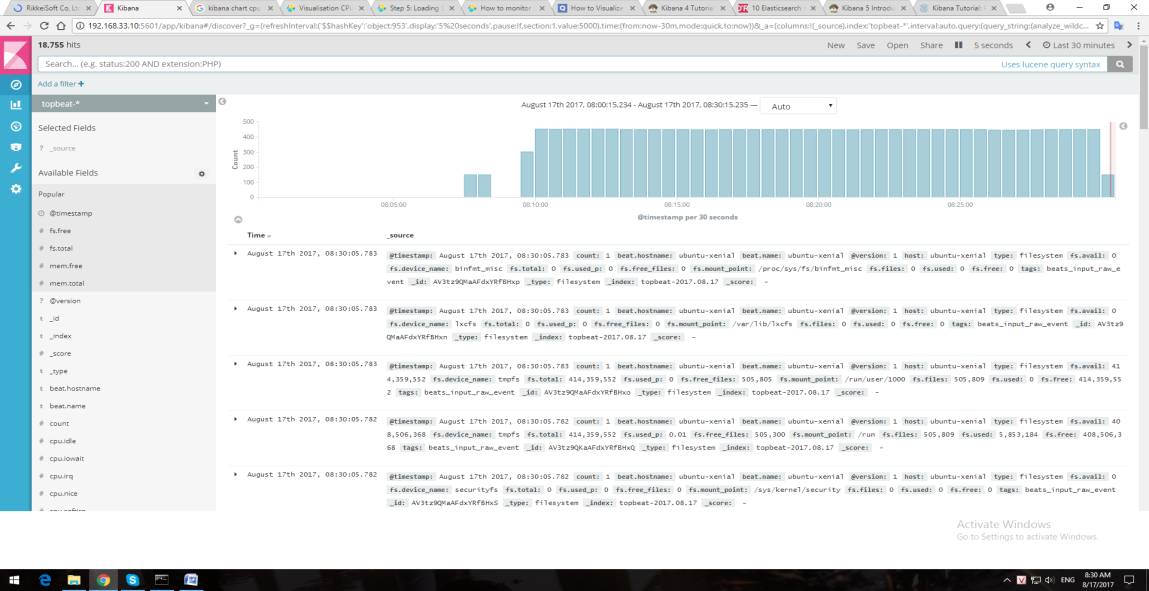
16/8/2017: Kibana

1. Kibana là gì?

Kibana là một nền phân tích và phân tích mã nguồn mở được thiết kế để làm việc với Elasticsearch. Bạn sử dụng Kibana để tìm kiếm, xem và tương tác với dữ liệu được lưu trữ trong các chỉ số Elasticsearch. Bạn có thể dễ dàng thực hiện phân tích dữ liệu tiên tiến và hình dung dữ liệu của bạn trong nhiều bảng xếp hạng, bảng biểu và bản đồ. Kibana giúp bạn dễ hiểu số lượng dữ liệu lớn. Giao diện đơn giản, dựa trên trình duyệt của nó cho phép bạn nhanh chóng tạo và chia sẻ bảng điều khiển động hiển thị thay đổi cho truy vấn Elasticsearch trong thời gian thực.

1. Giao diện
   1. Discover view được sử dụng để xem danh sách tài liệu và tìm kiếm các tài liệu cụ thể. 

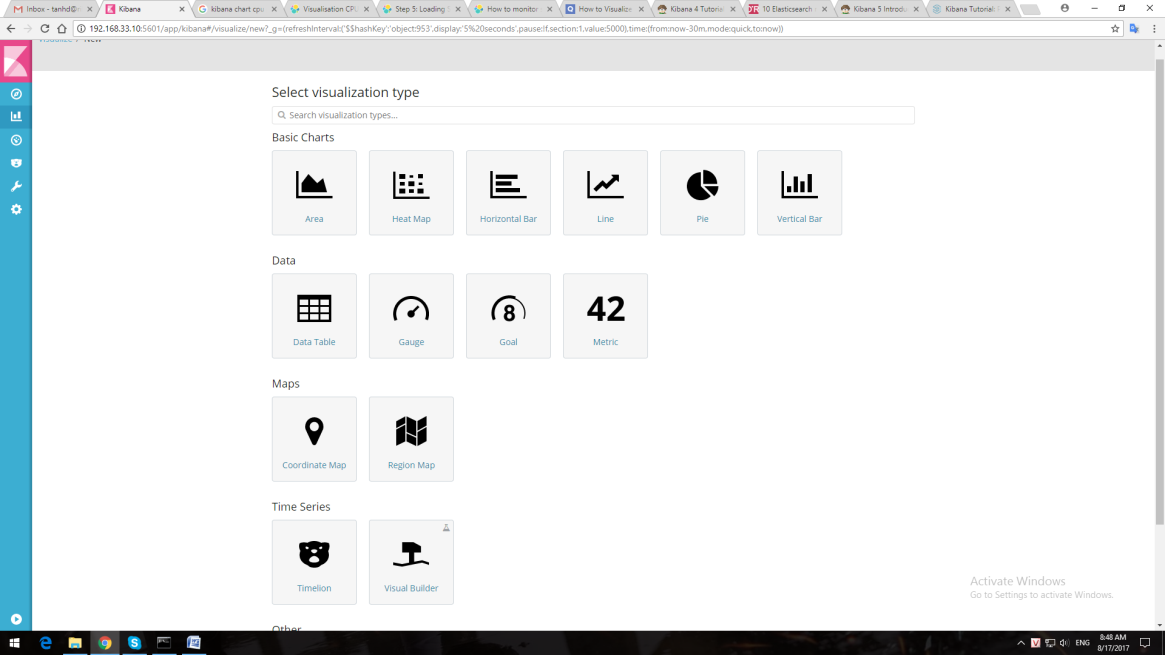
Search top bar để tìm kiếm các document. Có các options để save, load, share ở ngay bên trên thanh search.

Bên trái là danh sách các trường tồn tại trong document  
Trong khu vực chính của trang bạn tìm thấy một bản phân phối các tài liệu qua thời gian và danh sách tài liệu thực tế trong chỉ mục.

Đối với tất cả các chỉ số dựa trên thời gian, bạn có thể chọn phạm vi thời gian mà bạn thực sự muốn xem với trình chọn thời gian ở trên cùng bên phải. Bạn có thể đặt phạm vi lựa chọn một lựa chọn nhanh chóng hoặc chỉ định nó tương đối từ bây giờ hoặc như là phạm vi thời gian tuyệt đối.



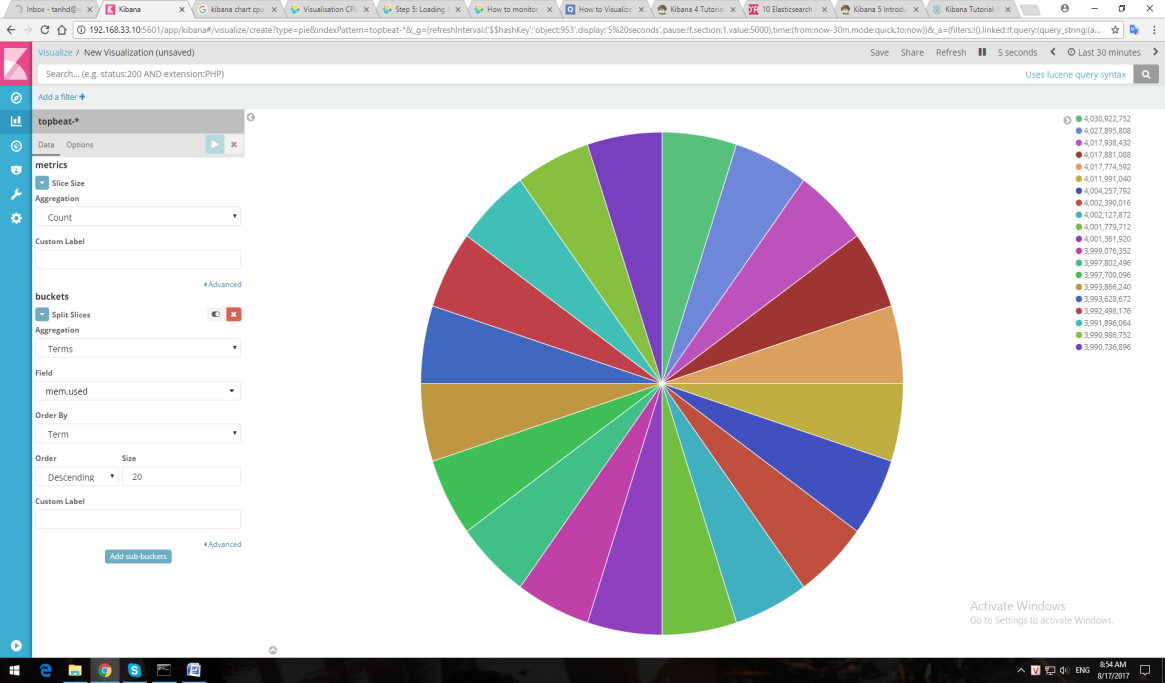
* 1. Visualize được sử dụng để tạo ra các hình ảnh hóa như đồ thị từ dữ liệu của bạn.



Có nhiều lữa chọn như trong hình.

* + 1. Pie chart

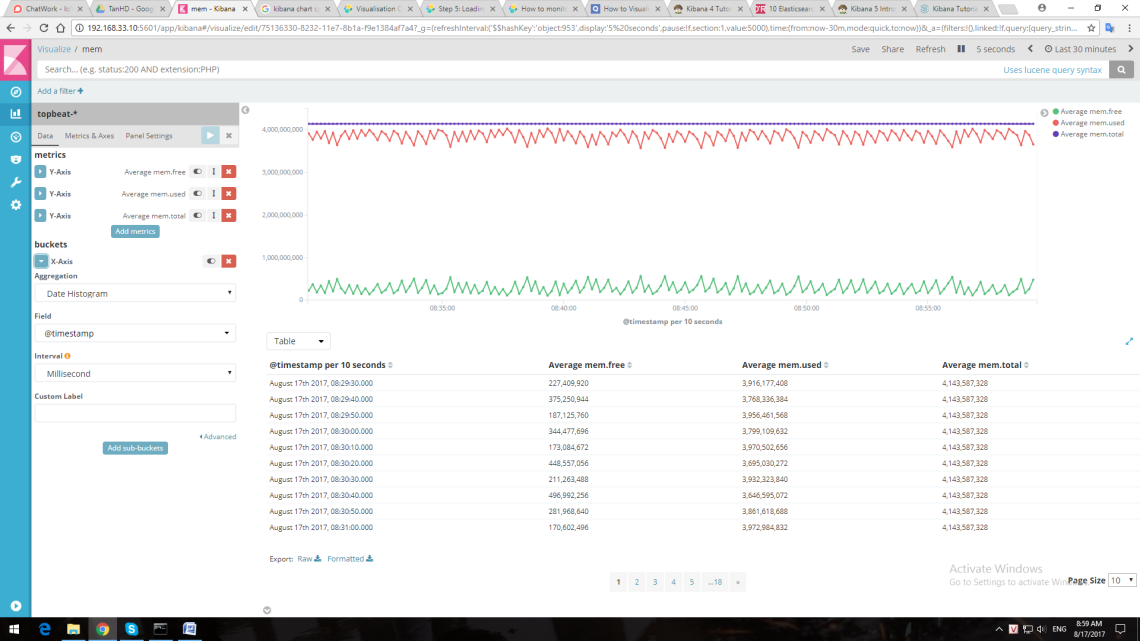
Sau khi bạn chọn kiểu hình ảnh hóa bạn đã chọn cho dù bạn muốn sử dụng dữ liệu hoàn chỉnh từ một chỉ mục hoặc dữ liệu từ một tìm kiếm đã lưu trước đó Trong trình chỉnh sửa hình ảnh mà bạn có thể nhìn thấy trong ảnh chụp màn hình bên dưới, bạn sẽ có thanh tìm kiếm ở đầu màn hình và các hành động Tạo, Save, Load và Share và trình chọn thời gian.



Để chia biểu đồ ta dùng Split slices

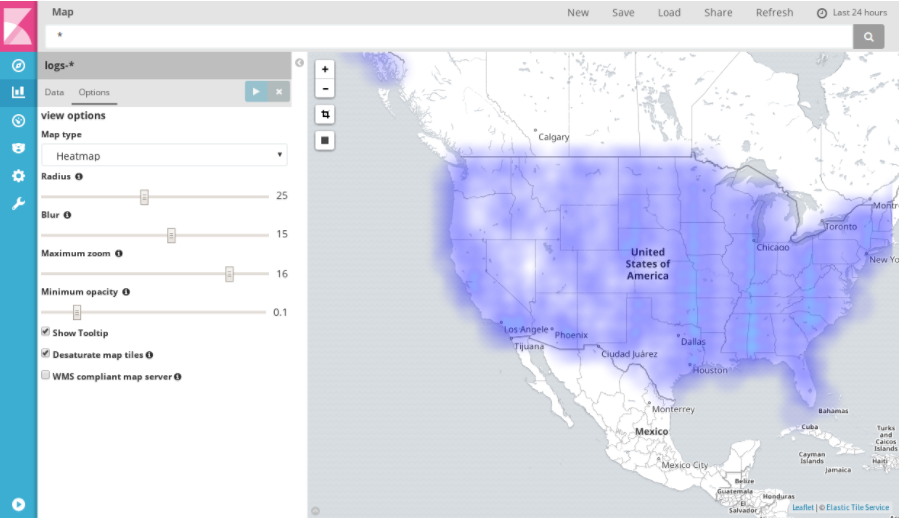
* + 1. Line Chart

Để tạo một biểu đồ cho thấy một số dữ liệu theo thời gian, chúng ta sử dụng tập hợp Histogram Date trên trường @timestamp của chúng ta.



* + 1. Tile Map

Việc kết hợp bản đồ ngói hơi khác một chút so với các biểu đồ cổ điển mà chúng ta đã xem xét cho đến nay. Nó có thể được sử dụng để hình dung dữ liệu chứa tọa độ địa lý



* 1. TImelion

Timelion sử dụng một ngôn ngữ biểu hiện tùy chỉnh để mô tả sơ đồ của bạn. Nó có khả năng làm một số công việc biểu đồ, mà bạn không thể đạt được với tập hợp một cách dễ dàng

Để lấy dữ liệu từ Elasticsearch, có thể sử dụng chức năng .es (). Nếu chúng ta muốn lọc các câu trả lời thành công, chúng ta có thể sử dụng tham số q cho hàm để chỉ định một truy vấn: .es (q = response: 200)

.es(q=response:200).label('current') .es(q=response:200, offset=-1d).label('previous day')

Nếu chúng ta muốn thêm chúng vào bảng điều khiển, chúng ta có thể sử dụng chức năng lưu và chọn Save current expression dưới dạng bảng điều khiển Kibana và chỉ định tên cho bảng điều khiển

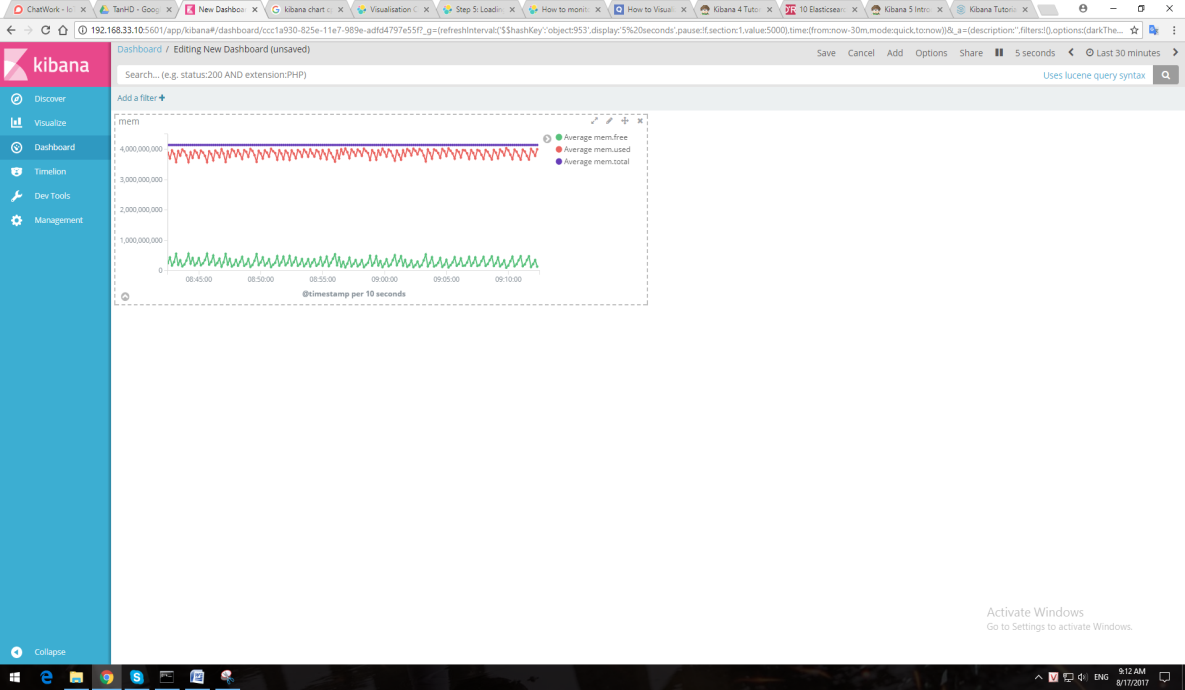
* 1. Dashboards

Bây giờ chúng tôi đã tạo ra một số hình ảnh hóa, vì vậy chúng tôi có thể hướng đến phần cuối của loạt bài giới thiệu này - tạo bảng điều khiển.

Nếu bạn chưa tạo bảng điều khiển nào, bạn sẽ bắt đầu với chế độ xem trống. Sử dụng nút Thêm trên đầu trang để thêm hình ảnh đã lưu trước đó.

Có thể xóa hoặ chỉnh sửa kích thước chỉ với các thao tác click chuột.

Một khi chúng ta hài lòng với cách bố trí, chúng ta có thể lưu bảng điều khiển. Bạn có thể sử dụng thời gian Store với tùy chọn bảng điều khiển để lưu khoảng thời gian hiện thời đã chọn từ bộ chọn ngày với bảng điều khiển.



1. Tài liệu :
   1. https://www.timroes.de/2016/10/23/kibana5-introduction/#dashboards