Kibana

1. Tổng quan

Khái niệm

* Kibana là một nền tảng phân tích hiển thị dữ liệu từ Elasticsearch một cách trực quan dễ sử dụng,Kibana cũng là một công cụ mã nguồn mở miễn phí, cho tất cả mọi người sử dụng.
* Kibana cung cấp các tính năng cho người dùng quản lý như biểu đồ cột, biểu đồ đường, biểu đồ tròn, biểu đồ nhiệt và nhiều loại chart khác nữa.
* Kibana cũng cung cấp một công cụ trình bày, được gọi là Canvas , cho phép người dùng tạo các bản trình chiếu lấy dữ liệu trực tiếp trực tiếp từ Elaticsearch.

1. Các tính năng chính của kibana

* **Khám phá dữ liệu** : Kibana cho phép người dùng khám phá các bộ dữ liệu lớn được lưu trữ trong Elaticsearch bằng nhiều tùy chọn tìm kiếm và lọc. Người dùng có thể thực hiện các truy vấn phức tạp, áp dụng các bộ lọc và đi sâu vào các tập hợp con cụ thể của dữ liệu để khám phá thông tin chi tiết và mẫu.
* **Trực quan hóa** : Kibana cung cấp nhiều tùy chọn trực quan hóa để chuyển đổi dữ liệu thành biểu đồ, đồ thị, bản đồ và bảng có ý nghĩa. Người dùng có thể tạo các hình ảnh trực quan hóa như biểu đồ thanh, biểu đồ đường, biểu đồ hình tròn, bản đồ nhiệt, v.v. để thể hiện dữ liệu của họ ở định dạng trực quan hấp dẫn và dễ hiểu.
* **Tạo bảng điều khiển** : Kibana cho phép người dùng tạo bảng điều khiển tương tác bằng cách kết hợp nhiều hình ảnh trực quan và thêm các yếu tố bổ sung như văn bản, hình ảnh và điều khiển. Trang tổng quan cho phép người dùng tạo chế độ xem toàn diện về dữ liệu của họ, theo dõi các số liệu chính và theo dõi các thay đổi theo thời gian thực.
* **Giám sát thời gian thực** : Kibana hỗ trợ giám sát và truyền dữ liệu thời gian thực. Người dùng có thể thiết lập trực quan hóa và bảng điều khiển để hiển thị cập nhật trực tiếp dữ liệu của họ, cho phép họ theo dõi các số liệu và chỉ số hiệu suất trong thời gian thực.
* **Cộng tác dữ liệu** : Kibana tạo điều kiện cộng tác dữ liệu bằng cách cho phép người dùng lưu, chia sẻ và xuất các hình ảnh trực quan, bảng điều khiển và truy vấn. Người dùng có thể cộng tác với các thành viên trong nhóm bằng cách chia sẻ liên kết hoặc nhúng trực quan hóa vào các ứng dụng hoặc trang web bên ngoài.
* **Cảnh báo và Báo cáo** : Kibana cung cấp khả năng cảnh báo và báo cáo để thông báo cho người dùng về các sự kiện hoặc điều kiện cụ thể trong dữ liệu của họ. Người dùng có thể thiết lập cảnh báo dựa trên các ngưỡng được xác định trước hoặc tiêu chí tùy chỉnh và nhận thông báo qua nhiều kênh khác nhau như tích hợp email, Slack hoặc webhook.

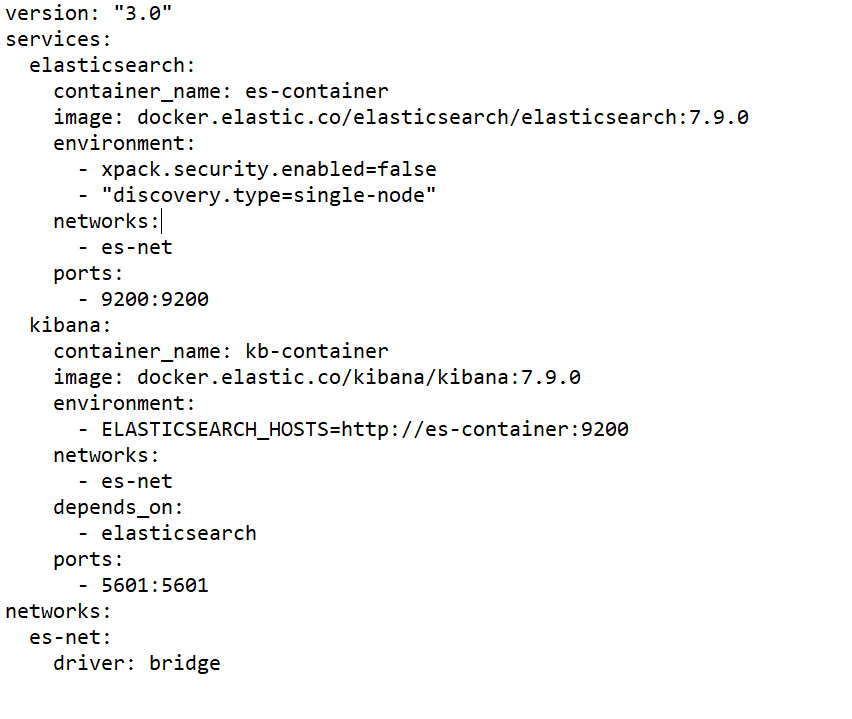
1. Các trường hợp sử dụng

* Giám sát nhật ký và cơ sở hạ tầng : Kibana có thể được sử dụng để giám sát và phân tích các tệp nhật ký và số liệu cơ sở hạ tầng. Nó cho phép người dùng khắc phục sự cố, phát hiện sự bất thường và có được khả năng hiển thị về tình trạng và hiệu suất của các hệ thống và ứng dụng.
* Phân tích bảo mật : Kibana thường được sử dụng cùng với các tính năng bảo mật của Elaticsearch để phân tích nhật ký bảo mật, phát hiện các mối đe dọa và điều tra các sự cố bảo mật. Nó cung cấp các hình ảnh trực quan và bảng điều khiển để xác định các mẫu và điểm bất thường trong dữ liệu bảo mật.
* Internet of Things (IoT) : Kibana có thể được sử dụng để trực quan hóa và giám sát các luồng dữ liệu IoT trong thời gian thực. Nó giúp phân tích dữ liệu cảm biến, theo dõi hiệu suất của thiết bị và xác định các mẫu hoặc điểm bất thường trong hệ sinh thái IoT.

1. Cài đặt Kibana

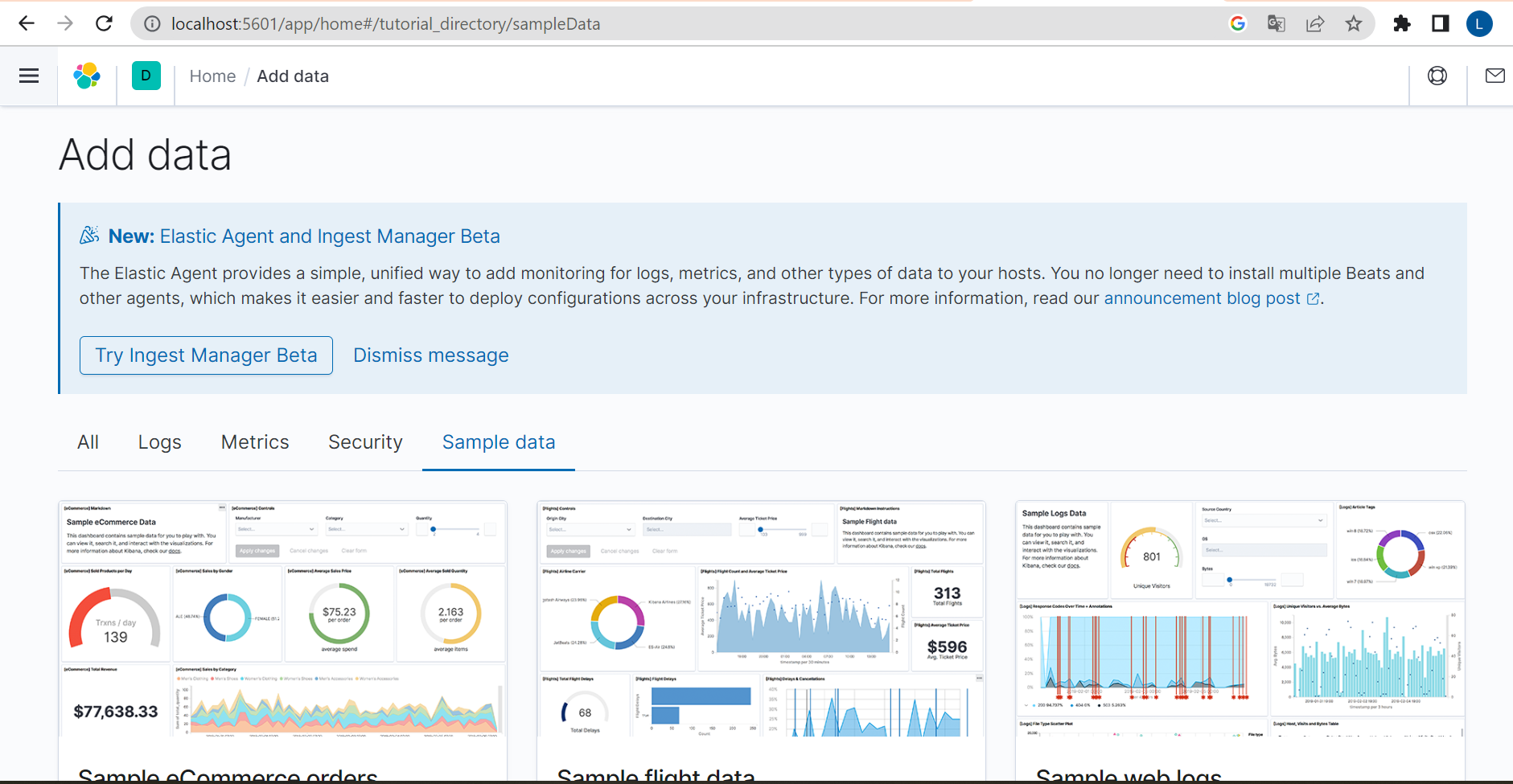
Đảm bảo rằng máy của bạn đã cài đặt Elasticsearch. Thông thường thì nên cài đặt bản Kibana cùng version với Elasticsearch

* Cài đặt trên docker
  + - Cài đặt Kibana dùng câu lệnh “ **docker run -d --name kibana --net somenetwork -p 5601:5601 kibana:7.9.0** ” với tag là version cần cài và lưu ý cần thêm network trước “ **docker network create somenetwork** “
    - Sau khi chạy xong truy cập “ <http://localhost:5601>” để truy cập vào kibana
  + Cài đặt với docker compose
    - Đảm bảo rằng đã cài docker compose viết file docker-compose.yml
    - Sau khi hoàn thành file docker compose dùng câu lệnh “ **docker-compose up -d “** để chạy service
    - Dùng câu lệnh “  **docker-compose down “** để dừng service



Ảnh 2.0 File docker-compose.yml

* Cài đặt trên windown
  + - Trên windown sau khi cài Elasticsearch ta tải thêm file rar của Kibana từ đường dẫn “ <https://www.elastic.co/fr/downloads/past-releases/kibana-7-9-0> ”. Bạn có thể cài các bản khác nhau.
    - Sau khi tải và giải nén ta tiến hành vào “**\kibana-7.9.0-windows-x86\_64\bin**” và chạy file **kibana.bat**
    - Sau khi chạy hoàn tất tiến hành truy cập <http://localhost:5601> để vào giao diện của kibana

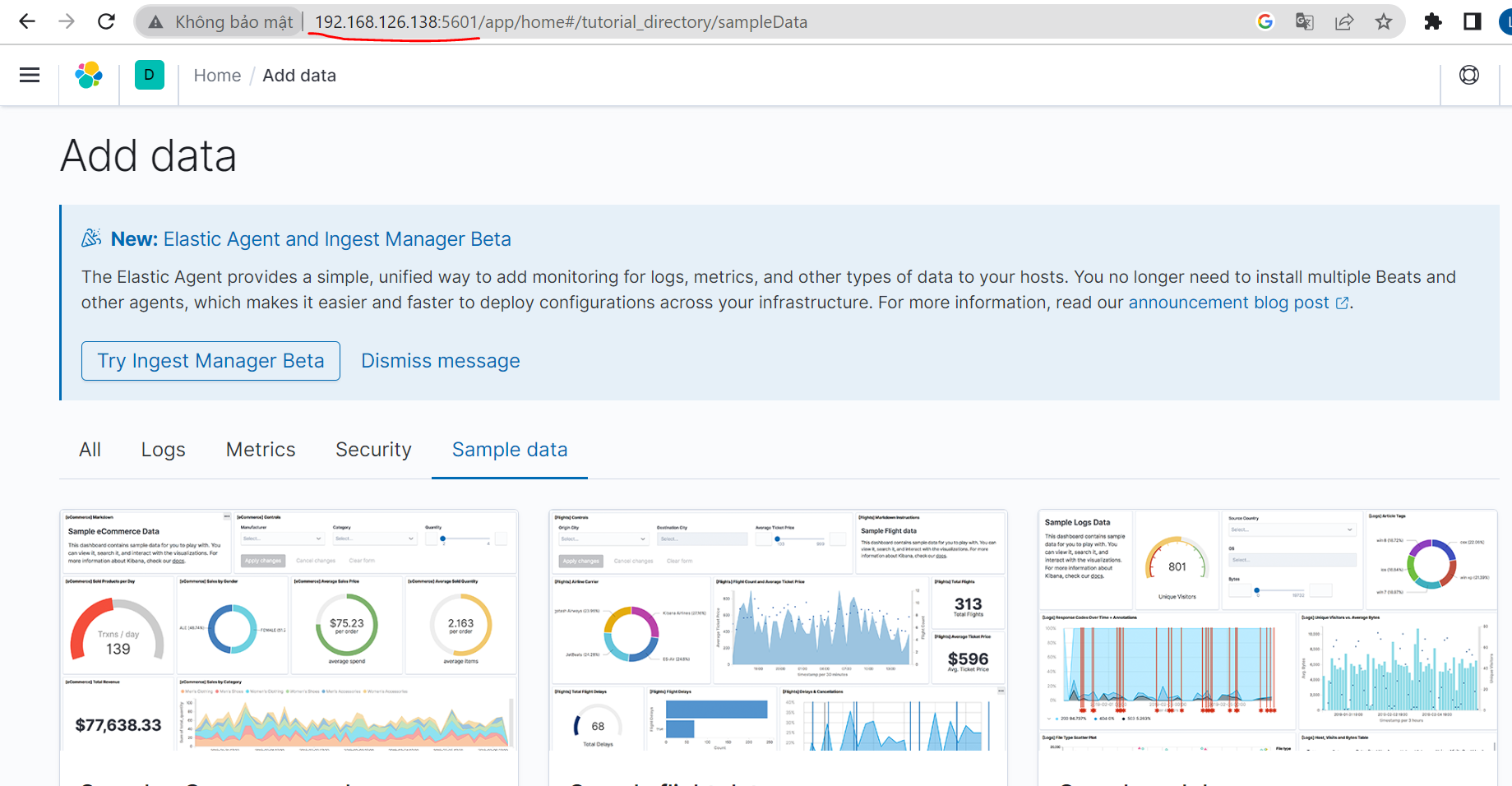


Ảnh 2.1 Giao diện kibana

* Cài đặt trên linux (centos)
  + - Để cài đặt Kibana trên linux đảm bảo rằng Elasticsearch đã được cài đặt và chạy ổn định.
    - Có nhiều cách để tải xuống kibana như cài qua repo hoặc cài qua wget để tải project xuống.
    - Trong ví dụ này tôi cài qua wget kibana dùng câu lệnh “ **wget** [**https://artifacts.elastic.co/downloads/kibana/kibana-7.9.0-x86\_64.rpm**](https://artifacts.elastic.co/downloads/kibana/kibana-7.9.0-x86_64.rpm) ”. Lưu ý vê vị trí lưu tệp để tránh việc không đủ bộ nhớ.

Sau khi tải xong tiến hành cài projetc với câu lệnh “**sudo rpm -ivh kibana-7.9.0-x86\_64.rpm**”.

* + - Sau khi cài xong tiến hành chạy Kibana với câu lệnh “**sudo systemctl start kibana**”. Để kibana khởi chạy cùng với hệ điều hành dùng câu lệnh “**sudo systemctl enable kibana**”. Lưu ý bên phía máy client phải mở firewall port 5601 như trên Elasticsearch.



Ảnh 2.2 Triển khai trên server linux

1. Kibana

* Custom giao diện trong Kibana
  + - Kibana Canvas: Canvas là một tính năng trong Kibana cho phép bạn tạo ra các bảng điều khiển tùy chỉnh, trình diễn dữ liệu và báo cáo trong một giao diện trực quan. Bạn có thể tạo các hình ảnh, biểu đồ, bảng và hiệu ứng để hiển thị dữ liệu theo cách riêng của bạn.
    - Kibana Visualization: Kibana cung cấp nhiều loại biểu đồ và hình ảnh để hiển thị dữ liệu. Bạn có thể tạo các biểu đồ cột, biểu đồ vòng, biểu đồ đường, biểu đồ phân tán và nhiều loại khác. Bạn có thể tùy chỉnh các thuộc tính, màu sắc và kiểu biểu đồ để phù hợp với giao diện của bạn.
    - Kibana Dashboard: Kibana cho phép bạn tạo bảng điều khiển tùy chỉnh bằng cách kết hợp các biểu đồ, hình ảnh và bảng đã tạo. Bạn có thể sắp xếp, thay đổi kích thước và tổ chức các phần tử trong bảng điều khiển để hiển thị dữ liệu theo ý muốn.
    - Kibana Plugin: Kibana hỗ trợ việc phát triển các plugin tùy chỉnh để mở rộng chức năng và giao diện của nó. Bạn có thể viết các plugin để thêm các tính năng mới, tùy chỉnh giao diện và tích hợp với các hệ thống và dịch vụ khác.
    - Kibana Styling: Bạn có thể tùy chỉnh giao diện bằng cách sử dụng CSS để thay đổi màu sắc, phông chữ, kích thước và kiểu chữ của các phần tử trong Kibana.