The Best & Brightest TMA

Technology Newsletter

APPLIED OBSERVABILITY

1 Applied Observability là gì?

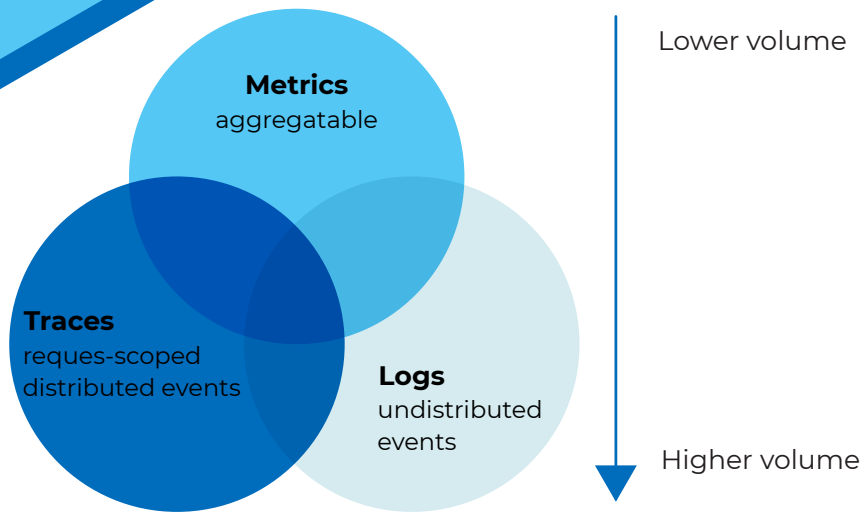
Trong việc quản lý và duy trì hệ thống thông tin ngày nay, khái niệm "Observability" (“Giám sát”) ngày càng trở nên quan trọng. Observability có thể hiểu đơn giản là khả năng giám sát và hiểu rõ hệ thống thông tin cũng như ứng phó với các vấn đề về hệ thống một cách hiệu quả trong khi nó hoạt động nhằm giữ cho hệ thống hoạt động hiệu quả, đáng tin cậy và hài lòng bởi người dùng cuối.

Observability khác với Monitoring (“Theo dõi”) ở chỗ không chỉ đơn thuần thu thập dữ liệu tập trung vào các chỉ số của hệ thống như CPU, bộ nhớ và số lượng yêu cầu vào hệ thống để đảm bảo chúng đang hoạt động như mong đợi mà còn đặt ra các câu hỏi tại sao và làm thế nào mọi thứ diễn ra như vậy. Dữ liệu có thể giám sát là dữ liệu do chính các hệ thống tạo ra, chẳng hạn như nhật ký, số liệu, dấu vết, sự kiện, v.v. Bằng cách phân tích dữ liệu này, tổ chức có thể hiểu rõ hơn về cách hệ thống hoạt động như trạng thái, hiệu năng và hành vi của nó, những vấn đề nào đang ảnh hưởng đến nó và những hành động mà tổ chức có thể thực hiện để cải thiện nó.

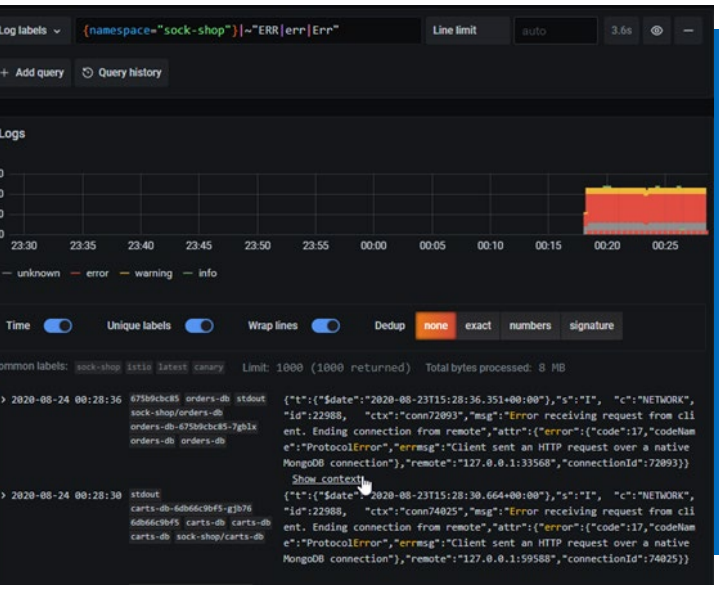
“Applied Observability” (“Giám sát có tính ứng dụng”) không phải là một công nghệ đơn lẻ mà là một cách tiếp cận tích hợp và đa chức năng trải rộng trên nhiều lớp kiến trúc CNTT của tổ chức. Trong các hệ thống hiện đại sử dụng điện toán đa đám mây, mọi thành phần phần cứng, phần mềm và cơ sở hạ tầng đám mây cũng như các container, công cụ mã nguồn mở, mircoservice đều tạo ra các dữ liệu hoạt động, do đó nó đòi hỏi các công cụ và kỹ thuật có thể kết nối, tối ưu hóa và nâng cao dữ liệu giám sát được. Applied Observability có thể giúp ta thực hiện các nhiệm vụ như khám phá, quản lý tài nguyên đám mây, tuân thủ SLA (Service Level Agreement – thỏa thuận cấp độ dịch vụ), độ tin cậy của hệ thống, an ninh mạng và quản lý sự cố.

2 Các thành phần chính

Ba thành phần chính cho việc giám sát là: nhật ký (logs), số liệu (metrics) và dấu vết (traces):

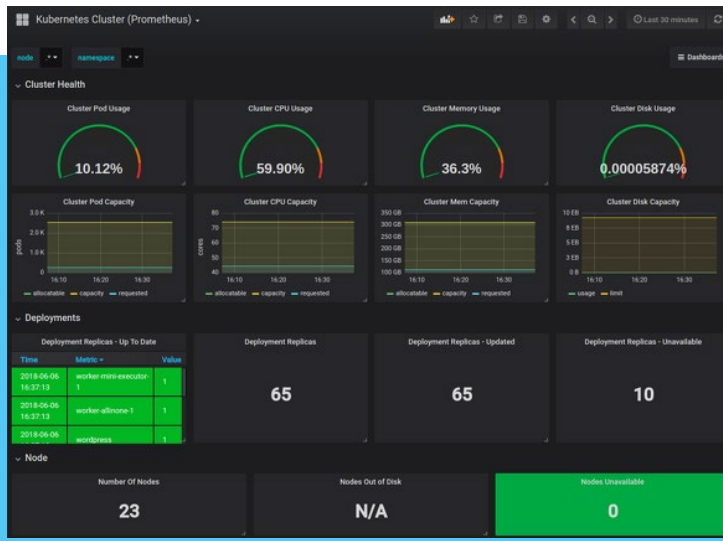


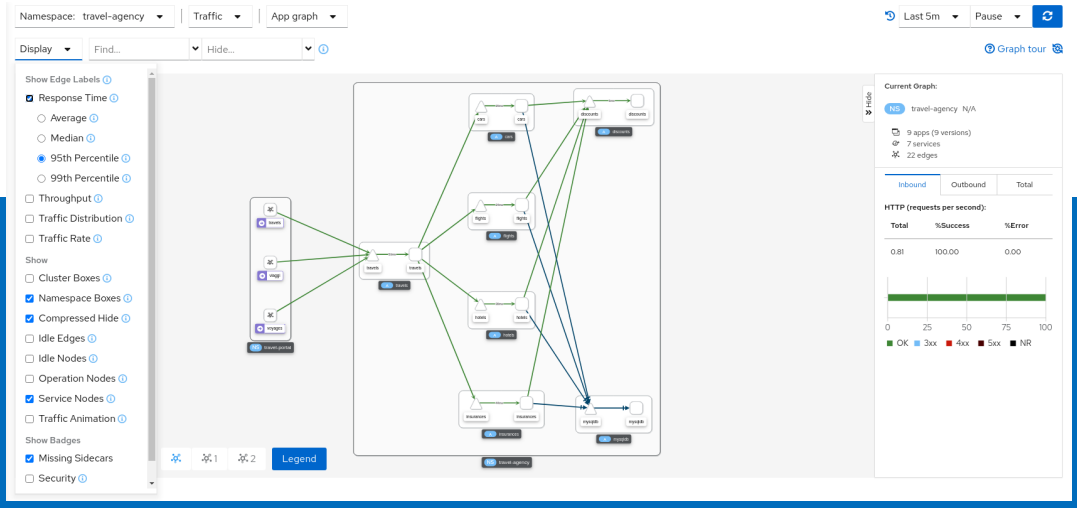
PRIMARY SIGNALS



Nhật ký: là bản ghi (record) các sự kiện, thường ở dạng văn bản hoặc dạng con người có thể đọc được, có cấu trúc (structured) hoặc không có cấu trúc (unstructured). Chúng có thể được tạo ra bởi các thành phần của cơ sở hạ tầng bao gồm các thiết bị mạng và máy chủ, hệ điều hành và các phần mềm ứng dụng. Một số ứng dụng sẽ ghi lại những gì mà nhà phát triển cho là thông tin quan trọng. Nhật ký thường có thông tin về thời gian xảy ra và thường được sử dụng để thiết lập bối cảnh trong quản lý hoạt động.

Số liệu: là loại dữ liệu được biểu thị dưới dạng số lượng hoặc thước đo có được bằng việc tính toán hay tổng hợp theo thời gian thực trong một khoảng thời gian xác định. Số liệu có thể bắt nguồn từ nhiều nguồn khác nhau, bao gồm cơ sở hạ tầng, máy chủ, dịch vụ, nền tảng đám mây và các nguồn bên ngoài.

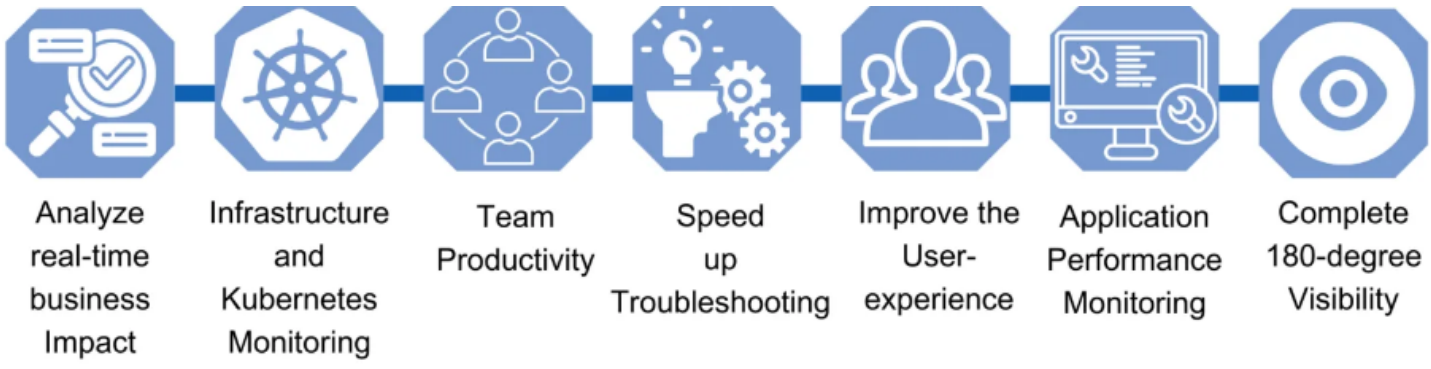




Dấu vết: là các bản ghi về luồng dữ liệu hoặc quy trình làm việc được thiết kế cho một đơn vị công việc, chẳng hạn như một giao dịch hay một yêu cầu xử lý, đi qua nhiều thành phần của hệ thống có sự phụ thuộc, liên quan với nhau. Để có thể trực quan hóa các luồng dữ liệu trên nhiều thành phần hệ thống cần phải kết hợp các công cụ theo dõi khi phát triển phần mềm ứng dụng. Việc này trở nên cần thiết trong các hệ thống sử dụng kiến trúc microservice nơi mà các thành phần hệ thống tương tác với nhau thường xuyên.

Cả ba thành phần đều quan trọng đối với việc giám sát, nhưng mỗi thành phần đều có hạn chế riêng. Với số liệu thì khó gắn thẻ và sắp xếp chúng cũng như khó sử dụng chúng để khắc phục sự cố; với nhật ký thì có thể gặp khó khăn trong việc sắp xếp và tổng hợp để đưa ra kết luận hoặc mối quan hệ có ý nghĩa; còn dấu vết có thể tạo ra lượng lớn dữ liệu không cần thiết. Do đó, những người thực hiện việc giám sát vẫn có thể gặp phải các khó khăn trong việc thu thập thông tin chi tiết thực sự, cảm thấy có quá nhiều nơi để tìm kiếm nguyên nhân vấn đề hoặc đi sâu vào việc chuyển vấn đề thành vấn đề có thể xử lý được.

3 Lợi ích



Applied Observability giúp người quản trị hiểu rõ hệ thống qua việc cung cấp cái nhìn sâu sắc và toàn diện về hoạt động của hệ thống trên tất cả các khía cạnh, từ đó, giúp nhanh chóng xác định và giải quyết các vấn đề hệ thống, từ lỗi đơn giản đến các vấn đề phức tạp, qua đó nâng cao hiệu suất làm việc của đội nhóm thực hiện việc giám sát, cũng như tối ưu hóa nguồn lực và cải thiện trải nghiệm người dùng.

Hạ tầng điện toán đám mây được sử dụng trong các hệ thống hiện đại mang lại nhiều lợi ích như khả năng mở rộng, tính linh hoạt và nhanh chóng, nhưng nó cũng đi kèm với những thách thức như độ phức tạp, chi phí và bảo mật. Applied Observability có thể giúp vượt qua những thách thức này bằng cách cung cấp khả năng hiển thị và kiểm soát tài nguyên đám mây như:

- Khám phá và kiểm kê tài sản, dịch vụ đám mây của tổ chức trên các nhà cung cấp và khu vực khác nhau.
- Theo dõi và tối ưu hóa việc sử dụng và chi phí trên các dịch vụ đám mây.
- Xác định và giải quyết các vấn đề về hiệu năng cũng như các điểm nghẽn trong dịch vụ đám mây.
- Tự động hóa và sắp xếp các hoạt động và quy trình làm việc trên đám mây.
- Đảm bảo tuân thủ các chính sách và quy định trong môi trường đám mây.

Về các ứng dụng sử dụng trong hệ thống thông tin của tổ chức, Appied Observability giúp giám sát toàn diện cho phép người quản trị tìm hiểu tận gốc các vấn đề về hiệu năng của ứng dụng nhanh hơn nhiều, gồm cả các vấn đề phát sinh từ môi trường microservice và các dịch vụ đám mây.

Về bảo mật hệ thống, Applied Observability cho phép người quản trị phát hiện và ngăn chặn các cuộc tấn công mạng vào hệ thống của tổ chức. An ninh mạng là mối quan tâm hàng đầu đối với bất kỳ hệ thống nào, đặc biệt là trong kỷ nguyên kỹ thuật số nơi các mối đe dọa ngày càng tinh vi và thường xuyên hơn. Nó có thể giúp bạn nâng cao tình trạng an ninh mạng bằng cách cung cấp cho bạn nhận thức và khả năng bảo vệ trước các rủi ro trên mạng.

- Giám sát và phân tích hành vi và hoạt động của người dùng hệ thống, thiết bị, mạng, ứng dụng và dữ liệu của tổ chức.
- Xác định các điểm bất thường, lỗ hổng và mối đe dọa trong hệ thống của tổ chức bằng cách sử dụng phân tích nâng cao và học máy.
- Ứng phó với sự cố nhanh chóng và hiệu quả bằng cách sử dụng tự động hóa và điều phối.
- Ngăn chặn các cuộc tấn công trong tương lai bằng cách áp dụng các bản vá, bản cập nhật, chính sách và các phương pháp hay nhất.

Trải nghiệm người dùng tốt có thể làm tăng danh tiếng của tổ chức và tăng doanh thu, mang lại lợi thế cạnh tranh. Applied Observability cho phép phát hiện và giải quyết tốt các vấn đề trước khi người dùng cuối phản hồi và thực hiện cải tiến trước khi được yêu cầu, tổ chức có thể tăng cường sự hài lòng và giữ chân khách hàng. Nó cũng có thể tối ưu hóa trải nghiệm người dùng thông qua tính năng phát lại trong thời gian thực, với một giao diện cho phép trải nghiệm lại như người dùng cuối, từ đó có thể nhanh chóng xác định những điểm cần cải thiện về trải nghiệm người dùng. Đo lường và cải thiện hiệu năng, tính khả dụng, độ tin cậy và chất lượng của hệ thống là những yếu tố quan trọng đối với bất kỳ hệ thống của tổ chức nào muốn mang lại giá trị gia tăng cho khách hàng và các bên liên quan. Applied Observability giúp tổ chức đạt được sự tuân thủ SLA (thỏa thuận cấp độ dịch vụ) bằng cách cung cấp cho tổ chức các số liệu và chỉ báo phản ánh mức độ đáp ứng hoặc vượt mục tiêu của hệ thống qua việc:

- Xác định và giám sát SLA và SLO (Service Level Objective – mục tiêu cấp độ dịch vụ) cho các thành phần và chức năng hệ thống của tổ chức.
- Thu thập và báo cáo SLI (Service Level Indicator – chỉ báo cấp độ dịch vụ) của tổ chức như độ trễ, băng thông, tỷ lệ lỗi, tính khả dụng, v.v.
- Phân tích và tối ưu hóa hiệu suất cũng như chất lượng hệ thống của tổ chức bằng cách sử dụng phân tích nguyên nhân, thử nghiệm tổng hợp, thử nghiệm tải...
- Truyền đạt và chứng minh sự tuân thủ SLA cũng như giá trị của tổ chức mang lại cho khách hàng và các bên liên quan bằng cách sử dụng bảng biểu, báo cáo...

4 Thách thức

Dữ liệu lớn và đa dạng: Với sự phát triển nhanh chóng của hệ thống và ứng dụng, lượng dữ liệu thu thập từ các nhật ký, số liệu và dấu vết có thể tăng rất nhanh và trở nên rất lớn và đa dạng, đặt ra thách thức về lưu trữ và xử lý dữ liệu.

Phức tạp trong triển khai: Việc triển khai Applied Observability đầy đủ và hiệu quả có thể phức tạp và đòi hỏi chuyên môn cao.

Chi phí: Một hệ thống Applied Observability mạnh mẽ thường đi kèm với chi phí, từ việc lưu trữ dữ liệu đến việc sử dụng các công cụ và dịch vụ chuyên nghiệp.

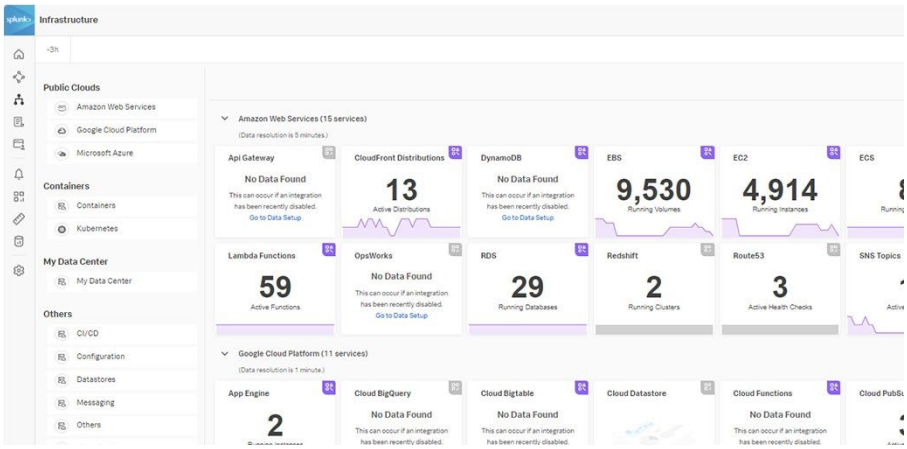
Triển khai và cấu hình thủ công: Trong một số trường hợp mà nguồn lực CNTT được dành để triển khai các công cụ và cấu hình theo cách thủ công, khi có một thành phần hệ thống mới, họ dành phần lớn thời gian để cố gắng thiết lập khả năng giám sát cho nó thay vì dành cho việc tìm cách làm mới, sáng tạo dựa trên những hiểu biết sâu sắc từ dữ liệu giám sát được.

Cần kết hợp nhiều công cụ khác nhau: Mặc dù một công cụ duy nhất có thể cung cấp cho tổ chức khả năng giám sát một khu vực nào đó trong hệ thống nhưng một công cụ đó có thể không cung cấp khả năng quan sát đầy đủ và hoàn chỉnh trên tất cả các ứng dụng và toàn hệ thống.

5

Một số công cụ hỗ trợ

Splunk



Splunk là một nền tảng có khả năng mở rộng cung cấp khả năng giám sát toàn diện và bảo mật thống nhất. Splunk hỗ trợ Splunkbase với hơn 3.000 ứng dụng và tiện ích bổ sung; và có thể thu thập dữ liệu đo từ xa trên các môi trường khác nhau như đa đám mây (multi-cloud), đám mây lai (hybrid cloud) và đám mây biên (edge cloud). Nền tảng này bao gồm khả năng tự động hóa tích hợp và khả năng điều phối được hỗ trợ bởi AI. Nó cũng bao gồm khả năng phân tích luồng dữ liệu trực tiếp giúp cung cấp những hiểu biết sâu sắc về hệ thống trong thời gian gần như thực và hỗ trợ ứng phó sự cố nhanh chóng.

Nền tảng Splunk có thể được cung cấp dưới dạng một dịch vụ đám mây, Splunk Cloud Platform hay tải về và cài đặt trong nội bộ tổ chức, Splunk Enterprise.

Splunk có thể giám sát cơ sở hạ tầng, ứng dụng, mạng, microservice và nền tảng của bên thứ ba. Splunk sử dụng kết hợp các tác nhân (agent), người chuyển tiếp (forwarders), lập chỉ mục và tìm kiếm để thu thập dữ liệu từ các thành phần được giám sát, chuyển đổi dữ liệu thành các sự kiện được lập chỉ mục và cung cấp dữ liệu cho người dùng.

Grafana

Grafana cung cấp một nền tảng tập trung để tìm hiểu và trực quan hóa các số liệu, nhật ký và dấu vết. Nền tảng này bao gồm các khả năng cảnh báo và cung cấp các công cụ để chuyển đổi dữ liệu theo thời gian (time-series data) thành các biểu đồ và hình ảnh trực quan. Người dùng có thể tạo các bảng biểu hiển thị dữ liệu đo từ xa từ nhiều nguồn khác nhau như cụm Kubernetes (Kubernetes cluster), dịch vụ đa đám mây, thiết bị Raspberry Pi và các dịch vụ như Google Sheets.

Grafana có thể được cung cấp dưới dạng dịch vụ đám mây, Grafana Cloud. Grafana Enterprise Stack là một nền tảng có thể được triển khai tại nội bộ tổ chức.

Grafana có thể giám sát cơ sở hạ tầng, ứng dụng, nguồn dữ liệu, microservices và nền tảng của bên thứ ba. Các tác nhân mã nguồn mở (open source agent) của Grafana chạy trên các thiết bị được giám sát và thu thập số liệu, nhật ký và dấu vết. Sau đó, tác nhân sẽ chuyển tiếp dữ liệu đo từ xa đến nền tảng Grafana, cho dù chạy trên đám mây hay tại nội bộ tổ chức.

Dynatrace

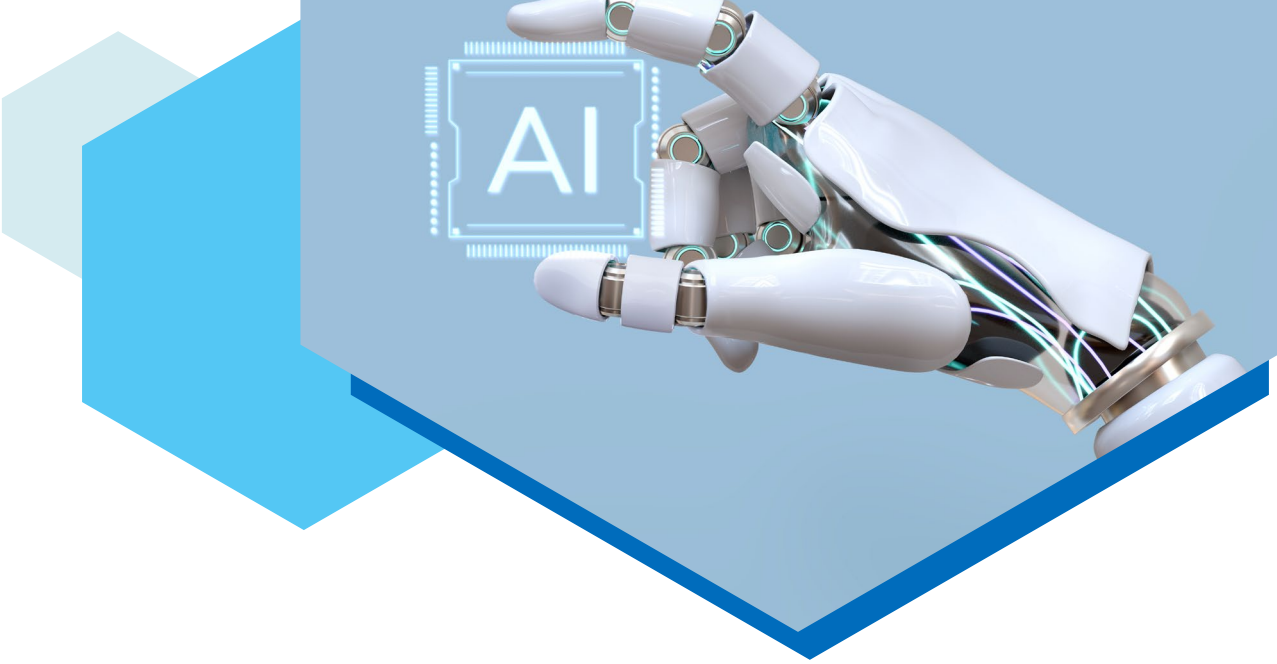
Dynatrace cung cấp nền tảng tích hợp để giám sát cơ sở hạ tầng và ứng dụng, bao gồm mạng, ứng dụng di động và dịch vụ phía máy chủ. Nền tảng này cũng có thể phân tích hiệu suất tương tác của người dùng với các ứng dụng và bao gồm một công cụ AI hỗ trợ phân tích nguyên nhân. Dynatrace hỗ trợ hơn 600 ứng dụng của bên thứ ba được xây dựng trên các tiêu chuẩn mở, từ đó cho phép các tổ chức mở rộng nền tảng Dynatrace bằng cách sử dụng API, SDK hoặc Dynatrace plugin.

Dynatrace thường được cung cấp dưới dạng dịch vụ phần mềm trên đám mây, nhưng cũng có thể được triển khai trong nội bộ tổ chức.

Dynatrace có thể giám sát cơ sở hạ tầng, ứng dụng, microservice và bảo mật ứng dụng, cũng như trải nghiệm người dùng và phân tích nghiệp vụ. Một tác nhân (agent) chạy trên mỗi máy chủ cần giám sát, thu thập dữ liệu hệ thống, ứng dụng, mạng và nhật ký rồi gửi dữ liệu đến nền tảng Dynatrace.

6 Tương lai

Theo Gartner, Applied Observability là một trong 10 xu hướng công nghệ chiến lược hàng đầu trong năm 2023. Họ dự đoán rằng đến năm 2026, 70% tổ chức áp dụng nó sẽ ra quyết định nhanh hơn và đạt được lợi thế cạnh tranh. Applied Observability là điều cần thiết đối với các tổ chức hiện đại muốn đi trước xu hướng và mang giá trị gia tăng cho khách hàng của mình.



Applied Observability sử dụng AI giúp khả năng giám sát thực sự khả thi bằng cách giải quyết các thách thức liên quan đến độ phức tạp của các hệ thống hiện đại, chẳng hạn trên môi trường tính toán nhiều đám mây. Sử dụng AI giúp việc diễn giải luồng dữ liệu khổng lồ thu thập từ xa từ nhiều nguồn với tốc độ ngày càng lớn trở nên dễ dàng hơn. Với một nguồn thông tin chính xác duy nhất, ta có thể xác định nhanh chóng và chính xác nguyên nhân cốt lõi của vấn đề trước khi chúng ảnh hưởng đến hiệu năng của ứng dụng hoặc trong trường hợp đã xảy ra lỗi, đẩy nhanh thời gian khôi phục.

Một cách liên tục tự động phát hiện, triển khai giám sát và baseline cho mọi thành phần hệ thống giúp chuyển nỗ lực CNTT từ công việc cấu hình thủ công sang công việc tìm cách làm mới sáng tạo dựa trên sự hiểu sâu sắc về những dữ liệu mà giám sát được. Nhờ đó, khả năng giám sát trở nên “luôn bật” (“always-on”) và có thể mở rộng, từ đó, các nhóm có thể làm được nhiều hơn với ít nguồn lực hơn.

7 Tham khảo

- What is observability? Not just logs, metrics and traces
- What is "Observability" - Why is it necessary and what are the considerations in cloud-native monitoring? - vol.1
- What is "Observability" - Why is it necessary and what are the considerations in cloud-native monitoring? - vol.2
- Top observability tools for 2024