close the Email Preview window.
12. Click **Next**.
13. At the **Action** step of the wizard, click **Submit**.
14. From the main menu, select **Activation** and then click **Activate**.
15. Verify that the new rule is listed as **Enabled**.

Task 9.2: Configure a Deep Tracing session

In this task, you will create a new Deep Tracing session for your organization’s Finance user. To configure a Deep Tracing session, follow these steps:

1. Ensure that Zscaler Client Connector is configured to enable the collection of machine host information.
   1. In a new browser window, go to your ZIA tenant at **https://admin.zscloud.net** and log in with your **Student Username** and **Password**.
   2. In the ZIA Admin Portal, click **Policy > Zscaler Client Connector Porta**l.
   3. Go to the Client Connector Support page (**Administration > Client Connector Support**).
   4. Click the **User Privacy** tab.
   5. Check the **Collect Machine Hostname Information** setting.
   6. **Enable**it if it is not already enabled.
   7. Click **Save**.
2. Switch back to the ZDX Admin Portal.
3. From the main menu on the left, select **Administration > Deep Tracing**.

**Note**: Refresh the ZDX Admin portal page if the portal was open when making the *Collect Machine Host Name Information* change.

1. Click **Start New Deep Tracing Session**.
2. Configure the Deep Tracing session details:
   1. Name: **Studentuser\_Issue**
   2. User: **Student Username**
   3. Device: **student (VMWare…)**
   4. Deep Tracing: **Enabled**
   5. Packet Capture Probing: **Disabled**
   6. Run Session For: **15 Minutes**
   7. Click **Next**.
   8. Device Probing: **Enabled**
   9. Application: **Outlook Online**
   10. Web Probe: **Outlook Online Login Page Probe**
3. Click **Save**.
4. The new session is now listed in the **In Progress** table on the Deep Tracing page.
5. Wait a few minutes and then click theicon to view the data that has been collected so far.
6. Once the session completed, review the results