

Use Case: Ensuring Exchange and Mail Routing Availability and Performance for your Business Lines

The Challenges

Microsoft Exchange is still at the core of almost every business relationship and process with both internal and external stakeholders.

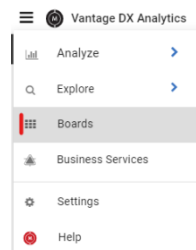
When it comes to monitoring performance of Exchange, Microsoft provides views at the tenant level of issues coming from their datacenter. However, there is no way for enterprises to measure, detect and troubleshoot issues that their business lines and users are experiencing.

Video Overview

In the demo video that accompanies this demo overview, we will show you how you can track the availability and performance of Exchange features from every critical location of your business lines to proactively ensure your employees are staying productive and connected.

Let's Get Started!

To begin, let's start with our Alerting board.



The alerting section of Vantage DX can be found in the burger menu (top left) under "Boards"

Once here you see the standard alerts we configure for our main customers.

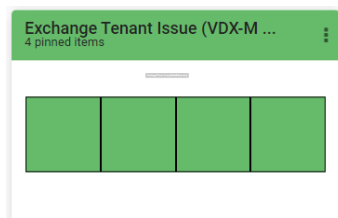


Each board shown here describes an alert condition (typically in the title) and the number of elements that have been found that have met the condition of the alert.

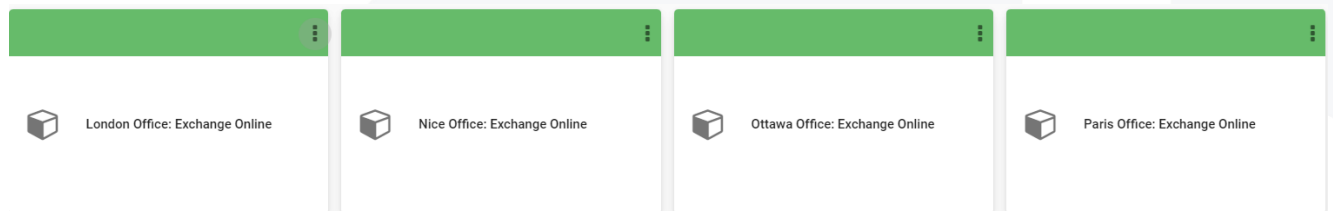
Immediately, you can see if you have specific condition that has an issue AND also the severity of the issue.

Keep in mind, that you can create and alert for *any* condition you want based on your Microsoft data.

Most of these standard alerts are also described in our video: "[Proactively Support Users With Microsoft Teams User Experience Alerting using Martello Vantage DX](#)".



From here we will focus on the alert Exchange Tenant Issues. This alert focuses on the availability and performance of Exchange features for all your critical locations. Let's open it by clicking on it.



We can see here that Martello Vantage DX is configured to test, measure and alert on Exchange service issues. These issues could also be experienced in multiple critical locations at once.

Let's go deeper and drill into the alerts to see what that has happened. By clicking on:

ALERTS (0)

Then unchecking:

Active

Show Only Active

From here we can see the alerts from the past 3 months.

Severity	Target/Message	State	Created On	Last Updated	Integration Type
●	Microsoft Exchange on Ottawa Office <i>Critical issue on Exchange Online</i>	Closed	Apr 2, 2023 7:45 PM	Apr 2, 2023 7:50 PM	Vantage DX Monitoring
●	Microsoft Exchange on London Office <i>Critical issue on Exchange Online</i>	Closed	Mar 29, 2023 6:10 PM	Mar 29, 2023 6:20 PM	Vantage DX Monitoring
●	Microsoft Exchange on Nice Office <i>Critical issue on Exchange Online</i>	Closed	Mar 29, 2023 6:10 PM	Mar 29, 2023 6:20 PM	Vantage DX Monitoring
●	Microsoft Exchange on Paris Office <i>Performance issue on Exchange Online</i>	Closed	Mar 29, 2023 5:55 PM	Mar 29, 2023 6:15 PM	Vantage DX Monitoring
●	Microsoft Exchange on Nice Office <i>Performance issue on Exchange Online</i>	Closed	Mar 29, 2023 5:40 PM	Mar 29, 2023 6:05 PM	Vantage DX Monitoring

Let's look at a "Critical" alert for the Ottawa location.

Details

VDX Monitoring

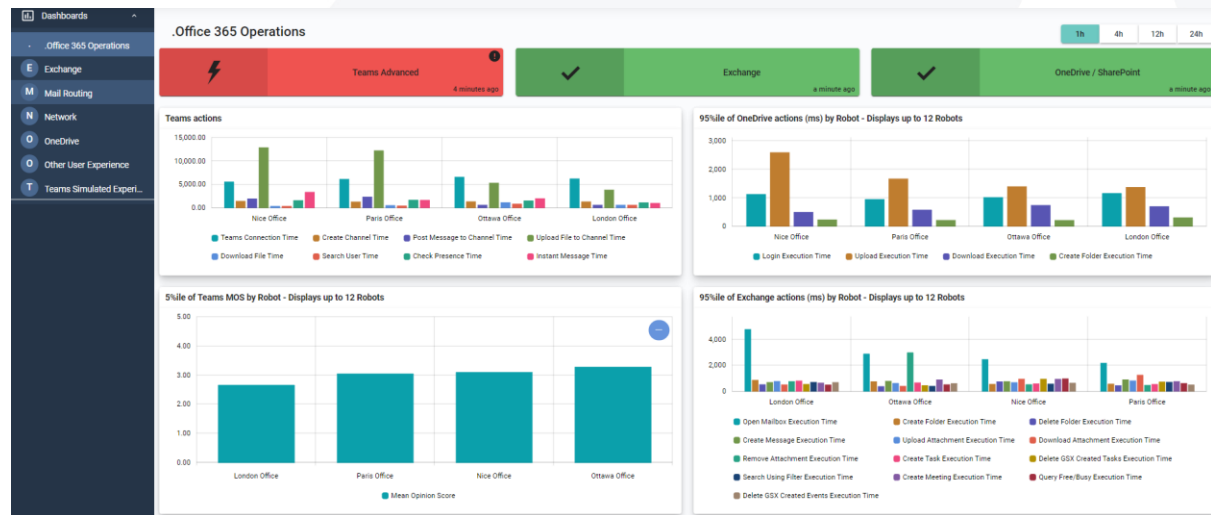
Message

Critical issue
On Ottawa Office / Configuration 'Exchange Online'
- Create Message Execution Time is above the threshold 6000 ms
- Search Using Filter Execution Time is above the threshold 6000 ms

On the right, you will see the detail of this alert. This detail is telling tell us that users in that location had several issues with messages.

If you want to have more information about these tests and alerts, we can switch to the detailed

view by clicking on the blue  icon on the bottom left.



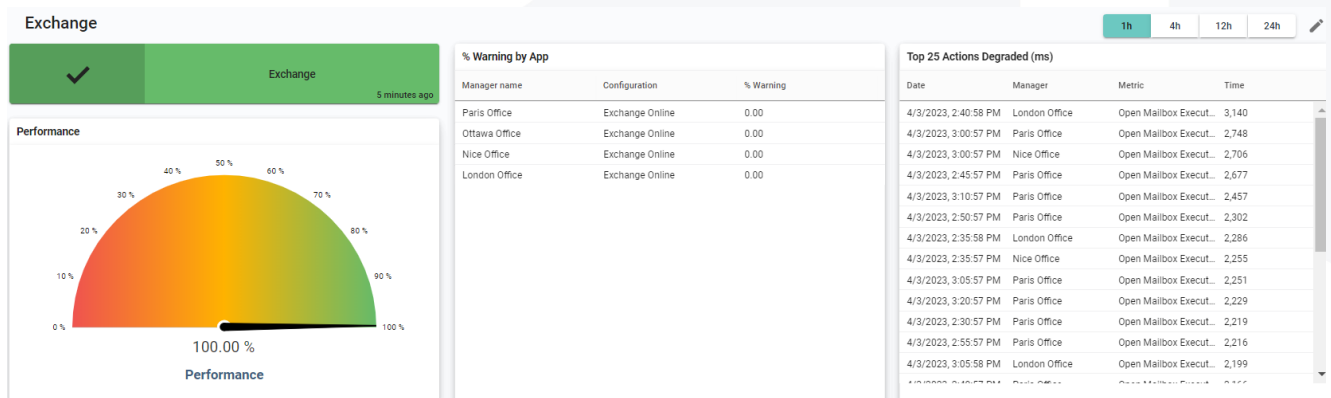
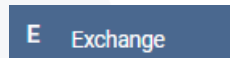
You are now on the main page that provides addition detail on the main workloads and feature tests that were made.

These synthetic transactions are performed by what we call robots that are installed all of your critical locations. At the end, they are just windows services that you can deploy on any windows machine, and they act as a user. They use the exact same protocol and embedded thick client to perform availability and performance tests for every critical feature of Microsoft 365.

We always recommend putting these robots on machines that are powered on and this way you can deliver 24/7 monitoring data and alerts for that location. Outages can happen during off hours and the only way to detect them and anticipate any business productivity issues is to continuously test the Microsoft services.

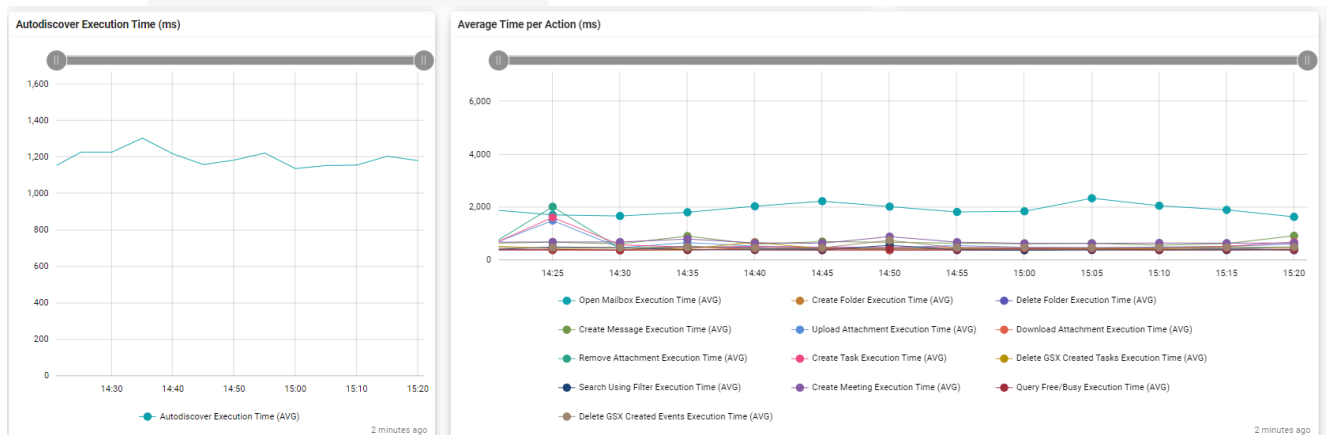
The goal is to have a service baseline so you can understand what is normal and what is not. This then helps you be able to detect local, regional, or global outages quickly to improve your response time to an incident and ensure a better service to your business lines.

To focus solely on Exchange, just select the Exchange tab on the left:



The first line of charts here shows the current availability and performance as well as the recent issues that have been detected through our tests.

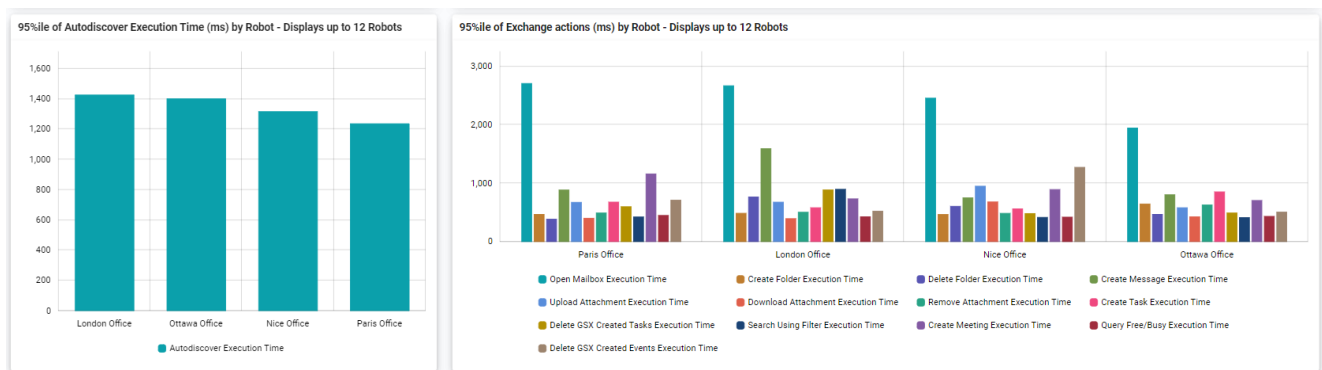
On the top right you can change the time period if needed.



The second line of graphs gives an average view of the Exchange environment for your company. You can see right away the list of tests we are doing:

- Autodiscover execution time
- All the other actions the robot is doing on a mailbox (open mailbox, create folder download attachment, etc.)

These tests reproduce exactly what a user would be doing when using their Outlook client or Outlook Web Access. This test also tells you in real time from your critical location the availability and the performance of these features. If a Microsoft outage is happening, you will be alerted immediately as all the robots will fail at the same time.



Below this, you can compare the results of the tests, location per location to determine if a specific location is underperforming in comparison to the others.

It is important to note that these tests can be done on both Exchange online and Exchange on premise. We also have tests that will cover the specifics of Exchange on premise that are not shown in this demo environment. If you want more information about that, we can discuss it during a technical call.

This means that Martello Vantage DX can monitor the Exchange service delivered through online, hybrid AND an on premises deployment.

Now, being able to use the Exchange features is key, but it is also critical to know that the Exchange Mail routing is healthy.

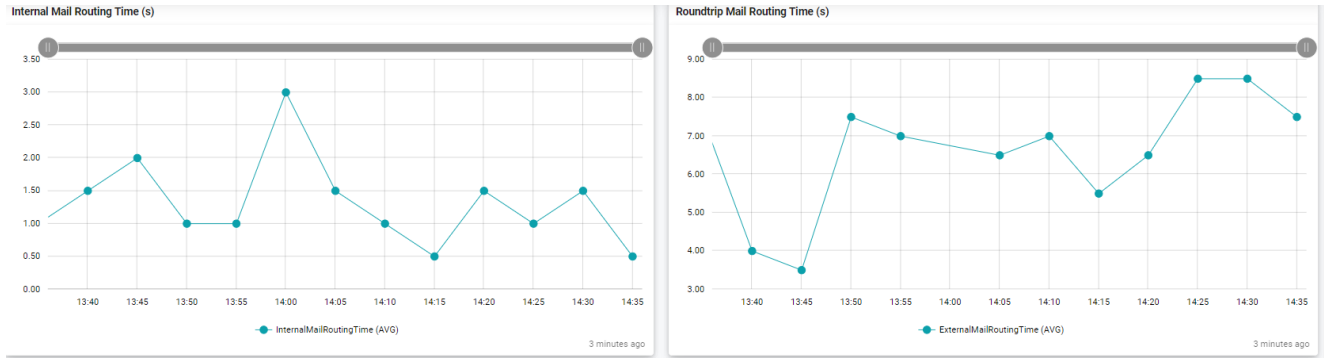
Let's click on the mail routing tab on the left M Mail Routing.

You are now in the Mail routing test results page.

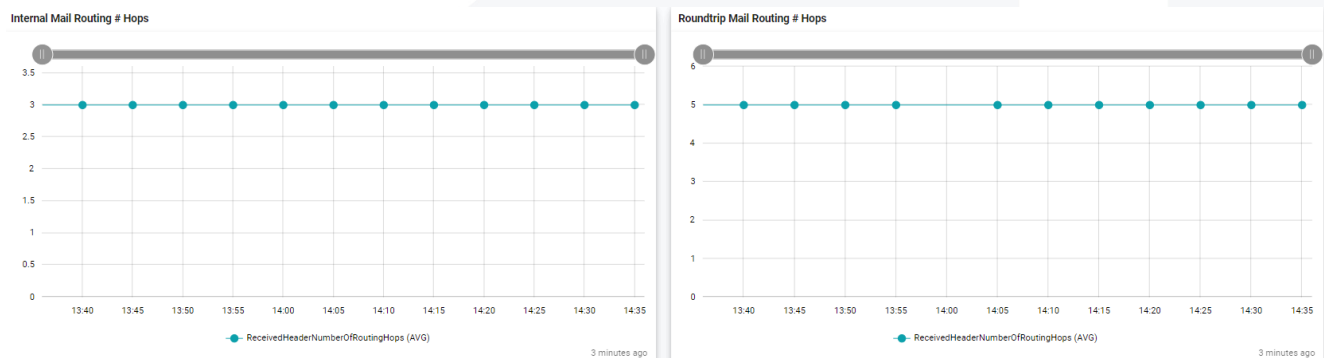
Mail routing can be tested both internally and round trip.

The internal test has the robot sending a real email from one of your mailbox accounts to another one.

The round trip test sends the email to an echo service that sends the email back. This allows us to make sure that your users are able to send and receive emails to and from outside the organization.



The first line of chart shows the performance of the Mail routing in real time.



The second line of chart shows the monitoring for of the number of hops for the Mail - from start to finish.

This detects changes in the mail path that can degrade the performance of the service.

Internal Mail Routing Hops details (slowest)

Hop	Submitting Host	Receiving Host	Time	Delay	Type
1	BYAPR05MB5238.namprd05.prod.outlook.com...	BYAPR05MB5238.namprd05.prod.outlook.com...	4/19/2023, 1:42:40 PM	0 seconds	mail id 15.20.6319.022
2	BYAPR05MB5238.namprd05.prod.outlook.com...	PH0PR05MB10062.namprd05.prod.outlook.co...	4/19/2023, 1:42:41 PM	1 second	Microsoft SMTP Server (version=TLS1_2, ciphe...
3	PH0PR05MB10062.namprd05.prod.outlook.co...	BYAPR05MB5238.namprd05.prod.outlook.com	4/19/2023, 1:42:44 PM	3 seconds	HTTPS

Roundtrip Mail Routing Hops details (slowest)

Hop	Submitting Host	Receiving Host	Time	Delay	Type
1	Debian-exim	localhost	4/19/2023, 2:22:44 PM	0 seconds	local (Exim 4.90_1) id 1pp6pg-0002dLV8 for vd...
2	localhost (51.124.8.220)	BN7NAM10FT019.mail.protection.outlook.com...	4/19/2023, 2:22:45 PM	1 second	Microsoft SMTP Server (version=TLS1_2, ciphe...
3	BN7NAM10FT019.eop-nam10.prod.protection...	BN9PR03CA0758.outlook.office365.com (2603...	4/19/2023, 2:22:47 PM	2 seconds	Microsoft SMTP Server (version=TLS1_2, ciphe...
4	BN9PR03CA0758.namprd03.prod.outlook.com...	BN7PR05MB5698.namprd05.prod.outlook.com...	4/19/2023, 2:22:47 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, ciphe...
5	BN7PR05MB5698.namprd05.prod.outlook.com...	BYAPR05MB5238.namprd05.prod.outlook.com	4/19/2023, 2:22:56 PM	9 seconds	HTTPS

For every report, you can choose precisely what data will affect the SLA performance and what additional data should be displayed to explain potential loss of service quality.

Here is what we can see here:

- The name of the service that you defined.
- The type of data used either for the SLA achievement or for troubleshooting (End-User, Application, Infrastructure).
- The number of alerts for this business service over time.
- The Incident synchronization with your ITSM tool (for example ServiceNow) that correlates alerts into service incidents that are then synchronized with that tool.
- And finally, the SLA achievement overtime.

For this use case we will focus on the Exchange business services we have created.


Let's explore it by clicking on it.




Here you see the result of the SLA for the current time period. Every red dot on the right diagram shows when a breach in the SLA occurred. By clicking on each of them you can then get detailed information below that shows the reason for the breach.

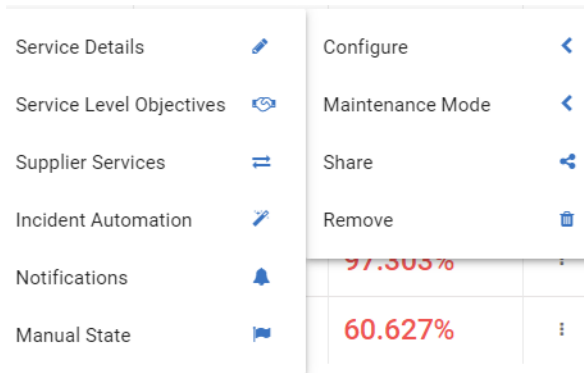
You'll see which robot at which location and at what time the issue was experienced.

Here you can schedule a report that can be sent to both your business lines and management.

Let's click  until we come back to the Business Services Overview.

As you are read only you won't be able to do what I am about to show, but let's check anyway how you can customize the performance report and the SLA you want to track.

If I click on the 3 dots at the right end of our Business Service section: 99.593%  and then select "Configure"



Service Details opens a pop up where you can choose what data type is taken in account to calculate the SLA (End user, Application, Infrastructure).

Service Level Objectives defines the target level of performance.

Incident Automation lets you to synchronize the status of the business services with your ITSM tool.

Notifications lets you to choose how and when to be alerted when your business service is failing.

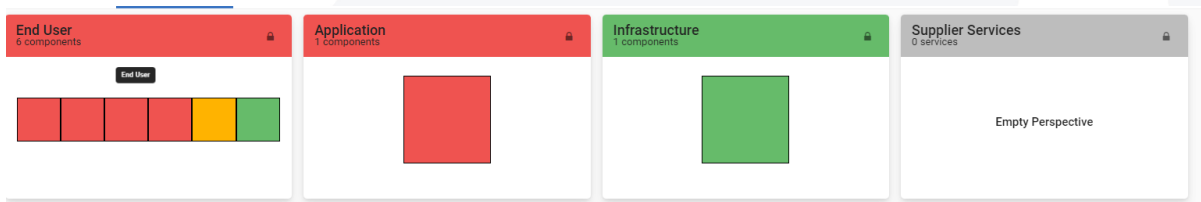
As you can see, Vantage DX provides several ways to group your users, define service quality targets, and then be alerted when Exchange has issues.

Let's come back to the Business Services (click on Exchange).

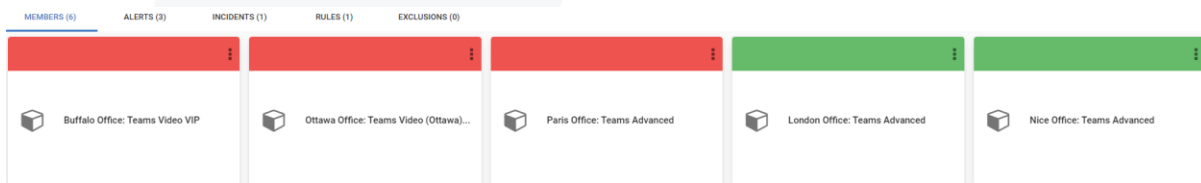
This SLA is based on the availability and performance of our robots testing the Exchange features from our main locations.

To see the data sources used in this SLA we can click on **MEMBERS (4)**

Then you see the data sources organized in 4 bricks:



This SLA has been configured to be calculated upon the data in the End User brick. The End User data is produced by our robots, acting as users from multiple locations, which test all the features of Exchange as we saw in the first part of this demo.



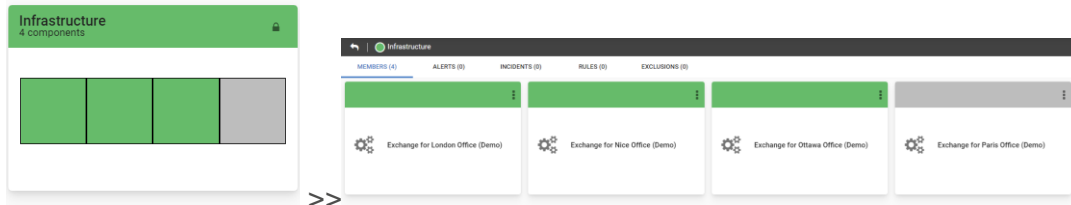
We see here that 3 robots are failing. If you want a summary of what happened for each robot you can click on it. And if you want to see the exact alert for these robots you can then click on

the **ALERTS (3)** tab. You can click on any of them to have the details for every alert.

To come back on the data sources for that SLA click  until you reach the member part.

In the application part, we have put the Microsoft service health. It doesn't impact the SLA but provides interesting complementary information especially if there is an issue.

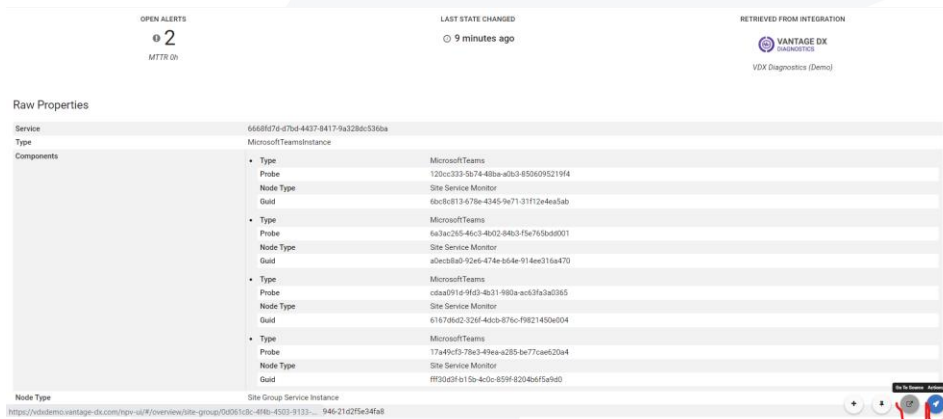
Click  to come back to the member page again. Now we will see the Infrastructure section.



If you click on Infrastructure you will reach the summary of the Martello Vantage DX Diagnostic probes running from our main locations and checking the network performance in between the locations and the Microsoft Exchange online services. This allows you to pinpoint exactly where the latency is introduced and who owns that issue. This is a very good way to quickly understand where the outage comes from and to qualify any third-party problems.

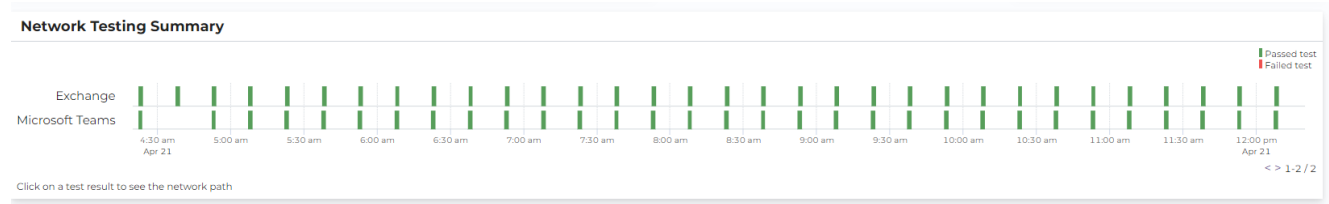
It is now the good time to introduce you to our Network Path monitoring feature.

For that, click on any of the tests (Nice) and then click on the blue rocket on the bottom right and then on the "Go to Source" button.

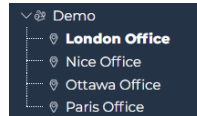


It will open the specific UI to manage and get more details on Martello Vantage DX Diagnostic's.

You'll arrive on this page:



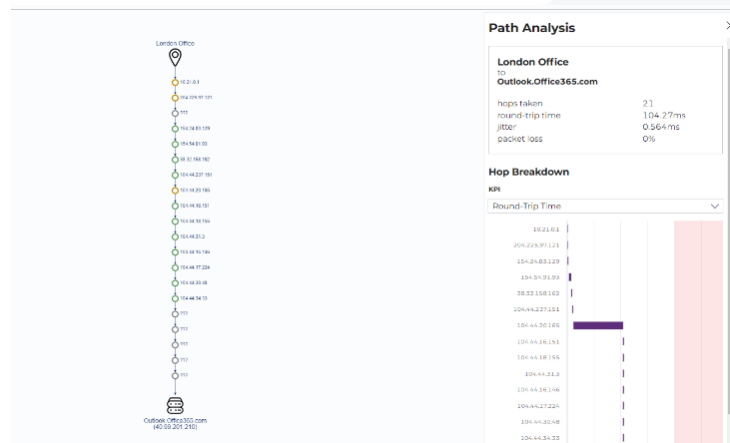
The middle part shows the details of the network tests that are done from the multiple locations



for Exchange and Teams. You can find them on the left:

Red line means a problem has been detected, and green is good. It seems that for Exchange, everything is good for now!

Let's click on any green bar for the location you have selected. We will arrive here:



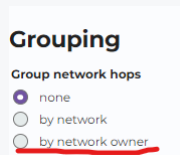
The diagram on the left represents each hop the data is going through to get to the Microsoft Exchange server.

We see that some hops are not performing as well as the others, but they aren't poor enough to represent an issue and trigger an alert.

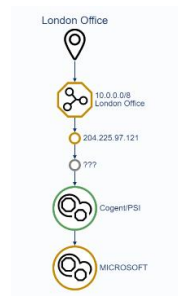
On the right side you have the summary and the details of the latency that has been found.

You can click on Hop Breakdown / Round trip time to switch to other network data such as packet loss and jitter.

Now let's check who owns each hop to quickly determine who is responsible when there is a problem.




On the left side, click on by network owner. Automatically, the hop owner is shown.



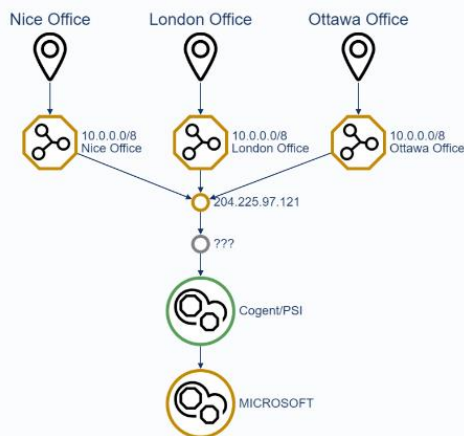
In this example we see that the worst performing hops are in the office itself and at Microsoft.

In seconds, we have been able to identify if they are network issues, and if yes, how bad they are and who is responsible for them.

If you click now on  **Auto-select sites with results**

on the left side, you will see the diagram for all the tests that are made for each critical location you can close the right panel for better visibility.

Path Analysis



From there you can get a further explanation of the tool testing for VIPs or users with recurring issue in our video: [**Proactively Support and Troubleshoot your Teams VIP Issues**](#)

Vantage DX Diagnostic is typically used to continuously monitor the performance of the route to the cloud from the critical locations you have. This allows you to automatically detect any latency, identify who owns it and then to speed up service remediation to prevent a business line productivity impact.

You can also configure the probe to not only check Microsoft Exchange but also any end point you want such as any Microsoft Workload, PowerApps, Azure, ISP or any internal devices.

This tool is also used to detect third party issues. If your security provider, or any other services are having a network issue, you will be able to detect it and be alerted so that you can stay proactive on the management of the quality of service. Feel free to explore the tool, the different tests, and results provided in this trial environment.

Conclusion

Thank you for watching this video. We have seen that Martello Vantage DX can monitor the Microsoft Exchange services delivered to your users in any location you want by testing the workload features, the mail routing performance, and the network quality. It provides early detection of any outage or service issue that would affect your users, and advanced troubleshooting for any network latency.

With Vantage DX you can define customizable alerts and performance reports that you can then share with your management and business lines. Check out our [other videos](#) about how to manage Teams, SharePoint & OneDrive performance and to see how Vantage DX can monitor the entire Microsoft 365 environment.