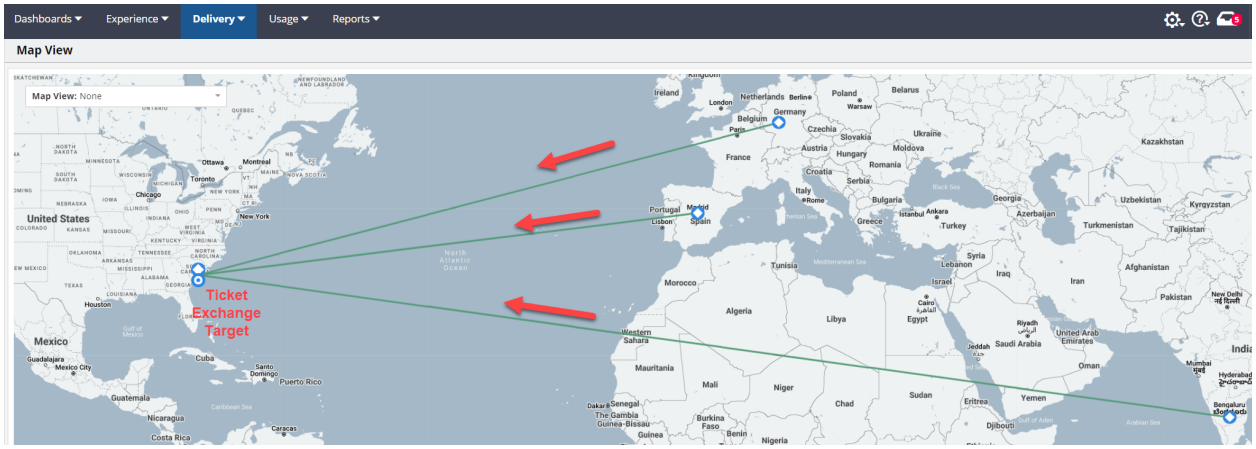
# Open Access - Experience-Driven NetOps Use Case



## Demo Environment Overview:




Access: https://demo.pm.appneta.com/pvc/login.html
User: open.access+demo@broadcom.com
Pass: CAdemo@123

There is a Cloud Web App (called Ticket Exchange) hosted in GCP US East Coast.
This WebApp is monitored from several AppNeta MPs (Monitored Points) in different locations (e.g. Frankfurt, Madrid, Mumbai). These MPs:

- send network delivery tests to gauge network path performance and obtain connectivity diagnostics to the Ticket Exchange Web Server
- send Synthetic Application Transactions (Selenium) to verify Ticket Exchange Web Server application performance

Use Cases described in this document:

| Use Cases | Value | How to trigger it | Behind the scenes | Products |
|---|---|---|---|---|
| **1. Experience Degradation** | Proactive e2e visibility to exonerate the Network from UX degradation | Auto-triggers every night at 04:00 CET | Cloud web App is degraded by bringing down a backend microservice. | AppNeta |
| **2a. Delivery Degradation - connectivity Loss** | Proactive e2e visibility into the network performance of every app/user/network | From Open Access Portal | Access to Cloud Web App is blocked at the GCP edge via script | AppNeta/DX NetOps |
| **2b. Delivery Degradation - Data Loss** | Proactive e2e visibility into the network performance of every app/user/network | Auto-triggers every hour | Data Loss is created at the User edge via script | AppNeta/DX NetOps |
| **3. Centralized Alarm Management** | Cross-silo Alarm correlation and Service-driven Monitoring | From Open Access Portal | DX OI receiving alarms from AppNeta (via RESTMon), DX UIM and DX Spectrum | AppNeta/DX NetOps + DX OI |

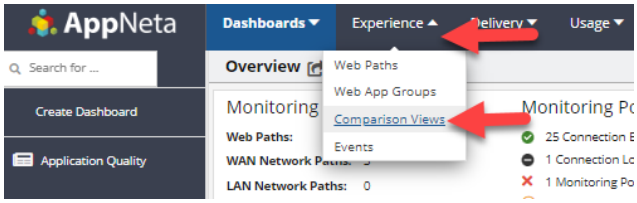
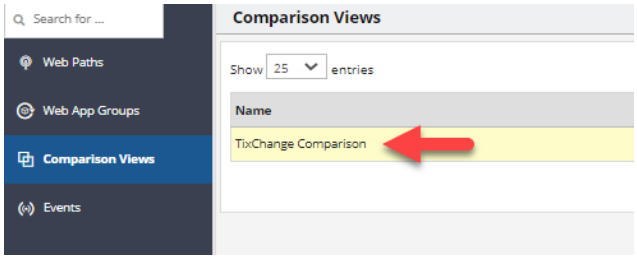
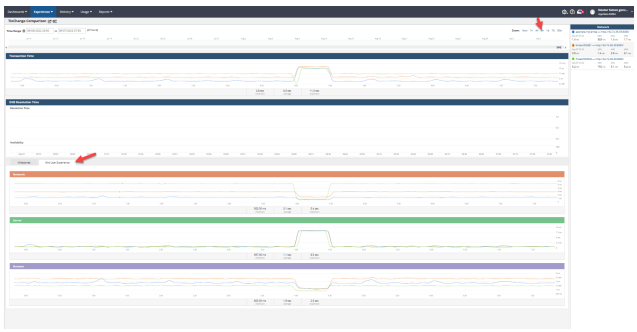
These UCs combined demonstrate how to Operationalize Experience in the New Enterprise Network. We will show how NetOps and AppNeta together empowers operators with valuable insights into the performance of applications over networks, regardless if owned or not.

Key Customer Takeaways:
- Operational awareness into UX impact of Network Performance
- Determine why users are experiencing application performance issues quickly
- Determine whether network and App service providers are meeting their SLAs
- Determine when additional capacity requirements are needed

# Use Case 1: Troubleshooting Application User Experience

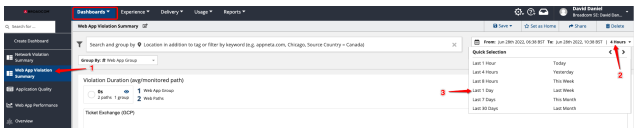
***The Story:*** Ticket Exchange users in India have reported that sometimes the Ticket Exchange is not working properly early in the morning. Complaints about purchasing Sports and Theatre Tickets are stacking up and revenue is lost! What is the root cause, who is to blame? Is the problem the network or an application issue?
See how AppNeta can be used to understand why users are experiencing application issues and prove the innocence of the network team.

***How is the UC triggered:*** The Ticket Exchange environment has a Web server, Database server and Authentication server. The Database server is shutdown down via a nightly job so a trigger is not required for this UC.

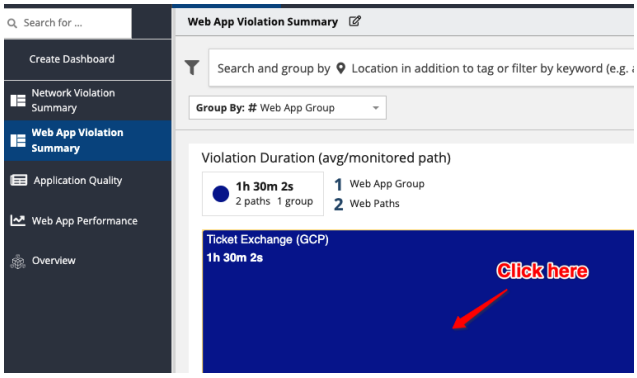
| Steps/Description | Screenshots |
|---|---|
| Let's investigate the problem. To do this, login to AppNeta and click on Experience, Comparison Views.<br>Is this isolated to one MP/region or is it a wide-spread issue? |  |
| Click now on the TixChange Comparison View. |  |
| Change the Timeframe to Last Day and verify how the same behavior is observed from all Monitoring Points. This is very valuable to determine that the issue is not isolated in a single region/MP and points to a Cloud Edge or MSP issue. |  |

Let's check now the Health of our Web Applications over the last day.

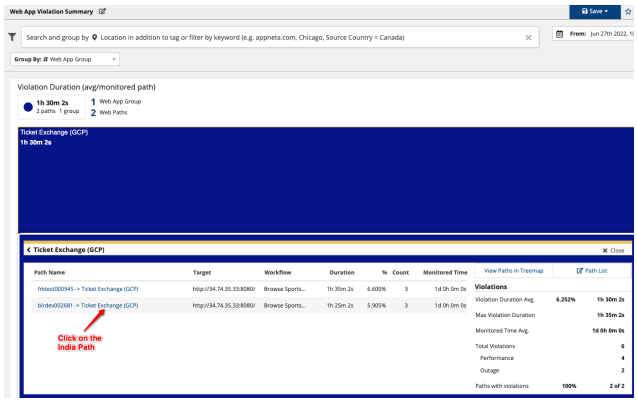
1. Go to *Dashboards Web App Violation Summary*
2. Select the time range drop down
3. **Select the last day**
4. We are displaying all violations reported for Last Day for Ticket Exchange App



Click on the blue area.
You should now be presented with summary violation data

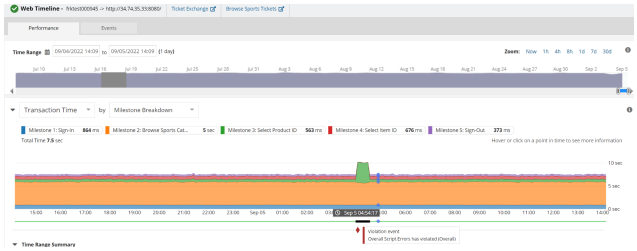


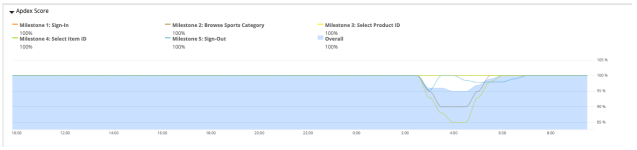
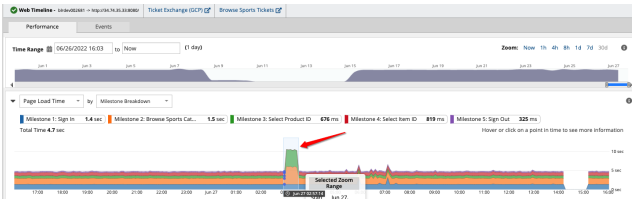
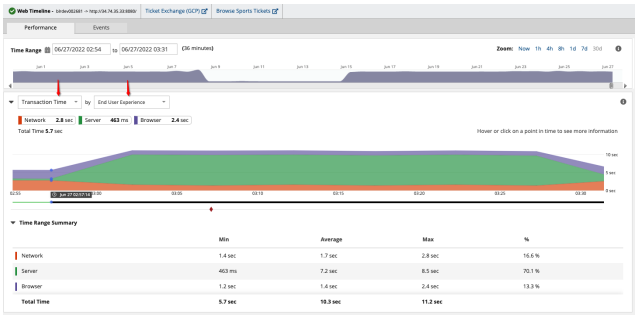

1. Click on the Path starting with "mumbai" which corresponds to India Monitoring Point - location from where Users are complaining.

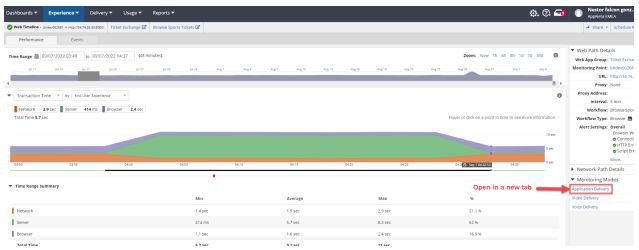
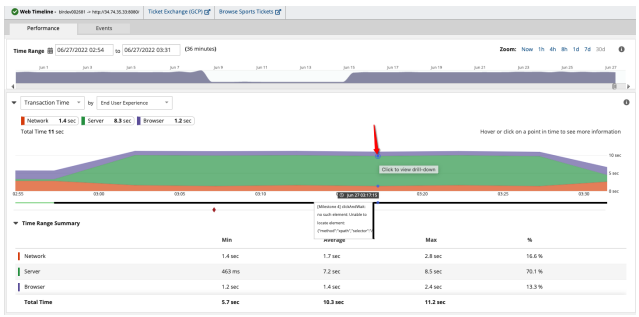
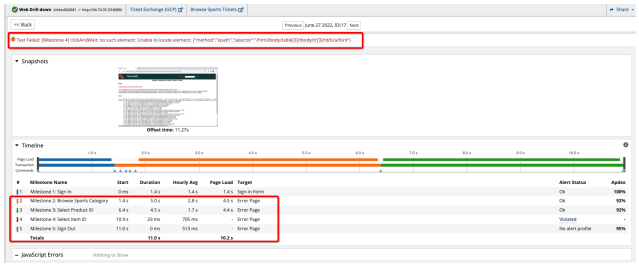
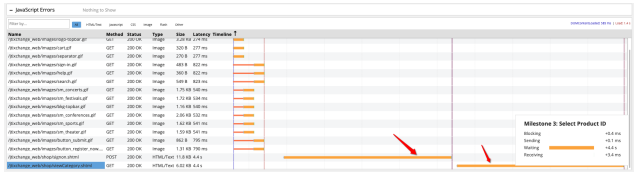


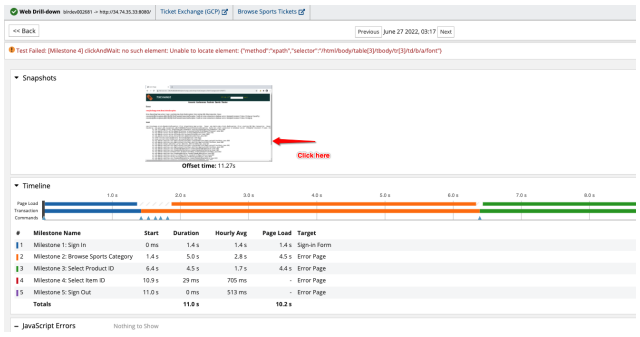
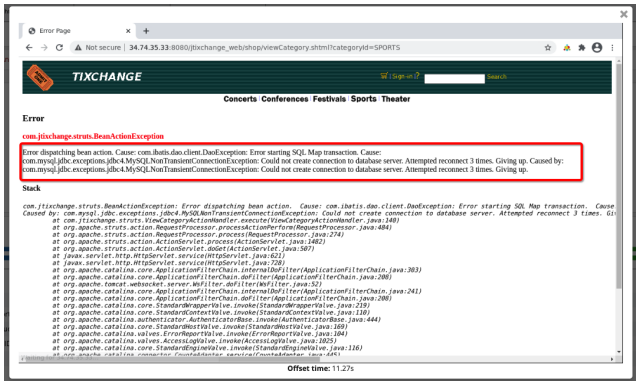

1. You will be redirected to the ***Web Timeline*** page for *the last day.* We can see a big spike early in the Timeline.
2. Notice you can mouse over the spike and the Events associated to it: Violation and Clear.

What does this mean and more importantly have users and the Ticket Exchange business been negatively impacted?



| | |
|---|---|
| Scroll down to the ***Apdex Score*** chart. We can see that UX satisfaction for around the same time of day starts to drop. Here AppNeta is giving clear insights into user satisfaction allowing operators to identify exactly where to focus their attention.<br><br>*Note: **Apdex** is an open standard developed by an alliance of companies for measuring performance of software applications in computing.* |  |
| Let's drill into the data spike we saw in the Web Timeline in more detail.<br><br>Scroll back up to the Web Timeline Page.<br><br>Now, left click, hold and drag your mouse across the data sample to zoom in and investigate. |  |
| Change drop-downs from<br><br>• *Page Load Time* to *Transaction Time*<br>• *Milestone Breakdown* to *End User Experience*<br><br>You should now have *Transaction Time by User Experience* selected. We can now profile the UX in terms of where the bottlenecks are. Is the problem related to the Network, Server (i.e. Application) or local Browser?<br><br>The Network & Client part of the user experience is very healthy! We can see that Network and Browser times are completing in a timely fashion, while most of the Transaction time is consumed waiting on the Server processing (i.e the TixChange Web Server App) |  |

| | |
|---|---|
| To prove that the issue is not related to the Network, you can click on the “Application Delivery” Link. This will take us in context to the associated Network Path showing key Network performance metrics.<br><br>**MTTI**: From the Delivery view, Network Team can prove their Innocence by validating that there is no issue on the network. |  <br>  |
| Go back to the Experience View - Web Timeline. Let’s prove the issue comes from the Application itself.<br>Click on the blue data point in the graph to drill in into the root cause. |  |
| We are now in the Web Drill-down view.<br><br>We can see that the synthetic transaction failed with “no such element error” at the top of the screen.<br><br>As we scroll down we can see a breakdown of the Milestones that are part of the overall user experience. We can see that Milestone 1 (User Login) completes successfully but that when users try to browse categories and products these pages fail. |  |
| Scroll down to the HTTP Methods breakdown chart.<br><br>The operator can see that HTTP methods for connecting to the database |  |

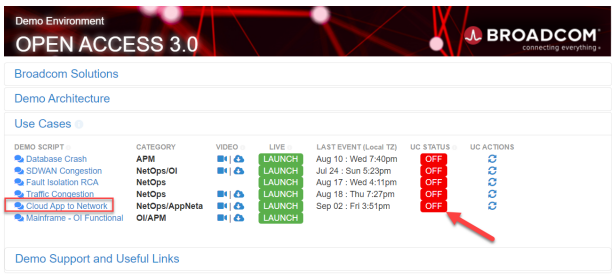
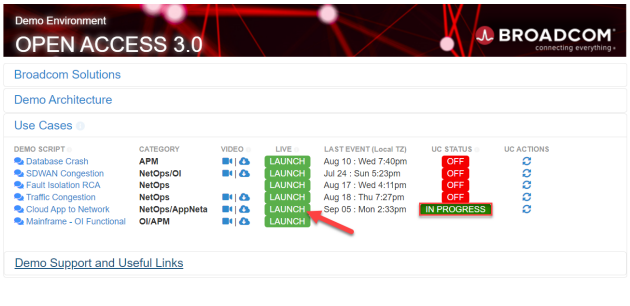
| | |
|---|---|
| server for browsing Categories and selecting Products ID's are taking a long time in comparison to the other methods. Over 4 seconds are spent "waiting" with no data received whereas the other methods are completed in milliseconds.<br><br>This is definitely starting to look like a problem connecting to the database server as we are able to connect to the web server but unable to browse contents data held in the database such as Product ID's. | |
| AppNeta also captures screen shots of synthetic transactions that fail. What does the screen shot tell us? |  |
| Instantly we have evidence of the problem. We can see that the Ticket Exchange Web Server is unable to connect to the back-end database server. Therefore, it is not possible to browse categories and products which require queries to the backend database.<br><br>The Network Team is quickly able to identify that the problem is not related to the network. They have also been able to identify that the problem is related to the databases using readily available metrics and screenshots as evidence.<br><br>This combined view of Network & User Experience diagnostics provides quick insights for both the Network and Application teams to drive down MTTI / MTTR. |  |

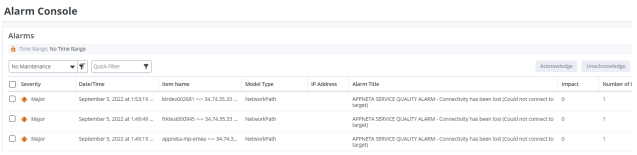
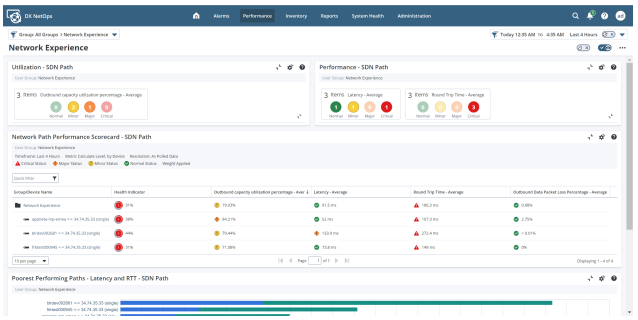
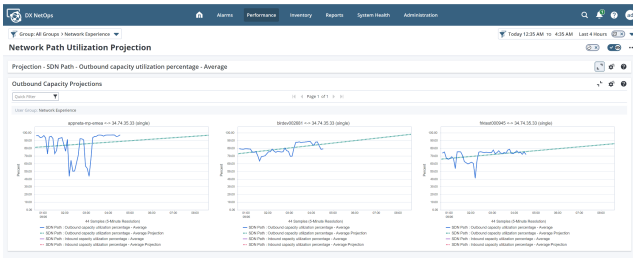
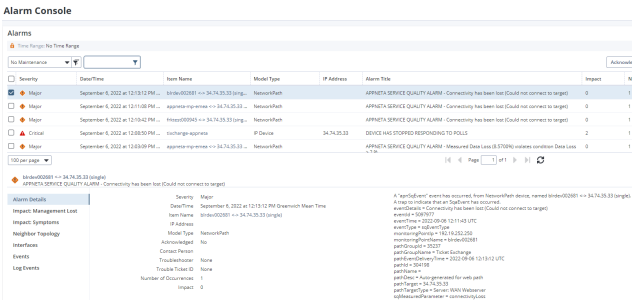
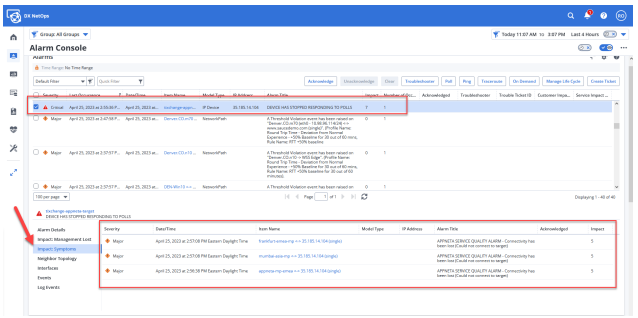
# Use Case 2: Troubleshooting Network Delivery

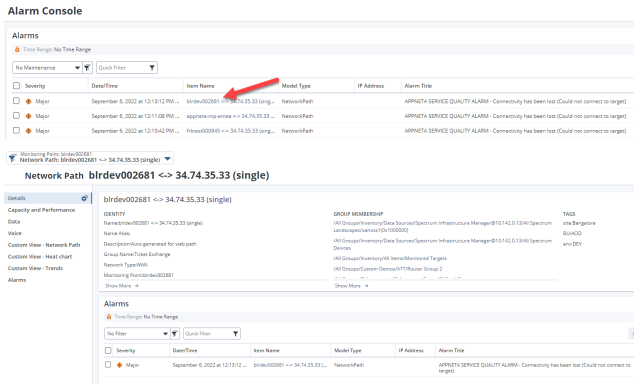
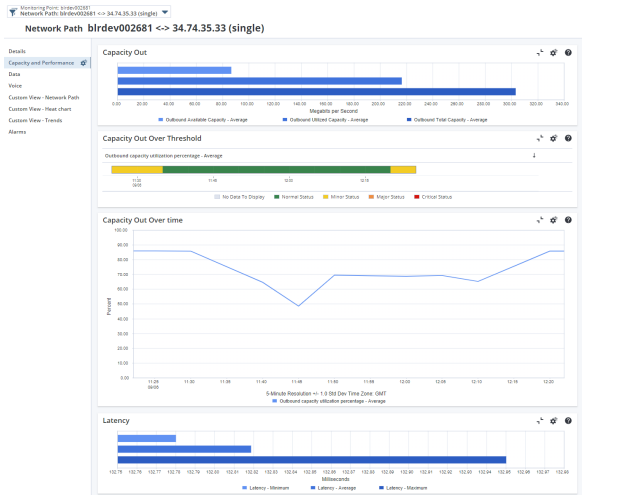
## Troubleshooting Connectivity Loss at the Cloud Edge

***The Story:*** A Cloud App Server used for trading tickets across the globe called the Ticket Exchange is unavailable. But why? How do the Network Operations team know where to focus their attention? Could the problem be internal or related to a third-party network provider (Blind Spot)? While the Ticket Exchange Server is unavailable revenue is lost!

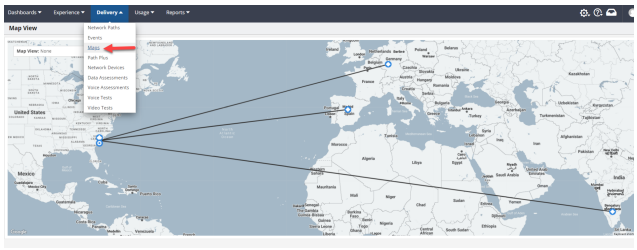
***How to Trigger the UC:*** *The Ticket Exchange Web Server is hosted in Google Cloud Platform (GCP) and you can block access to it from Open Access.* See steps below to trigger the Use Case.

| Steps/Description | Screenshots |
|---|---|
| - Login to Open Access Portal<br>- Expand *Use Cases*<br>- Locate *"Cloud App to Network"*<br>- Click on the red "OFF" button to trigger the network issue.<br><br>**Note**: If you would like to showcase the AppNeta Violation received via Slack notification. Join the channel: #notifications-appneta-openaccess A notification will be received 3-4 minutes after activating the trigger.<br><br>You can also showcase Google Chat integration. Join the space DX NetOps Open Access Alarms. |  |
| Click on the LAUNCH button. The AppNeta Demo Environment should launch in a separate tab.<br>Login to the Appneta environment using the following credentials:<br><br>User: open.access+demo@broadcom.com<br>Pass: CAdemo@123 |  |

| | |
|---|---|
| Also, login to NetOps Portal with your Open Access credentials.<br>http://netops.forwardinc.biz:8181/pc/desktop/page<br>After a couple of minutes there will be several AppNeta Events raised and synched to NetOps Portal - Alarm Console.<br>This is one of the Operators Entry Point to start troubleshooting |  |
| Another operator entry point is the Network Experience Dashboards in NetOps portal. Important to pitch our Unified Visibility key differentiator.<br>Walk through these Dashboards in NetOps portal:<br>(Make sure the Group context is set to Network Experience group)<br>1. Performance - Operations Displays - Network Experience<br>2. Performance - Operations Displays - Network Path Utilization Projections<br><br>Explain the value of being able to leverage key experience and capacity metrics from ISP and Cloud Network Paths in NetOps Portal: Unification AND Visibility. |  <br>  |
| Let's now troubleshoot the availability issue on the TixChange Cloud App.<br>Start in NetOps Portal Alarm Console.<br>You should see several AppNeta Events related to a connectivity issue.<br>Explain that these events have been generated proactively by AppNeta MPs when detecting threshold breaches or excessive network changes.<br><br>If you do not see the AppNeta Service Quality Alarms in the console, you might want to click on the exchange-appneta-target "Device Has stopped responding to Polls" alarms and inspect the tabs Symptoms.<br>This is important for noise reduction as a target going down could produce hundreds of "Connectivity Loss" alarms from Monitoring Points. |  <br>  |

| | |
|---|---|
| Deviations from baseline alarms (netops generated alarms) are also possible and very powerful to add value on top of AppNeta performance data. | |
| To begin the Triage click on the Item Name of the Alarm.<br>This will bring us to the context page for this specific path showing attributes, groups and tags associated to that Network path. |  |
| Access to metrics associated to this Path by clicking on the left menu of the Network Path view:<br>- Capacity and Performance<br>- Data<br><br>Metrics displayed on these Views look normal: No major data loss, no Capacity issues.<br><br>At this point we will need to investigate the Network Path topology to understand the connectivity issue.<br><br>NOTE: Current version of AppNeta-NetOps integration does not include a deepLink to jump to AppNeta from NetOps portal. Hence, login to AppNeta and click on Delivery, Maps. |  |

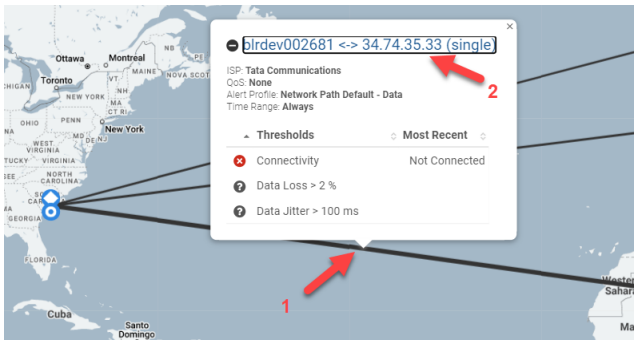
The black lines between the MPs and Ticket Exchange Server indicate a connectivity issue from all Monitoring Points.



Click on either of the network paths to see high level connectivity details. We can see that there is a connectivity issue but how will network operations diagnose the root of the problem?

Click on the path to deep dive into this connectivity situation that is affecting the Ticket Exchange Server and more importantly the revenue it generates.

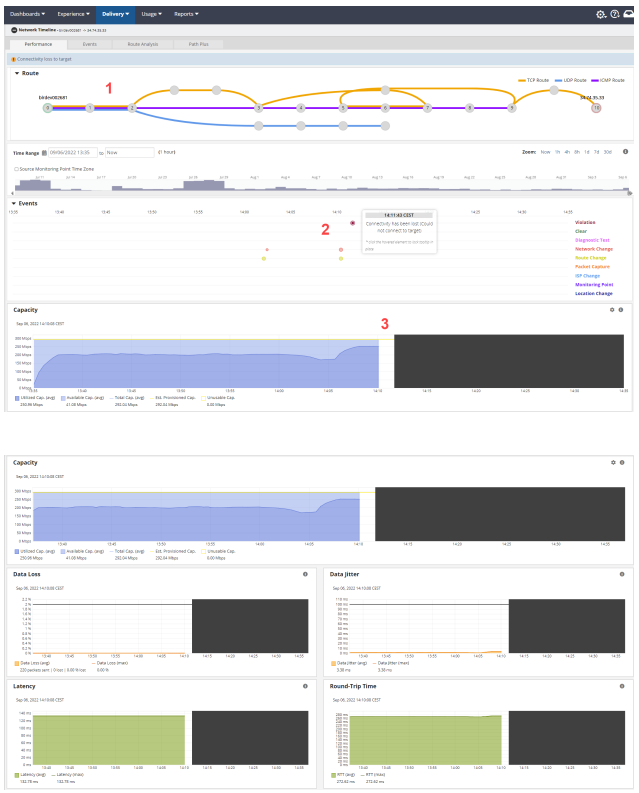
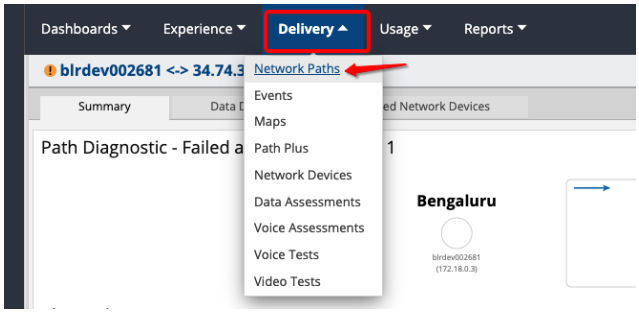
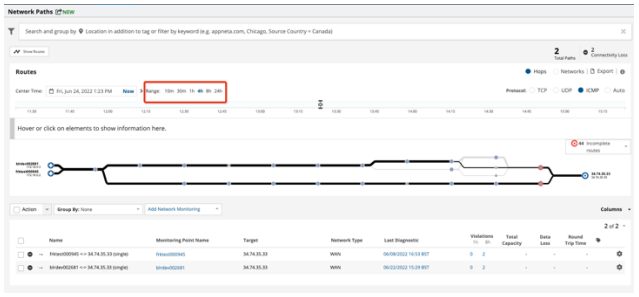
(Alternatively, start with the Slack notification received from AppNeta event or Google Chat)

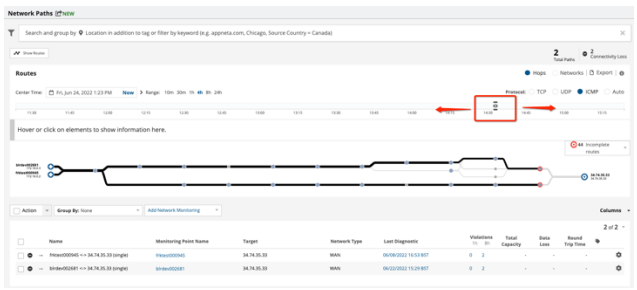
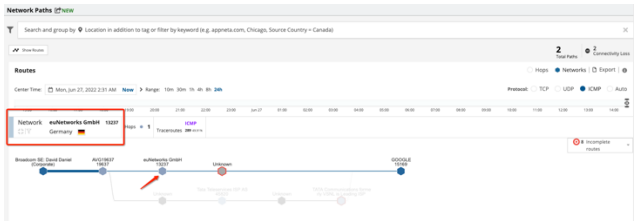


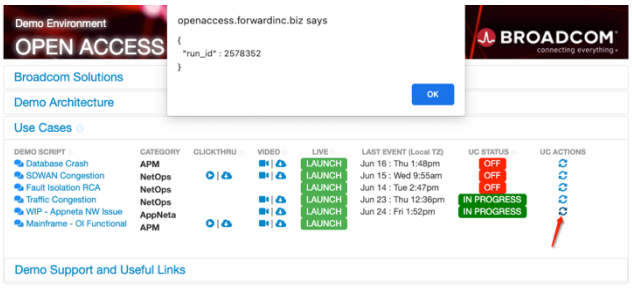

NetOps Alarms App 9 min

**Message:** APPNETA EXCESSIVE NETWORK CHANGES
**Date:** 07/11/2023 08:32:41
**Severity:** MAJOR
**Device:** frankfurt-emea-mp <-> 35.185.14.104 (single)
**Troubleshooter:**
**Service Impacted:**
TixChangeGermany (0x1005343,Degraded)
TixChangeIndia (0x1005347,Degraded)
TixChange (0x100516a,Degraded)
**Customer Impacted:**
German TixChange Users
India TixChange Users

Reply

| | |
|---|---|
| 1. Incredibly detailed path analysis giving hop by hop insights into current network path are presented.<br><br>2. Note in the Event Timeline, there is also an alert detailing the time when connectivity was lost and the violation type.<br><br>Scroll down in AppNeta to see next set of charts:<br>Capacity, Data Loss, Jitter, Latency, RTT Charts are all black since the issue occurred (refer back to event time) showing a complete loss of connectivity. |  |
| Let's deep dive into the Network path.<br>Go to:<br><br>*Delivery → Network Paths* |  |
| Change Time Range to 4 hours<br><br>Scroll left or right to find incomplete routes or routes where AppNeta Delivery tests have completed successfully. This tells a story of network path health over time. |  |

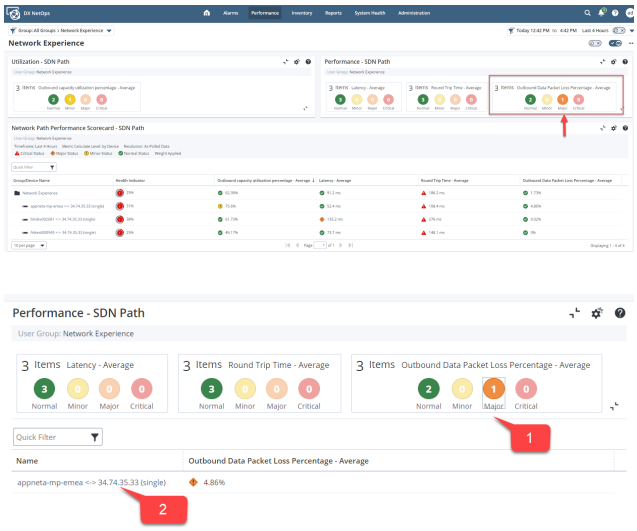
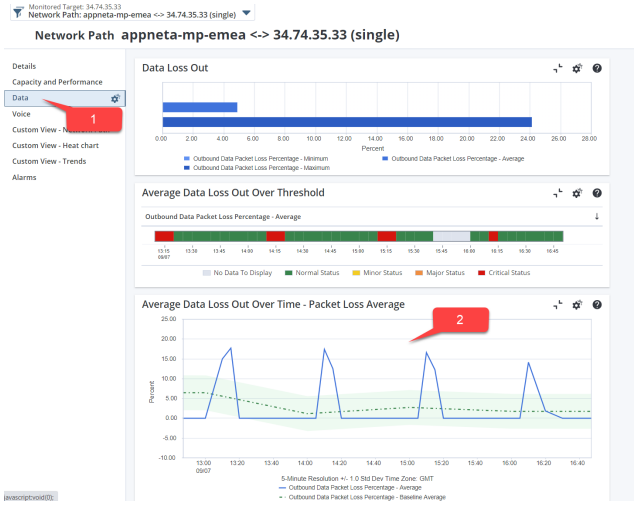
| | |
|---|---|
| |  |
| By clicking on the red circle you can see exactly where the AppNeta Delivery test fails.<br>In this case ICMP terminates on the last hop before the Ticket Exchange Server.<br><br>This information is gold to determine the hop where connectivity is failing. In this case, all points to the last hop in the ISP, right before the Ticket Exchange Server. We can now report the issue with enriched information about the issue happening in the piece of the network that we do not own.<br><br>You can also see service provider information together with RTT, ICMP data.<br><br>By clicking on the ***Networks*** hexagon icon (located upper right of screen) you can see the entire journey of the delivery test.<br><br>These hop-by-hop insights are incredibly powerful as they provide Network Operations insights of exactly who the responsible party is and where to focus their attention. |  <br>  |
| Summary:<br><br>NetOps and AppNeta together have given the Network Operations team full visibility of network delivery issues to the ticket Exchange Server. | |

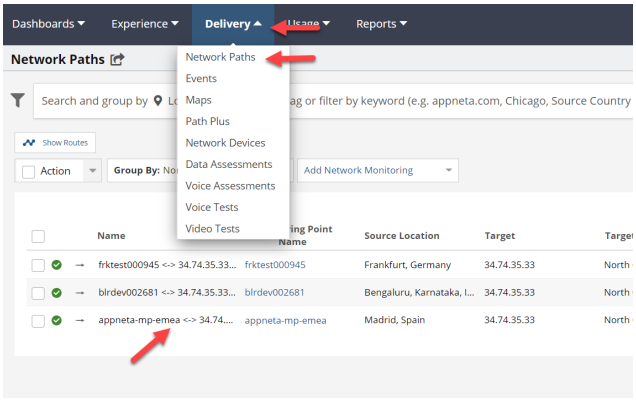
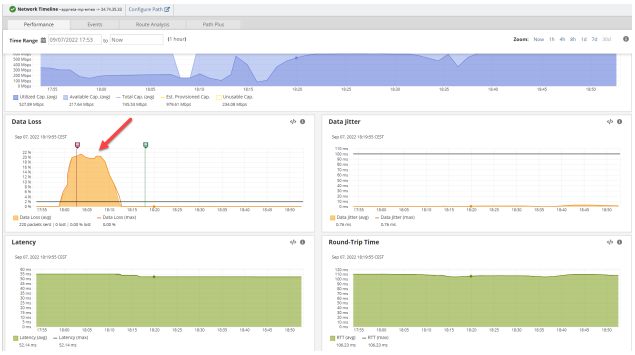
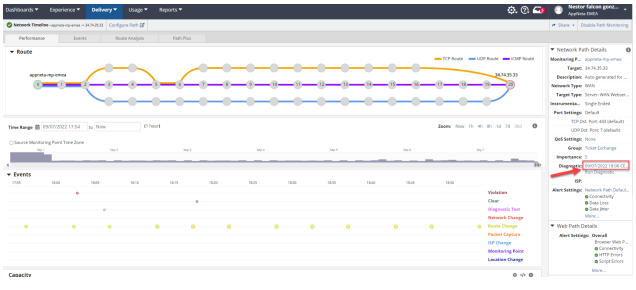
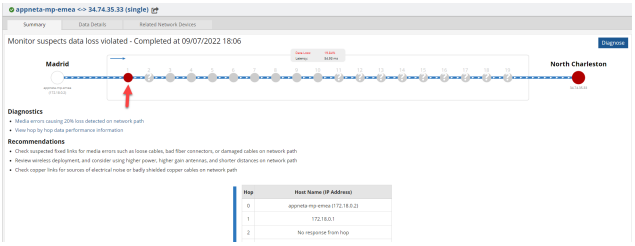
| | |
|---|---|
| Network Operations quickly discovered that the path was unavailable and were able to determine the exact hop at which the problem starts. In this specific case *TATA Communications* (subject to change) is unable to communicate with the server hosted in GCP. Hence, Network Operations know exactly where to focus their attention, saving valuable time during a business critical situation. | |
| **After the demo the use case must be reset!**<br><br>**Reset the demo manually. To do this, click on the UC ACTIONS reset button as shown in the screen shot.** |  |

## Troubleshooting Data Loss at the User edge

In the previous Use Case we have showcased an issue occurring at the Cloud Edge (e.g. Connectivity Loss at the TixChange Cloud Server - “Down” condition).
This short guide will explain how to troubleshoot a “Slow” condition at the User edge instead.

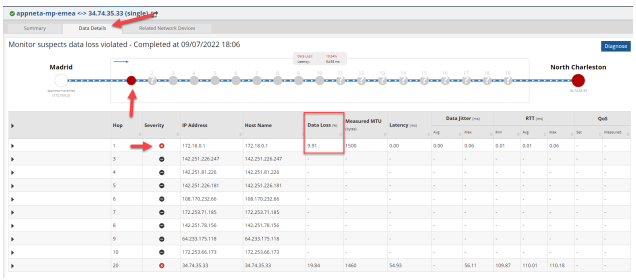
Login to NetOps Portal with your Open Access credentials.
http://netops.forwardinc.biz:8181/pc/desktop/page

| Steps/Description | Screenshots |
|---|---|
| Entry point: Network Experience Dashboards in NetOps portal.<br>Pitch here our Unified Visibility key differentiator.<br><br>Open the Dashboard:<br>Performance - Operations Displays - Network Experience<br>(Make sure the Group context is set to Network Experience group)<br><br>Note under the Performance View how one of the Network Path is presenting Data Loss.<br>We will investigate why.<br>Click on the orange/red icon from the “Outbound Data Packet Loss”.<br>Then on the Network Path entity. |  |
| In the Network Path View, click on the “Data” tab, focus on the “Average Data Loss” View.<br>This specific Network Path is experiencing a repetitive Data Loss every hour.<br>Let’s identify if this issue is happening at the User edge, ISP or Cloud edge.<br><br>We will need to switch to AppNeta at this point and access to Network Path “appneta-mp-emea” <-> 34.74.35.33 |  |

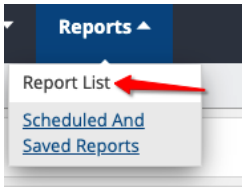
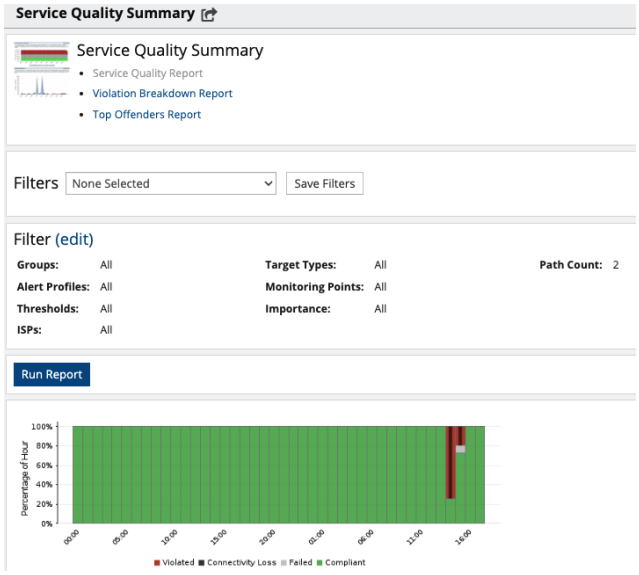
| | |
|---|---|
| [Login to AppNeta](#)<br>Access to Delivery, Network Paths and drill down to:<br>“appneta-mp-emea” <-> 34.74.35.33<br>By clicking on the Name column |  |
| Switch to Last 4 hours if needed.<br>Scroll-down and inspect the Data Loss Metric.<br>Verify how AppNeta is raising an event associated with Data Loss on this Network Path.<br><br>At the time of the issue, AppNeta has leveraged its TruPath™ technology, not only to detect degradation symptoms but also to automatically perform a diagnostic to isolate the root cause of the issue. |  |
| Scroll-up and click on the last Diagnostic performance by AppNeta on this Network Path as a result of the performance degradation. |  |
| AppNeta has determined that the Data Loss issue comes from the first hop in the Network Path.<br><br>Note the first hop flagged in red. This first hop is the local gateway of the end user, which indicates that the MP itself (user endpoint) is presenting a Data Loss condition |  |

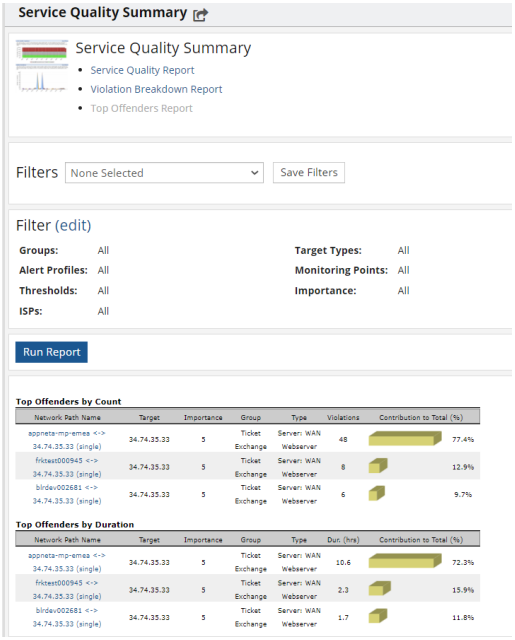
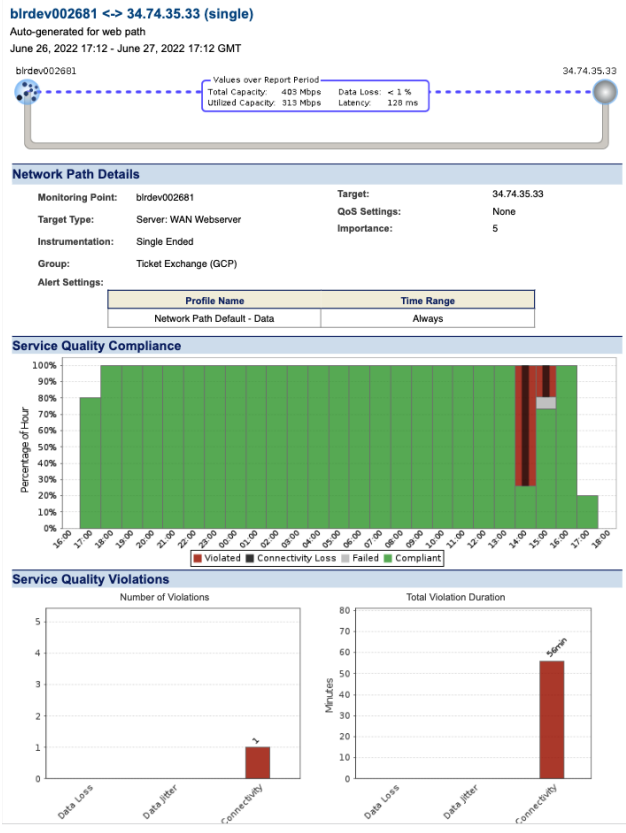
Switch to the tab “Data Details” and verify the Performance Metrics for each hop of the network path.
It is enough to see that hop #1 has about 10% of Data Loss to report that the root cause is at the source of the Network Path.

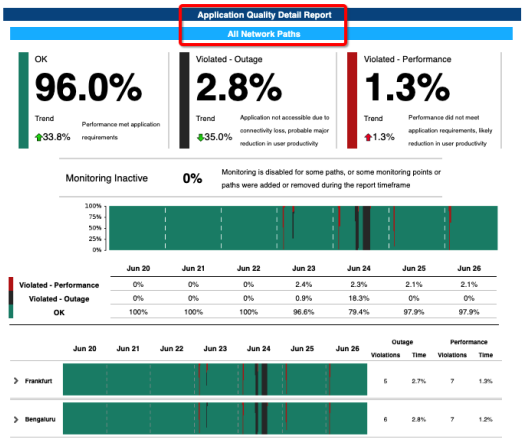
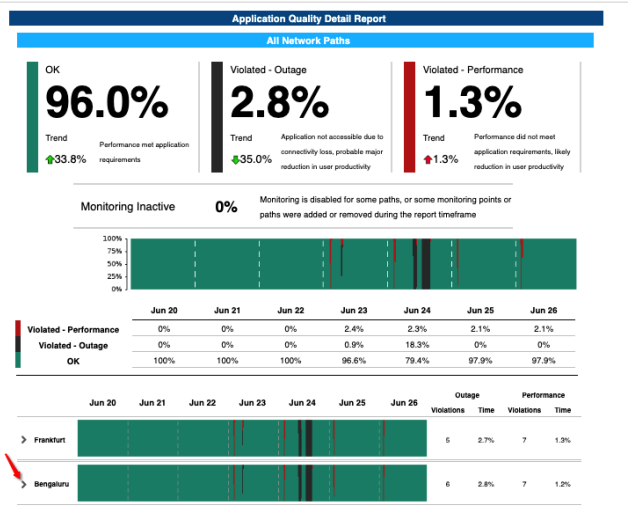
Unprecedented level of end to end visibility: From the User edge, into the public internet and 3rd party networks.



## AppNeta Reporting

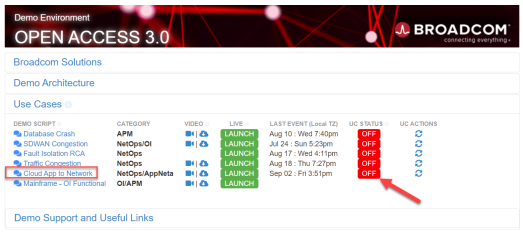
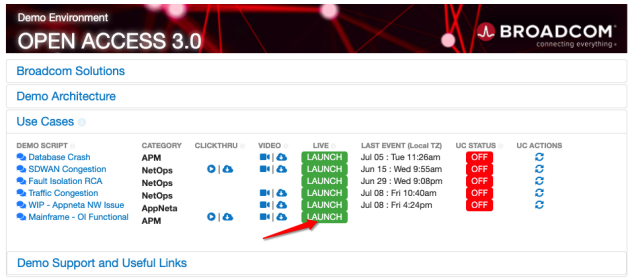
| Steps/Description | Screenshots |
|---|---|
| Want to provide more insights about Network Delivery, User Experience and track how well your ISP is performing?<br><br>Think about a scenario in a real customer Network with 1000's of Network paths. How would they know where to focus their attention?<br><br>Go to *Reports List* and Run the reports for<br><br>***Service Quality***, focus on highlighting service quality issues.<br>**Violation Breakdown**, focus on the violation type percentage (Data Loss, Connectivity)<br>**Top Offenders**, focus on the most problematic Network Paths. |  <br>Service Quality:<br>  |

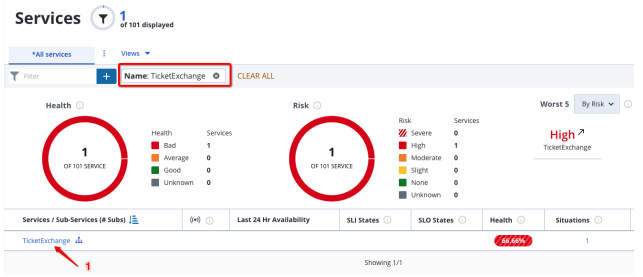
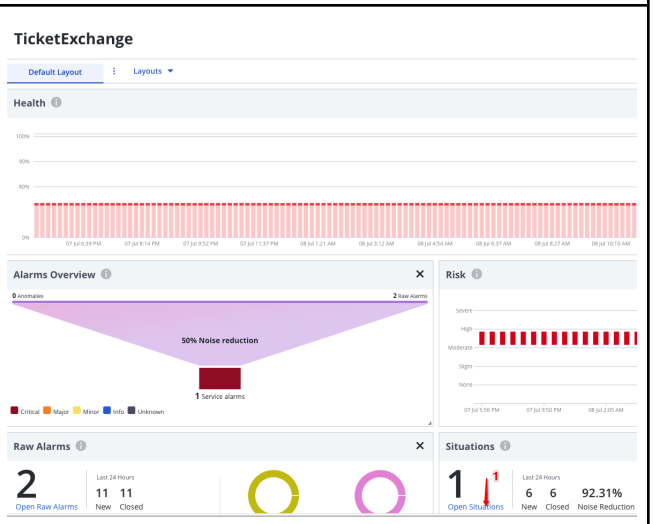
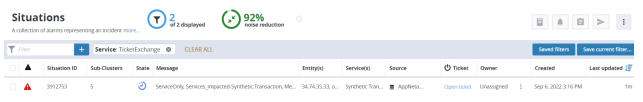
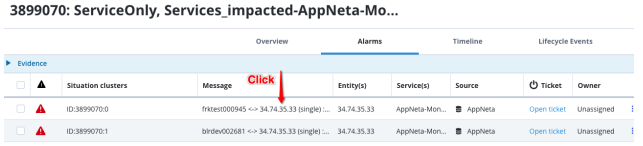
| | |
|---|---|
| |  |
| ***Network Path Detail***, a view of service quality compliance and performance metrics for selected network paths. |  |

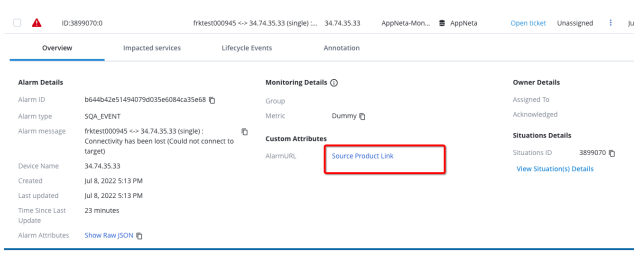
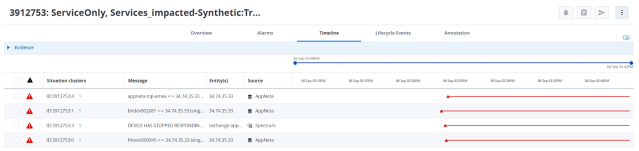
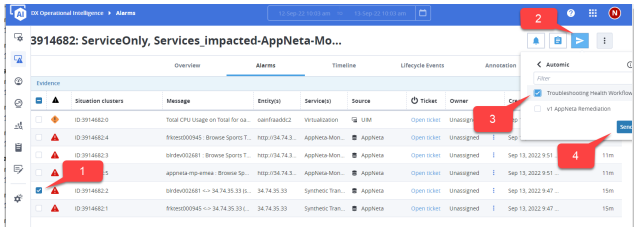
| | |
|---|---|
| ***Application Quality,*** summary report of impacted applications. In Performance Data, make sure you select All Network Paths, Network and Web Paths. |  |
| ***Location Bandwidth Quality Report,*** Compare the performance of a WAN network path to the stated performance of the Internet service package you purchased from your ISP. Quantify any differences in terms of dollars and cents so that you can adjust your service level, leverage better rates, or recover costs for poor performance. |  |

# Use Case 3: Centralized Alarm Management

Show how DX OI can be leveraged to reduce alert fatigue, grouping alerts into clusters, and execute remediation on demand to resolve service impacting issues.
This Use Case is bound to Use Case 2 as it will consume AppNeta events raised from UC2 and cluster them with NetOps and DX UIM alarms.

| Steps/Description | Screenshots |
|---|---|
| **Login to Open Access Portal**<br><br>- Expand *Use Cases*<br>- Locate *"Cloud App to Network"*<br>- Click on the red "OFF" button to trigger & activate the network issue.<br><br>**Note**: If you would like to showcase the AppNeta Violation received via Slack notification. Join the channel: #notifications-appneta-openaccess A notification will be received 3-4 minutes after activating the trigger. |  |
| Login to Mainframe OI Functional in Open Access. |  |
| We have two entry points for this use case:<br>1. Consume the event sent to Slack Channel. Alarm Triage use case<br>2. Start by showing Service Health. Service observability use case. | |
| 1. An operator might start by clicking on the DX OI alarm URL in slack.<br>2. Or, in DX OI, Service Analytics: filter by service *Name* "TicketExchange"<br><br>Click on the "TicketExchange" service |  |

| | |
|---|---|
| |  |
| In the “TicketExchange” service dashboard click on Open Situations. |  |
| You should see a recent Situation for the TicketExchange service with several alerts clustered.<br><br>Imagine a scenario where there are a couple of dozen alerts, or more, OI is able to reduce noise allowing the operator to focus their attention on the service impacting issue rather than individual alarms.<br><br>Click on the Situation ID to see lists of alerts that belong to that cluster. |  |
| Select one of the Alert Messages if you would like to talk through the alert details, impacted services or leverage Source Product Link to dive straight into the AppNeta Dashboards in context saving valuable time during the troubleshooting process. |  |

| | |
|---|---|
| |  |
| Explore the Cluster Timeline to see the arrival order of all the clustered Alarms |  |
| To trigger automation, go back to Alarms Tab, select one of the clustered alarms and click on the top right to invoke an Automic workflow.<br>From here we can trigger a Troubleshooting workflow “Troubleshooting Health Workflow” (that will add an annotation to the alarm) or a Remediation workflow “v1 AppNeta Remediation” that will remediate the issue restoring connectivity.<br><br>This can also be triggered via Policy. |  |
| Validate that after executing the “Troubleshooting Health Workflow” an Annotation is added to the Alarm, with the output of the automatic Health check executed. Great added value to reduce MTTR/MTTI.<br>The user can now proceed and open a ticket with enriched troubleshooting information attached to it. |  |