

## Tracking Microsoft and your Third Parties' Quality of Service with Martello Vantage DX

### The Challenge

Ensuring 24/7 service quality for Microsoft 365 and Microsoft Teams is challenging. IT teams should be able to track the availability and performance of Microsoft Services as well as the service providers playing a role in the service delivery. Unfortunately, Microsoft does not provide any way to achieve this goal

### Overview

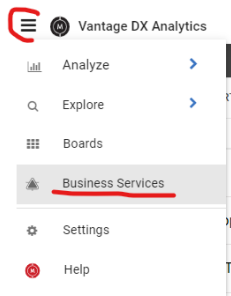
Discover how you can track and report on the service quality delivered by Microsoft Teams and Microsoft 365 applications and how you can detect third party outages that directly affect your employee productivity.

### Let's Get Started!

Let's start by measuring and reporting on an SLA for the Microsoft services that you provide to your business lines or that Microsoft provides out of its data center.

For that we will check our business service feature.

Click on the Burger then Business service.



This brings us to our business service page where you can:

- Create customized SLA reports based on every alert generated by Vantage DX (synthetic transaction, network path monitoring, Teams audio & video performance) as well as import alerts from your existing monitoring tool (Nagios, PRTG, SCOM, etc.).
- Define how the SLA is calculated, what can it impact and what data is used to explain the SLA breaches without impacting it.
- Provide reports to your business lines or upper management.

Ensure at this time that you are on this page.

| 7 Business Services        |  |          |             |                |                   |        |           |          |  |
|----------------------------|--|----------|-------------|----------------|-------------------|--------|-----------|----------|--|
| CREATE GENERATE SLA REPORT |  |          |             |                |                   |        |           |          |  |
| <input type="checkbox"/>   | Name                                       | End-User | Application | Infrastructure | Supplier Services | Alerts | Incidents | SLA      |  |
| <input type="checkbox"/>   | Teams                                      | ⊗        | ⊗           | ⚠              | ⊗                 | 7      | 1         | 60.579%  |  |
| <input type="checkbox"/>   | Teams Rooms (MTRs)                         | ⚠        | ⊗           | ⊗              | ⊗                 | 0      | 0         | 100.000% |  |
| <input type="checkbox"/>   | Teams VIP                                  | ✓        | ⊗           | ⊗              | ⊗                 | 83     | 0         | 99.593%  |  |
| <input type="checkbox"/>   | Teams Service at Offices (Dynamic Offices) | ✓        | ⊗           | ⊗              | ⊗                 | 13     | 0         | 99.048%  |  |
| <input type="checkbox"/>   | Exchange                                   | ✓        | ⊗           | ⊗              | ⊗                 | 4      | 0         | 97.298%  |  |
| <input type="checkbox"/>   | SharePoint OneDrive                        | ✓        | ⊗           | ⊗              | ⊗                 | 1      | 0         | 97.303%  |  |
| <input type="checkbox"/>   | Office 365 Web Apps                        | ⊗        | ⊗           | ⊗              | ⊗                 | 5      | 0         | 60.627%  |  |

This is where you can define and track performance reports for anything in your environment that is used to measure an SLA or internal OLA.

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

Here is what we can see here:

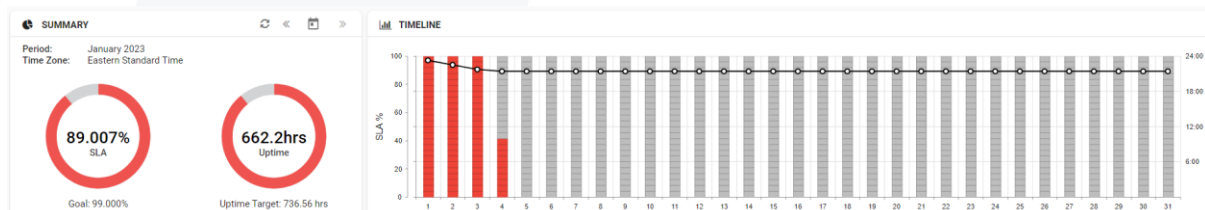
- The name of the service that you define.
- The type of data used either for the SLA achievement or for troubleshooting (End-User, Application, Infrastructure).
- The number of alerts for this business service over time.
- The Incident synchronization with your existing ITSM tools (for example: ServiceNow)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

For this instance, we will focus on two business services we have created. But feel free to explore the other ones as well.

Let's explore the first one: Teams.

If you click on it (click on the word) you will open the rendering and configuration of the SLA.

|                          |                     |   |   |   |   |   |   |         |  |
|--------------------------|---------------------|---|---|---|---|---|---|---------|--|
| <input type="checkbox"/> | Teams               | ⊗ | ⊗ | ⊗ | ⊗ | 8 | 1 | 89.309% |  |
| <input type="checkbox"/> | Office 365 Web Apps | ⊗ | ⊗ | ⊗ | ⊗ | 4 | 0 | 89.309% |  |



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 happened. Clicking on each of them will then show below the reason of the breach.

## Components Impacting SLA (5)

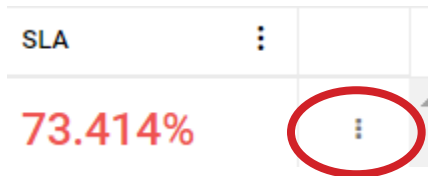
| Impact      | Name                                       | Perspective | SLA Impact Start Time | SLA Impact End Time | Integration Type |
|-------------|--|-------------|-----------------------|---------------------|------------------|
| 2 hr 44 min | Paris Office: Teams Advanced               | End User    | Nov 24, 2022 12:28 AM |                     | Gizmo            |
| 1 hr 0 min  | Buffalo Office: Teams Video VIP            | End User    | Dec 27, 2022 10:21 AM |                     | Gizmo            |
| 1 hr 0 min  | Nice Office: Teams Advanced                | End User    | Dec 1, 2022 11:08 AM  |                     | Gizmo            |
| 1 hr 0 min  | Ottawa Office: Teams Video (Ottawa) - Copy | End User    | Nov 21, 2022 6:12 PM  |                     | Gizmo            |
| 0 hr 28 min | Ottawa Office: Teams Advanced              | End User    | Jan 1, 2023 7:07 PM   | Jan 1, 2023 8:13 PM | Gizmo            |

You can also see which robot breached, t which location and show the time when you experienced the issue.

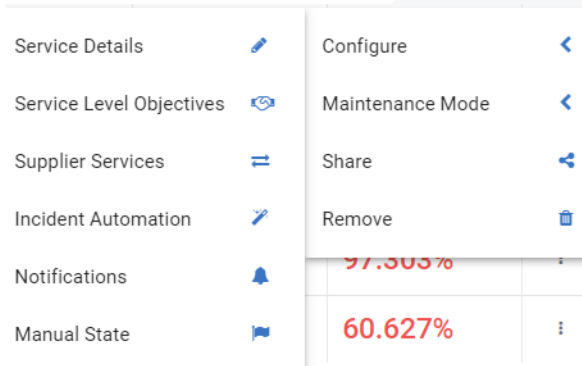
This is also where you can schedule a report that can be sent to your business lines and management.

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

Now clicking on the 3 dots at the right end of our Teams Business Service:



Open the menu for configuration. That only works if you have admin access to the demo environment.



Configure > Service details opens the pop up where you can choose what data type is taken into account to calculate the SLA (End user, Application, Infrastructure).

Service Level Objectives defines the target level of performance.

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

Finally, Notifications enables you to choose how and when to be alerted when your Business Service Teams is failing.

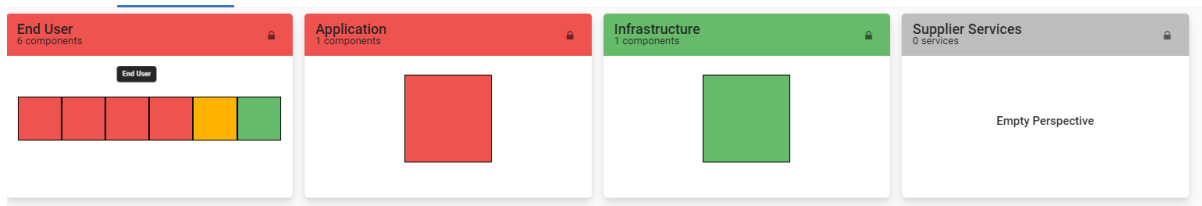
As you can see, Vantage DX provides several ways to group your users, define service quality targets, and be alerted when Microsoft Teams has issues.

Let's come back in this business service (click on Teams).

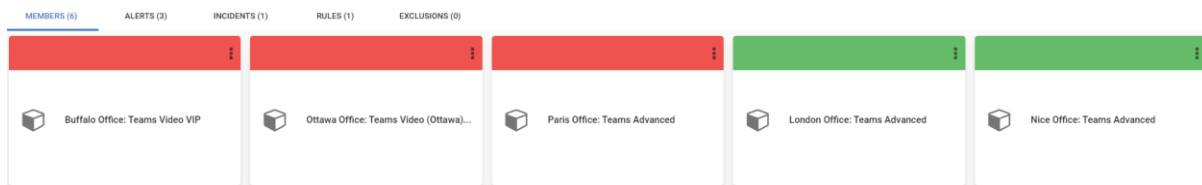
This SLA is based on the availability and performance of our robots testing the Microsoft Teams features from our main location.

To see the data source that is 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. In here that the End User data is produced by our robots, acting as users would use Teams from multiple locations and testing all the features of Teams.

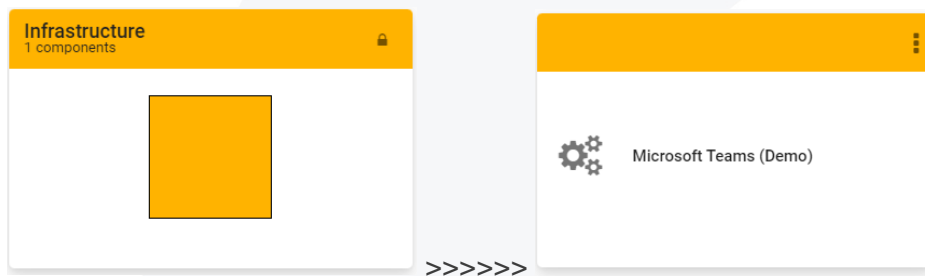


We see here that 3 robots are failing. If you want a summary of what happens for each robot you can click on it. And if you want to see the exact alert for these robots you can then click on the **ALERTS (3)** tab. You can click on any of them to have the details for each of the alerts.

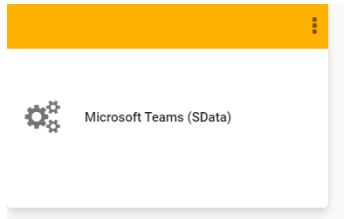
To come back to the data sources for that SLA click  until you reach the member part.

In the application part, we have put the Microsoft Service Health. It doesn't impact the SLA, but it does provide interesting additional information if there is a problem.

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



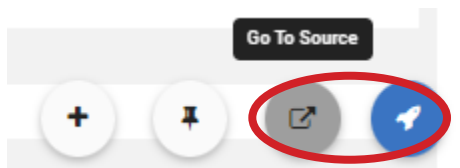
If you click on it, then you will reach the summary of the Martello Vantage Diagnostic probes that are running from multiple locations and checking the network performance in between your locations and the Microsoft Teams cloud services. This allows you to pinpoint where the latency is introduced and who owns that issue. This is a very good way to quickly understand where the outage comes from and qualify if there are any additional third party problems.



Let's click on

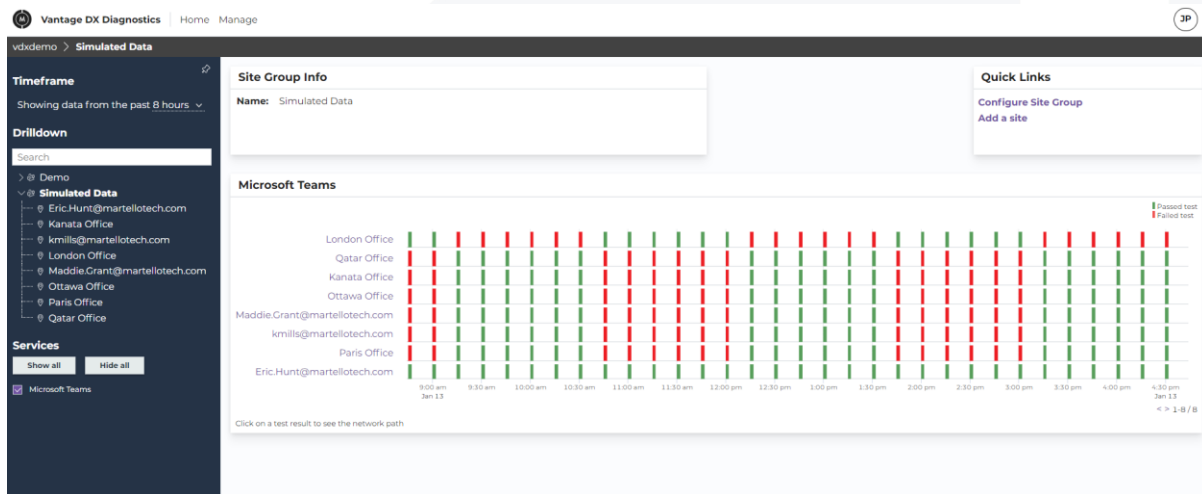
It is now a good time to introduce you to our Network Path Monitoring feature.

For that, click on the blue rocket on the bottom right then Go to Source.



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

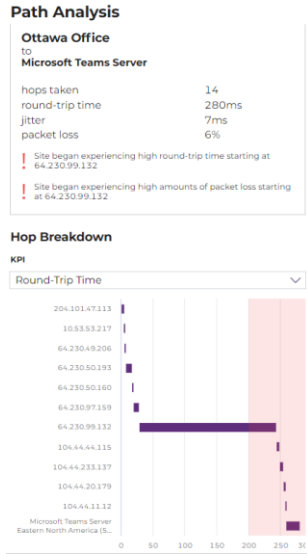
You'll arrive on this page:



The middle section features the Teams the details of the network tests that were performed from multiple locations.

A red line means a problem has been detected, and green is good.

Let's click on any red line for the Ottawa location to dig a little deeper.



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

Clearly we see that hop 64.390.99.132 has an issue.

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 we know this hop has an issue. We want to know who owns it and who is responsible for the issue.

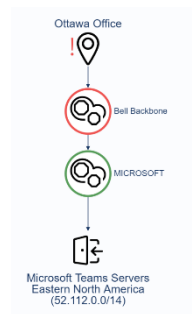
On the left side, click on 'by network owner'. Automatically, the hop owner is shown.

### Grouping

Group network hops

- none
- by network
- by network owner

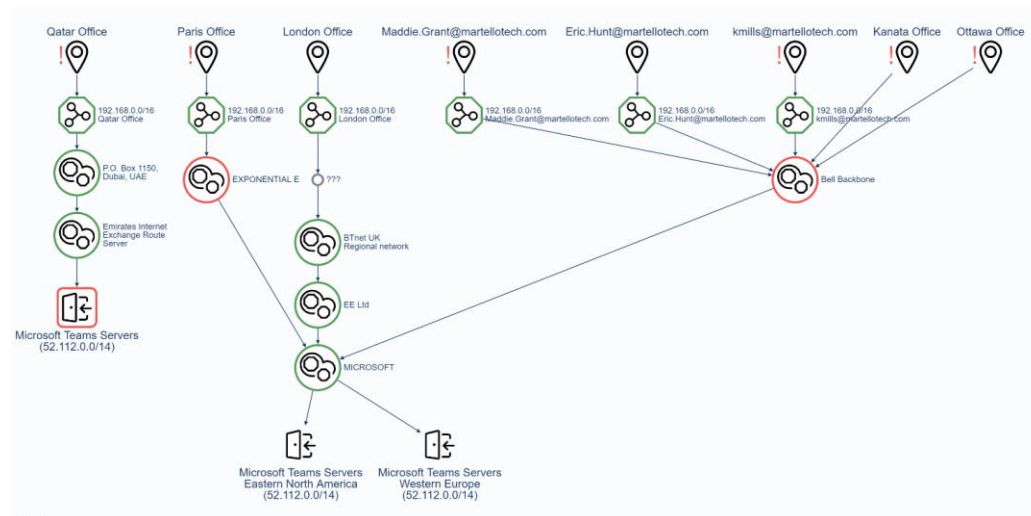
Show network owners



The problem is clearly identified at Bell Canada.

In seconds, we have been able to identify that the network issues for the Ottawa office, which introduce round trip time and packet loss in the route to Microsoft are rooted with the ISP.

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 and for some individuals (close the right panel for better visibility).



You can get more detail on our network testing tool for VIPs or users with recurring issues in our video: Proactively Support and Troubleshoot Microsoft Teams VIP Issues with Martello Vantage DX: <https://youtu.be/T60KR5q9hUU>

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

You can configure the probe to not only check Microsoft Teams but also any end point you want to monitor – for example any Microsoft workload, PowerApps, Azure or any internal devices.

This tool is also used to detect third party issues, as in this case the Bell ISP. If your security provider, or any other services are having network issues, you will be able to detect it and be alerted immediately. This helps you stay proactive on the management of your quality of service.

Feel free to explore the tool and the different tests and results that it provides in this trial environment.

## Conclusion

You have seen how you can easily setup 24/7 monitoring for Microsoft Teams and every other workload of Microsoft 365. You can also create and follow your SLA, choose *what* is impacting the SLA and *how* the additional information helps you better understand the SLA breach.

You have also seen how Vantage DX Diagnostics can track overall network performance between your key locations or users and Microsoft's services and then detect any kind of outage coming from the third-party services that are involved in Teams and Microsoft 365 service delivery.